INTERNATIONAL STANDARD

ISO/IEC 15408-1

Third edition
2009-12-15

Corrected version
2014-01-15

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

Part 1: Introduction and general model

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 1: Introduction et modèle général

Reference number
ISO/IEC 15408-1:2009(E)

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

Contents

Page

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 15408-1 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. The common XML source for both publications can be found at http://www.commoncriteriaportal.org/cc/

This third edition cancels and replaces the second edition (ISO/IEC 15408-1:2005), 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 components*

— *Part 3: Security assurance components*

This corrected version of ISO/IEC 15408-1:2009 incorporates miscellaneous editorial corrections related to the following:

— terminology: correction for the terms "security problem" and "security domains";

— clause 8.3: explanation of strict conformance, removal of former Figure 4.

Introduction

ISO/IEC 15408 permits comparability between the results of independent security evaluations. ISO/IEC 15408 does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

ISO/IEC 15408 is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using ISO/IEC 15408 in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

ISO/IEC 15408 addresses protection of assets from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. ISO/IEC 15408 may also be applicable to aspects of IT security outside of these three. ISO/IEC 15408 is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. Apart from IT security, ISO/IEC 15408 may be applied in other areas of IT, but makes no claim of applicability in these areas.

Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of ISO/IEC 15408. Some of these are identified below.

a) ISO/IEC 15408 does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognised that significant security can often be achieved through or supported by administrative measures such as organisational, personnel, physical, and procedural controls.

b) The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area.

c) ISO/IEC 15408 does not address the evaluation methodology under which the criteria should be applied. This methodology is given in ISO/IEC 18045.

d) ISO/IEC 15408 does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that ISO/IEC 15408 will be used for evaluation purposes in the context of such a framework.

e) The procedures for use of evaluation results in accreditation are outside the scope of ISO/IEC 15408. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors should make separate provisions for those aspects.

f) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in ISO/IEC 15408. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

ISO terminology, such as "can", "informative", "may", "normative", "shall" and "should" used throughout the document are defined in the ISO/IEC Directives, Part 2. Note that the term "should" has an additional meaning applicable when using this standard. See the note below. The following definition is given for the use of “should” in ISO/IEC 15408.

should

within normative text, “should” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC Directives, Part 2).

NOTE ISO/IEC 15408 interprets “not necessarily required” to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

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

Part 1: Introduction and general model

1 Scope

This part of ISO/IEC 15408 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

Part one provides an overview of all parts of ISO/IEC 15408 standard. It describes the various parts of the standard; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); the evaluation context and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation, evaluation results are described. This part of ISO/IEC 15408 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology are given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

2 Normative references

The following referenced documents are indispensable for the application of ISO/IEC 15408 part 1. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE This clause contains only those terms which are used in a specialized way throughout ISO/IEC 15408. Some combinations of common terms used in ISO/IEC 15408, while not meriting inclusion in this clause, are explained for clarity in the context where they are used.

3.1 Terms and definitions common in ISO/IEC 15408

3.1.1
adverse actions
actions performed by a threat agent on an asset

3.1.2
assets
entities that the owner of the TOE presumably places value upon

3.1.3
assignment
specification of an identified parameter in a component (of ISO/IEC 15408) or requirement

3.1.4
assurance
grounds for confidence that a TOE meets the SFRs

3.1.5
attack potential
measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation

3.1.6
augmentation
addition of one or more requirement(s) to a package

3.1.7
authentication data
information used to verify the claimed identity of a user

3.1.8
authorised user
TOE user who may, in accordance with the SFRs, perform an operation

3.1.9
class
set of ISO/IEC 15408 families that share a common focus

3.1.10
coherent
logically ordered and having discernible meaning

NOTE 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.

3.1.11
complete
property where all necessary parts of an entity have been provided

NOTE 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.

3.1.12
component
smallest selectable set of elements on which requirements may be based

3.1.13
composed assurance package
assurance package consisting of requirements drawn from ISO/IEC 15408-3 (predominately from the ACO class), representing a point on ISO/IEC 15408 predefined composition assurance scale

3.1.14
confirm
declare that something has been reviewed in detail with an independent determination of sufficiency

NOTE The level of rigour required depends on the nature of the subject matter. This term is only applied to evaluator actions.

3.1.15
connectivity
property of the TOE allowing interaction with IT entities external to the TOE

NOTE This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

3.1.16
consistent
relationship between two or more entities such that there are no apparent contradictions between these entities

3.1.17
counter, verb
meet an attack where the impact of a particular threat is mitigated but not necessarily eradicated

3.1.18
demonstrable conformance
relation between an ST and a PP, where the ST provides a solution which solves the generic security problem in the PP

NOTE The PP and the ST may contain entirely different statements that discuss different entities, use different concepts etc. Demonstrable conformance is also suitable for a TOE type where several similar PPs already exist, thus allowing the ST author to claim conformance to these PPs simultaneously, thereby saving work.

3.1.19
demonstrate
provide a conclusion gained by an analysis which is less rigorous than a “proof”

3.1.20
dependency
relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

3.1.21
describe
provide specific details of an entity

3.1.22
determine
affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion

NOTE The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms “confirm” or “verify” which imply that an analysis has already been performed which needs to be reviewed

3.1.23
development environment
environment in which the TOE is developed

3.1.24
element
indivisible statement of a security need

3.1.25
ensure
guarantee a strong causal relationship between an action and its consequences

NOTE When this term is preceded by the word “help” it indicates that the consequence is not fully certain, on the basis of that action alone.

3.1.26
evaluation
assessment of a PP, an ST or a TOE, against defined criteria

3.1.27
evaluation assurance level
set of assurance requirements drawn from ISO/IEC 15408-3, representing a point on the ISO/IEC 15408 predefined assurance scale, that form an assurance package

3.1.28
evaluation authority
body that sets the standards and monitors the quality of evaluations conducted by bodies within a specific community and implements ISO/IEC 15408 for that community by means of an evaluation scheme

3.1.29
evaluation scheme
administrative and regulatory framework under which ISO/IEC 15408 is applied by an evaluation authority within a specific community

3.1.30
exhaustive
characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan

NOTE This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is related to “systematic” but is considerably stronger, in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to ensure that all possible avenues have been exercised.

3.1.31
explain
give argument accounting for the reason for taking a course of action

NOTE 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.

3.1.32
extension
addition to an ST or PP of functional requirements not contained in ISO/IEC 15408-2 and/or assurance requirements not contained in ISO/IEC 15408-3

3.1.33
external entity
human or IT entity possibly interacting with the TOE from outside of the TOE boundary

NOTE An external entity can also be referred to as a user.

3.1.34
family
set of components that share a similar goal but differ in emphasis or rigour

3.1.35
formal
expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts

3.1.36
guidance documentation
documentation that describes the delivery, preparation, operation, management and/or use of the TOE

3.1.37
identity
representation uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE

NOTE An example of such a representation is a string. For a human user, the representation can be the full or abbreviated name or a (still unique) pseudonym.

3.1.38
informal
expressed in natural language

3.1.39
inter TSF transfers
communicating data between the TOE and the security functionality of other trusted IT products

3.1.40
internal communication channel
communication channel between separated parts of the TOE

3.1.41
internal TOE transfer
communicating data between separated parts of the TOE

3.1.42
internally consistent
no apparent contradictions exist between any aspects of an entity

NOTE In terms of documentation, this means that there can be no statements within the documentation that can be taken to contradict each other.

3.1.43
iteration
use of the same component to express two or more distinct requirements

3.1.44
justification
analysis leading to a conclusion

NOTE "Justification" 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.

3.1.45
object
passive entity in the TOE, that contains or receives information, and upon which subjects perform operations

3.1.46
operation
⟨on a component of ISO/IEC 15408⟩ modification or repetition of a component

NOTE Allowed operations on components are assignment, iteration, refinement and selection.

3.1.47
operation
⟨on an object⟩ specific type of action performed by a subject on an object

3.1.48
operational environment
environment in which the TOE is operated

3.1.49
organizational security policy
set of security rules, procedures, or guidelines for an organization

NOTE A policy may pertain to a specific operational environment.

3.1.50
package
named set of either security functional or security assurance requirements

NOTE An example of a package is “EAL 3”.

3.1.51
Protection Profile evaluation
assessment of a PP against defined criteria

3.1.52
Protection Profile
implementation-independent statement of security needs for a TOE type

3.1.53
prove
show correspondence by formal analysis in its mathematical sense

NOTE It is completely rigorous 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.

3.1.54
refinement
addition of details to a component

3.1.55
role
predefined set of rules establishing the allowed interactions between a user and the TOE

3.1.56
secret
information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP

3.1.57
secure state
state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs

3.1.58
security attribute
property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs

3.1.59
security function policy
set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs

3.1.60
security objective
statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions

3.1.61
security problem
statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address

NOTE This statement consists of a combination of:

— threats to be countered by the TOE and its operational environment,

— the OSPs enforced by the TOE and its operational environment, and

— the assumptions that are upheld for the operational environment of the TOE.

3.1.62
security requirement
requirement, stated in a standardised language, which is meant to contribute to achieving the security objectives for a TOE

3.1.63
Security Target
implementation-dependent statement of security needs for a specific identified TOE

3.1.64
selection
specification of one or more items from a list in a component

3.1.65
semiformal
expressed in a restricted syntax language with defined semantics

3.1.66
specify
provide specific details about an entity in a rigorous and precise manner

3.1.67
strict conformance
hierarchical relationship between a PP and an ST where all the requirements in the PP also exist in the ST

NOTE This relation can be roughly defined as “the ST shall contain all statements that are in the PP, but may contain more”. Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner.

3.1.68
ST evaluation
assessment of an ST against defined criteria

3.1.69
subject
active entity in the TOE that performs operations on objects

3.1.70
target of evaluation
set of software, firmware and/or hardware possibly accompanied by guidance

3.1.71
threat agent
entity that can adversely act on assets

3.1.72
TOE evaluation
assessment of a TOE against defined criteria

3.1.73
TOE resource
anything useable or consumable in the TOE

3.1.74
TOE security functionality
combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

3.1.75
trace, verb
perform an informal correspondence analysis between two entities with only a minimal level of rigour

3.1.76
transfers outside of the TOE
TSF mediated communication of data to entities not under the control of the TSF

3.1.77
translation
describes the process of describing security requirements in a standardised language.

NOTE Use of the term translation in this context is not literal and does not imply that every SFR expressed in standardised language can also be translated back to the security objectives.

3.1.78
trusted channel
a means by which a TSF and another trusted IT product can communicate with necessary confidence

3.1.79
trusted IT product
IT product, other than the TOE, which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly

NOTE An example of a trusted IT product would be one that has been separately evaluated.

3.1.80
trusted path
means by which a user and a TSF can communicate with the necessary confidence

3.1.81
TSF data
data for the operation of the TOE upon which the enforcement of the SFR relies

3.1.82
TSF interface
means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF

3.1.83
user data
data for the user, that does not affect the operation of the TSF

3.1.84
verify
rigorously review in detail with an independent determination of sufficiency

NOTE Also see "confirm". This term has more rigorous connotations. The term "verify" is used in the context of evaluator actions where an independent effort is required of the evaluator.

3.2 Terms and definitions related to the ADV class

NOTE The following terms are used in the requirements for software internal structuring. Some of these are derived from the IEEE Std 610.12-1990, *Standard glossary of software engineering terminology, Institute of Electrical and Electronics Engineers*.

3.2.1
administrator
entity that has a level of trust with respect to all policies implemented by the TSF

NOTE Not all PPs or STs assume the same level of trust for administrators. Typically administrators are assumed to adhere at all times to the policies in the ST of the TOE. Some of these policies may be related to the functionality of the TOE, others may be related to the operational environment.

3.2.2
call tree
identifies the modules in a system in diagrammatic form showing which modules call one another

NOTE Adapted from IEEE Std 610.12-1990.

3.2.3
cohesion
module strength
manner and degree to which the tasks performed by a single software module are related to one another

[IEEE Std 610.12-1990]

NOTE Types of cohesion include coincidental, communicational, functional, logical, sequential, and temporal. These types of cohesion are described by the relevant term entry.

3.2.4
coincidental cohesion
module with the characteristic of performing unrelated, or loosely related, activities

[IEEE Std 610.12-1990]

NOTE See also cohesion (3.2.3).

3.2.5
communicational cohesion
module containing functions that produce output for, or use output from, other functions within the module

[IEEE Std 610.12-1990]

NOTE 1 See also cohesion (3.2.3).

NOTE 2 An example of a communicationally cohesive module is an access check module that includes mandatory, discretionary, and capability checks.

3.2.6
complexity
measure of how difficult software is to understand, and thus to analyse, test, and maintain

[IEEE Std 610.12-1990]

NOTE Reducing complexity is the ultimate goal for using modular decomposition, layering and minimization. Controlling coupling and cohesion contributes significantly to this goal.

A good deal of effort in the software engineering field has been expended in attempting to develop metrics to measure the complexity of source code. Most of these metrics use easily computed properties of the source code, such as the number of operators and operands, the complexity of the control flow graph (cyclomatic complexity), the number of lines of source code, the ratio of comments to executable code, and similar measures. Coding standards have been found to be a useful tool in generating code that is more readily understood.

The TSF internals (ADV_INT) family calls for a complexity analysis in all components. It is expected that the developer will provide support for the claims that there has been a sufficient reduction in complexity. This support could include the developer's programming standards, and an indication that all modules meet the standard (or that there are some exceptions that are justified by software engineering arguments). It could include the results of tools used to measure some of the properties of the source code, or it could include other support that the developer finds appropriate.

3.2.7
coupling
manner and degree of interdependence between software modules

[IEEE Std 610.12-1990]

NOTE Types of coupling include call, common and content coupling. These are characterised below.

3.2.8
call coupling
relationship between two modules communicating strictly through their documented function calls

NOTE Examples of call coupling are data, stamp and control.

3.2.9
call coupling
⟨data⟩ relationship between two modules communicating strictly through the use of call parameters that represent single data items

NOTE See also call coupling (3.2.8).

3.2.10
call coupling
⟨stamp⟩ relationship between two modules communicating through the use of call parameters that comprise multiple fields or that have meaningful internal structures

NOTE See also call coupling (3.2.8).

3.2.11
call coupling
⟨control⟩ relationship between two modules if one passes information that is intended to influence the internal logic of the other

NOTE See also call coupling (3.2.8).

3.2.12
common coupling
relationship between two modules sharing a common data area or other common system resource

NOTE Global variables indicate that modules using those global variables are common coupled. Common coupling through global variables is generally allowed, but only to a limited degree.

For example, variables that are placed into a global area, but are used by only a single module, are inappropriately placed, and should be removed. Other factors that need to be considered in assessing the suitability of global variables are:

The number of modules that modify a global variable: In general, only a single module should be allocated the responsibility for controlling the contents of a global variable, but there may be situations in which a second module may share that responsibility; in such a case, sufficient justification must be provided. It is unacceptable for this responsibility to be shared by more than two modules. (In making this assessment, care should be given to determining the module actually responsible for the contents of the variable; for example, if a single routine is used to modify the variable, but that routine simply performs the modification requested by its caller, it is the calling module that is responsible, and there may be more than one such module). Further, as part of the complexity determination, if two modules are responsible for the contents of a global variable, there should be clear indications of how the modifications are coordinated between them.

The number of modules that reference a global variable: Although there is generally no limit on the number of modules that reference a global variable, cases in which many modules make such a reference should be examined for validity and necessity.

3.2.13
content coupling
relationship between two modules where one makes direct reference to the internals of the other

NOTE Examples include modifying code of, or referencing labels internal to, the other module. The result is that some or all of the content of one module are effectively included in the other. Content coupling can be thought of as using unadvertised module interfaces; this is in contrast to call coupling, which uses only advertised module interfaces.

3.2.14
domain separation
security architecture property whereby the TSF defines separate security domains for each user and for the TSF and ensures that no user process can affect the contents of a security domain of another user or of the TSF

3.2.15
functional cohesion
functional property of a module which performs activities related to a single purpose

[IEEE Std 610.12-1990]

NOTE A functionally cohesive module transforms a single type of input into a single type of output, such as a stack manager or a queue manager. See also cohesion (3.2.3).

3.2.16
interaction
general communication-based activity between entities

3.2.17
interface
means of interaction with a component or module

3.2.18
layering
design technique where separate groups of modules (the layers) are hierarchically organised to have separate responsibilities such that one layer depends only on layers below it in the hierarchy for services, and provides its services only to the layers above it

NOTE Strict layering adds the constraint that each layer receives services only from the layer immediately beneath it, and provides services only to the layer immediately above it.

3.2.19
logical cohesion
procedural cohesion
characteristics of a module performing similar activities on different data structures

NOTE A module exhibits logical cohesion if its functions perform related, but different, operations on different inputs. See also “cohesion”.

3.2.20
modular decomposition
process of breaking a system into components to facilitate design, development and evaluation

[IEEE Std 610.12-1990]

3.2.21
non-bypassability
〈of the TSF〉 security architecture property whereby all SFR-related actions are mediated by the TSF

3.2.22
security domains
environments provided by the TSF for the use by untrusted entities in such a way that these environments are isolated and protected from each other

3.2.23
sequential cohesion
module containing functions each of whose output is input for the following function in the module

[IEEE Std 610.12-1990]

NOTE An example of a sequentially cohesive module is one that contains the functions to write audit records and to maintain a running count of the accumulated number of audit violations of a specified type.

3.2.24
software engineering
application of a systematic, disciplined, quantifiable approach to the development and maintenance of software; that is, the application of engineering to software

[IEEE Std 610.12-1990]

NOTE As with engineering practices in general, some amount of judgement must be used in applying engineering principles. Many factors affect choices, not just the application of measures of modular decomposition, layering, and minimization. For example, a developer may design a system with future applications in mind that will not be implemented initially. The developer may choose to include some logic to handle these future applications without fully implementing them; further, the developer may include some calls to as-yet unimplemented modules, leaving call stubs. The developer's justification for such deviations from well-structured programs will have to be assessed using judgement, as well as the application of good software engineering discipline.

3.2.25
temporal cohesion
characteristics of a module containing functions that need to be executed at about the same time

NOTE 1 Adapted from [IEEE Std 610.12-1990].

NOTE 2 Examples of temporally cohesive modules include initialization, recovery, and shutdown modules.

3.2.26
TSF self-protection
security architecture property whereby the TSF cannot be corrupted by non-TSF code or entities

3.3 Terms and definitions related to the AGD class

3.3.1
installation
procedure performed by a human user embedding the TOE in its operational environment and putting it into an operational state

NOTE This operation is performed normally only once, after receipt and acceptance of the TOE. The TOE is expected to be progressed to a configuration allowed by the ST. If similar processes have to be performed by the developer they are denoted as "generation" throughout ALC: Life-cycle support. If the TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as installation.

3.3.2
operation
usage phase of the TOE including "normal usage", administration and maintenance of the TOE after delivery and preparation

3.3.3
preparation
activity in the life-cycle phase of a product, comprising the customer's acceptance of the delivered TOE and its installation which may include such things as booting, initialisation, start-up and progressing the TOE to a state ready for operation

3.4 Terms and definitions related to the ALC class

3.4.1
acceptance criteria
criteria to be applied when performing the acceptance procedures (e.g. successful document review, or successful testing in the case of software, firmware or hardware)

3.4.2
acceptance procedures
procedures followed in order to accept newly created or modified configuration items as part of the TOE, or to move them to the next step of the life-cycle

NOTE These procedures identify the roles or individuals responsible for the acceptance and the criteria to be applied in order to decide on the acceptance.

There are several types of acceptance situations some of which may overlap:

a) acceptance of an item into the configuration management system for the first time, in particular inclusion of software, firmware and hardware components from other manufacturers into the TOE ("integration");

b) progression of configuration items to the next life-cycle phase at each stage of the construction of the TOE (e.g. module, subsystem, quality control of the finished TOE);

c) subsequent to transports of configuration items (for example parts of the TOE or preliminary products) between different development sites;

d) subsequent to the delivery of the TOE to the consumer.

3.4.3
configuration management
CM
discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status and verify compliance with specified requirements

NOTE Adapted from IEEE Std 610.12.

3.4.4
CM documentation
all CM documentation including CM output, CM list (configuration list), CM system records, CM plan and CM usage documentation

3.4.5
configuration management evidence
everything that may be used to establish confidence in the correct operation of the CM system

NOTE For example, CM output, rationales provided by the developer, observations, experiments or interviews made by the evaluator during a site visit.

3.4.6
configuration item
object managed by the CM system during the TOE development

NOTE These may be either parts of the TOE or objects related to the development of the TOE like evaluation documents or development tools. CM items may be stored in the CM system directly (for example files) or by reference (for example hardware parts) together with their version.

3.4.7
configuration list
configuration management output document listing all configuration items for a specific product together with the exact version of each configuration management item relevant for a specific version of the complete product

NOTE This list allows distinguishing the items belonging to the evaluated version of the product from other versions of these items belonging to other versions of the product. The final configuration management list is a specific document for a specific version of a specific product. (Of course the list can be an electronic document inside of a configuration management tool. In that case it can be seen as a specific view into the system or a part of the system rather than an output of the system. However, for the practical use in an evaluation the configuration list will probably be delivered as a part of the evaluation documentation.) The configuration list defines the items that are under the configuration management requirements of ALC_CMC.

3.4.8
configuration management output
results, related to configuration management, produced or enforced by the configuration management system

NOTE These configuration management related results could occur as documents (for example filled paper forms, configuration management system records, logging data, hard-copies and electronic output data) as well as actions (for example manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are configuration lists, configuration management plans and/or behaviours during the product life-cycle.

3.4.9
configuration management plan
description of how the configuration management system is used for the TOE

NOTE The objective of issuing a configuration management plan is that staff members can see clearly what they have to do. From the point of view of the overall configuration management system this can be seen as an output document (because it may be produced as part of the application of the configuration management system). From the point of view of the concrete project it is a usage document because members of the project team use it in order to understand the steps that they have to perform during the project. The configuration management plan defines the usage

of the system for the specific product; the same system may be used to a different extent for other products. That means the configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE development.

3.4.10
configuration management system
set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of his products during their life-cycles

NOTE Configuration management systems may have varying degrees of rigour and function. At higher levels, configuration management systems may be automated, with flaw remediation, change controls, and other tracking mechanisms.

3.4.11
configuration management system records
output produced during the operation of the configuration management system documenting important configuration management activities

NOTE Examples of configuration management system records are configuration management item change control forms or configuration management item access approval forms.

3.4.12
configuration management tools
manually operated or automated tools realising or supporting a configuration management system

NOTE For example tools for the version management of the parts of the TOE.

3.4.13
configuration management usage documentation
part of the configuration management system, which describes, how the configuration management system is defined and applied by using for example handbooks, regulations and/or documentation of tools and procedures

3.4.14
delivery
transmission of the finished TOE from the production environment into the hands of the customer

NOTE This product life-cycle phase may include packaging and storage at the development site, but does not include transportations of the unfinished TOE or parts of the TOE between different developers or different development sites.

3.4.15
developer
organisation responsible for the development of the TOE

3.4.16
development
product life-cycle phase which is concerned with generating the implementation representation of the TOE

NOTE Throughout the ALC: Life-cycle support requirements, development and related terms (developer, develop) are meant in the more general sense to comprise development and production.

3.4.17
development tools
tools (including test software, if applicable) supporting the development and production of the TOE

NOTE For example for a software TOE, development tools are usually programming languages, compilers, linkers and generating tools.

3.4.18
implementation representation
least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement

NOTE 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.

3.4.19
life-cycle
sequence of stages of existence of an object (for example a product or a system) in time

3.4.20
life-cycle definition
definition of the life-cycle model

3.4.21
life cycle model
description of the stages and their relations to each other that are used in the management of the life-cycle of a certain object, how the sequence of stages looks like and which high level characteristics the stages have

NOTE See also Figure 1.

3.4.22
production
production life-cycle phase follows the development phase and consists of transforming the implementation representation into the implementation of the TOE, i.e. into a state acceptable for delivery to the customer

NOTE This phase may comprise manufacturing, integration, generation, internal transports, storage, and labelling of the TOE.

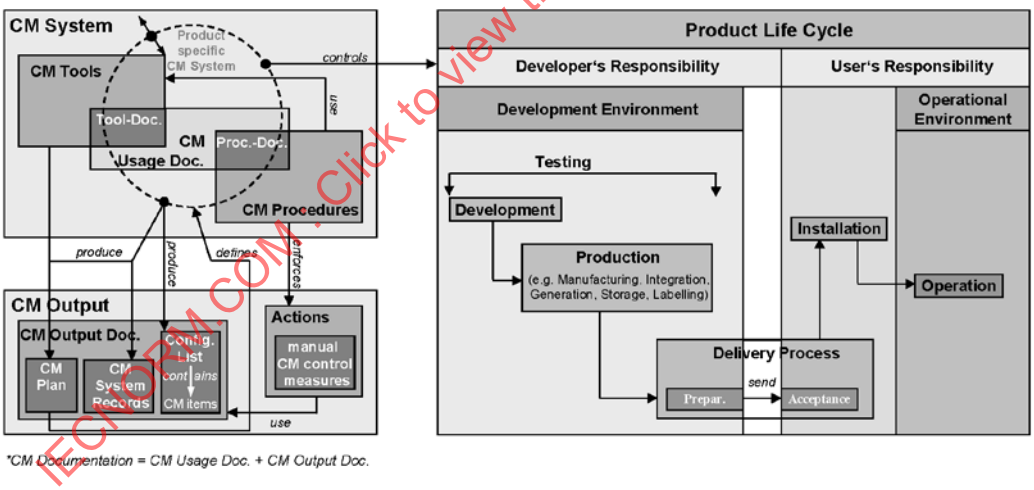

Figure 1 - Terminology in CM and in the product life-cycle

3.5 Terms and definitions related to the AVA class

3.5.1
covert channel
enforced, illicit signalling channel that allows a user to surreptitiously contravene the multi-level separation policy and unobservability requirements of the TOE

3.5.2
encountered potential vulnerabilities
potential weakness in the TOE identified by the evaluator while performing evaluation activities that could be used to violate the SFRs

3.5.3
exploitable vulnerability
weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE

3.5.4
monitoring attacks
generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds to the guidance documents

3.5.5
potential vulnerability
suspected, but not confirmed, weakness

NOTE Suspicion is by virtue of a postulated attack path to violate the SFRs.

3.5.6
residual vulnerability
weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE

3.5.7
vulnerability
weakness in the TOE that can be used to violate the SFRs in some environment

3.6 Terms and definitions related to the ACO class

3.6.1
base component
entity in a composed TOE, which has itself been the subject of an evaluation, providing services and resources to a dependent component

3.6.2
compatible (components)
property of a component able to provide the services required by the other component, through the corresponding interfaces of each component, in consistent operational environments

3.6.3
component TOE
successfully evaluated TOE that is part of another composed TOE

3.6.4
composed TOE
TOE comprised solely of two or more components that have been successfully evaluated

3.6.5
dependent component
entity in a composed TOE, which is itself the subject of an evaluation, relying on the provision on services by a base component

3.6.6
functional interface
external interface providing a user with access to functionality of the TOE which is not directly involved in enforcing security functional requirements

NOTE In a composed TOE these are the interfaces provided by the base component that are required by the dependent component to support the operation of the composed TOE.

4 Abbreviated terms

The following abbreviations are used in one or more parts of ISO/IEC 15408:

API	Application Programming Interface
CAP	Composed Assurance Package
CM	Configuration Management
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
GHz	Gigahertz
GUI	Graphical User Interface
IC	Integrated Circuit
IOCTL	Input Output Control
IP	Internet Protocol
IT	Information Technology
MB	Mega Byte
OS	Operating System
OSP	Organisational Security Policy
PC	Personal Computer
PCI	Peripheral Component Interconnect
PKI	Public Key Infrastructure
PP	Protection Profile
RAM	Random Access Memory
RPC	Remote Procedure Call
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Function Policy
SPD	Security Problem Definition
ST	Security Target

TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
VPN	Virtual Private Network

5 Overview

5.1 General

This Clause introduces the main concepts of ISO/IEC 15408. It identifies the concept "TOE", the target audience of ISO/IEC 15408, and the approach taken to present the material in the remainder of ISO/IEC 15408.

5.2 The TOE

ISO/IEC 15408 is flexible in what to evaluate and is therefore not tied to the boundaries of IT products as commonly understood. Therefore in the context of evaluation, ISO/IEC 15408 uses the term "TOE" (Target of Evaluation).

A TOE is defined as a set of software, firmware and/or hardware possibly accompanied by guidance.

While there are cases where a TOE consists of an IT product, this need not be the case. The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these.

As far as ISO/IEC 15408 is concerned, the precise relation between the TOE and any IT products is only important in one aspect: the evaluation of a TOE containing only part of an IT product should not be misrepresented as the evaluation of the entire IT product.

Examples of TOEs include:

- A software application;
- An operating system;
- A software application in combination with an operating system;
- A software application in combination with an operating system and a workstation;
- An operating system in combination with a workstation;
- A smart card integrated circuit;
- The cryptographic co-processor of a smart card integrated circuit;
- A Local Area Network including all terminals, servers, network equipment and software;
- A database application excluding the remote client software normally associated with that database application.

5.2.1 Different representations of the TOE

In ISO/IEC 15408, a TOE can occur in several representations, such as (for a software TOE):

- a list of files in a configuration management system;

- a single master copy, that has just been compiled;
- a box containing a CD-ROM and a manual, ready to be shipped to a customer;
- an installed and operational version.

All of these are considered to be a TOE: and wherever the term “TOE” is used in the remainder of ISO/IEC 15408, the context determines the representation that is meant.

5.2.2 Different configurations of the TOE

In general, IT products can be configured in many ways: installed in different ways, with different options enabled or disabled. As, during an ISO/IEC 15408 evaluation, it will be determined whether a TOE meets certain requirements, this flexibility in configuration may lead to problems, as all possible configurations of the TOE must meet the requirements. For these reasons, it is often the case that the guidance part of the TOE strongly constrains the possible configurations of the TOE. That is: the guidance of the TOE may be different from the general guidance of the IT product.

An example is an operating system IT product. This product can be configured in many ways (e.g. types of users, number of users, types of external connections allowed/disallowed, options enabled/disabled etc.).

If the same IT product is to be a TOE, and is evaluated against a reasonable set of requirements, the configuration should be much more tightly controlled, as many options (e.g. allow all types of external connections or the system administrator does not need to be authenticated) will lead to a TOE not meeting the requirements.

For this reason, there would normally be a difference between the guidance of the IT product (allowing many configurations) and the guidance of the TOE (allowing only one or only configurations that do not differ in security-relevant ways).

Note that if the guidance of the TOE still allows more than one configuration, these configurations are collectively called “the TOE” and each such configuration must meet the requirements levied on the TOE.

5.3 Target audience of ISO/IEC 15408

There are three groups with a general interest in evaluation of the security properties of TOEs: consumers, developers and evaluators. The criteria presented in ISO/IEC 15408 part 1 have been structured to support the needs of all three groups. They are all considered to be the principal users of ISO/IEC 15408. The three groups can benefit from the criteria as explained in the following paragraphs.

5.3.1 Consumers

ISO/IEC 15408 is written to ensure that evaluation fulfils the needs of the consumers as this is the fundamental purpose and justification for the evaluation process.

Consumers can use the results of evaluations to help decide whether a TOE fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Consumers can also use the evaluation results to compare different TOEs.

ISO/IEC 15408 gives consumers, especially in consumer groups and communities of interest, an implementation-independent structure, termed the Protection Profile (PP), in which to express their security requirements in an unambiguous manner.

5.3.2 Developers

ISO/IEC 15408 is intended to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the Security Target (ST). This ST may be based on one or

more PPs to show that the ST conforms to the security requirements from consumers as laid down in those PPs.

ISO/IEC 15408 can then be used to determine the responsibilities and actions to provide evidence that is necessary to support the evaluation of the TOE against these requirements. It also defines the content and presentation of that evidence.

5.3.3 Evaluators

ISO/IEC 15408 contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. ISO/IEC 15408 describes the set of general actions the evaluator is to carry out. Note that ISO/IEC 15408 does not specify procedures to be followed in carrying out those actions. More information on these procedures may be found in 5.5.

5.3.4 Others

While ISO/IEC 15408 is oriented towards specification and evaluation of the IT security properties of TOEs, it may also be useful as reference material to all parties with an interest in or responsibility for IT security. Some of the additional interest groups that can benefit from information contained in ISO/IEC 15408 are:

a) system custodians and system security officers responsible for determining and meeting organisational IT security policies and requirements;

b) auditors, both internal and external, responsible for assessing the adequacy of the security of an IT solution (which may consist of or contain a TOE);

c) security architects and designers responsible for the specification of security properties of IT products;

d) accreditors responsible for accepting an IT solution for use within a particular environment;

e) sponsors of evaluation responsible for requesting and supporting an evaluation; and

f) evaluation authorities responsible for the management and oversight of IT security evaluation programmes.

5.4 The different parts of ISO/IEC 15408

ISO/IEC 15408 is presented as a set of distinct but related parts as identified below. Terms used in the description of the parts are explained in Clause 6.

a) **Part 1, Introduction and general model** is the introduction to ISO/IEC 15408. It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation.

b) **Part 2, Security functional components** establishes a set of functional components that serve as standard templates upon which to base functional requirements for TOEs. ISO/IEC 15408-2 catalogues the set of functional components and organises them in families and classes.

c) **Part 3, Security assurance components** establishes a set of assurance components that serve as standard templates upon which to base assurance requirements for TOEs. ISO/IEC 15408-3 catalogues the set of assurance components and organises them into families and classes. ISO/IEC 15408-3 also defines evaluation criteria for PPs and STs and presents seven pre-defined assurance packages which are called the Evaluation Assurance Levels (EALs).

In support of the three parts of ISO/IEC 15408 listed above, other documents have been published. For example, ISO/IEC 18045 provides the methodology for IT security evaluation using ISO/IEC 15408 as a basis. It is anticipated that other documents will be published, including technical rationale material and guidance documents.

The following table presents, for the three key target audience groupings, how the parts of ISO/IEC 15408 will be of interest.

	Consumers	Developers	Evaluators
Part 1	Use for background information and are obliged to use for reference purposes. Guidance structure for PPs.	Use for background information and reference purposes. Are obliged to use for the development of security specifications for TOEs.	Are obliged to use for reference purposes and for guidance in the structure for PPs and STs.
Part 2	Use for guidance and reference when formulating statements of requirements for a TOE.	Are obliged to use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Are obliged to use for reference when interpreting statements of functional requirements.
Part 3	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use for reference when interpreting statements of assurance requirements.

Table 1 — Road map to the "Evaluation criteria for IT security"

5.5 Evaluation context

In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations to which the evaluation facilities and evaluators must conform.

ISO/IEC 15408 does not state requirements for the regulatory framework. However, consistency between the regulatory frameworks of different evaluation authorities will be necessary to achieve the goal of mutual recognition of the results of such evaluations.

A second way of achieving greater comparability between evaluation results is using a common methodology to achieve these results. For ISO/IEC 15408 this methodology is given in ISO/IEC 18045.

Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results may be submitted to a certification process.

The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval, which is normally publicly available. The certification process is a means of gaining greater consistency in the application of IT security criteria.

The evaluation schemes and certification processes are the responsibility of the evaluation authorities that run such schemes and processes and are outside the scope of ISO/IEC 15408.

6 General model

6.1 Introduction to the general model

This clause presents the general concepts used throughout ISO/IEC 15408, including the context in which the concepts are to be used and ISO/IEC 15408 approach for applying the concepts. ISO/IEC 15408-2 and ISO/IEC 15408-3, which are obliged to be consulted by users of this part of ISO/IEC 15408, expand on the use of these concepts and assume that the approach described is used. Further, for users of ISO/IEC 15408 who intend to perform evaluation activities ISO/IEC 18045 is applicable. This clause assumes some knowledge of IT security and does not propose to act as a tutorial in this area.

ISO/IEC 15408 discusses security using a set of security concepts and terminology. An understanding of these concepts and the terminology is a prerequisite to the effective use of ISO/IEC 15408. However, the concepts themselves are quite general and are not intended to restrict the class of IT security problems to which ISO/IEC 15408 is applicable.

6.2 Assets and countermeasures

Security is concerned with the protection of assets. Assets are entities that someone places value upon. Examples of assets include:

- contents of a file or a server;
- the authenticity of votes cast in an election;
- the availability of an electronic commerce process;
- the ability to use an expensive printer;
- access to a classified facility.

but given that value is highly subjective, almost anything can be an asset.

The environment(s) in which these assets are located is called the operational environment. Examples of (aspects of) operational environments are:

- the computer room of a bank;
- a computer network connected to the Internet;
- a LAN;
- a general office environment.

Many assets are in the form of information that is stored, processed and transmitted by IT products to meet requirements laid down by owners of the information. Information owners may require that availability, dissemination and modification of any such information are strictly controlled and that the assets are protected from threats by countermeasures. Figure 2 illustrates these high level concepts and relationships.

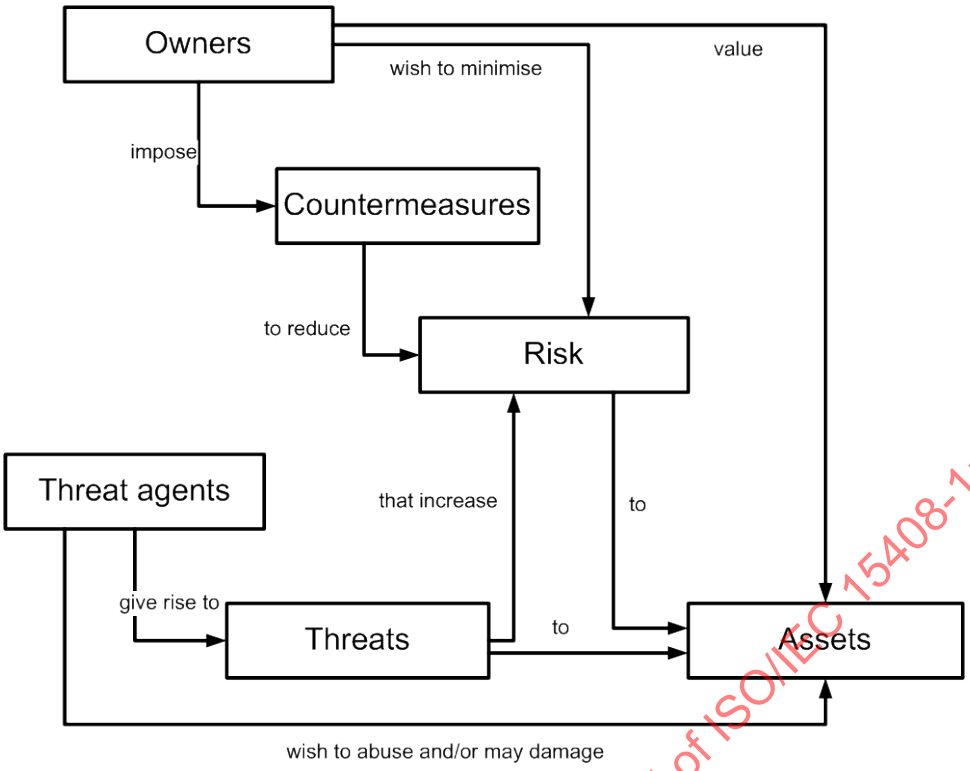

Figure 2 - Security concepts and relationships

Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner. Examples of threat agents include hackers, malicious users, non-malicious users (who sometimes make errors), computer processes and accidents.

The owners of the assets will perceive such threats as potential for impairment of the assets such that the value of the assets to the owners would be reduced. Security-specific impairment commonly includes, but is not limited to: loss of asset confidentiality, loss of asset integrity and loss of asset availability.

These threats therefore give rise to risks to the assets, based on the likelihood of a threat being realised and the impact on the assets when that threat is realised. Subsequently countermeasures are imposed to reduce the risks to assets. These countermeasures may consist of IT countermeasures (such as firewalls and smart cards) and non-IT countermeasures (such as guards and procedures). See also ISO/IEC 27001 and ISO/IEC 27002 for a more general discussion on security countermeasures (controls) and how to implement and manage them.

Owners of assets may be (held) responsible for those assets and therefore should be able to defend the decision to accept the risks of exposing the assets to the threats.

Two important elements in defending this decision are being able to demonstrate that:

- the countermeasures are *sufficient*: if the countermeasures do what they claim to do, the threats to the assets are countered;

- the countermeasures are *correct*: the countermeasures do what they claim to do.

Many owners of assets lack the knowledge, expertise or resources necessary to judge sufficiency and correctness of the countermeasures, and they may not wish to rely solely on the assertions of the developers of the countermeasures. These consumers may therefore choose to increase their confidence in the sufficiency and correctness of some or all of their countermeasures by ordering an evaluation of these countermeasures.

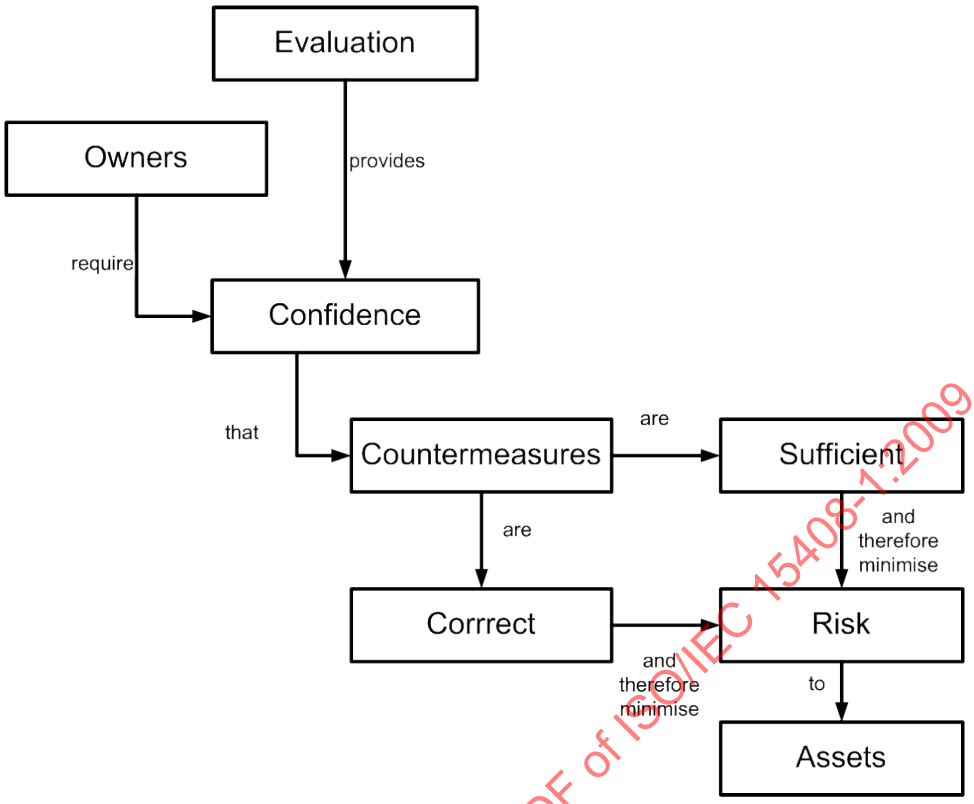

Figure 3 - Evaluation concepts and relationships

6.2.1 Sufficiency of the countermeasures

In an evaluation, sufficiency of the countermeasures is analysed through a construct called the Security Target. In this subclause a simplified view on this construct is provided: a more detailed and complete description may be found in Annex A.

The Security Target begins with describing the assets and the threats to those assets. The Security Target then describes the countermeasures (in the form of Security Objectives) and demonstrates that these countermeasures are sufficient to counter these threats: if the countermeasures do what they claim to do, the threats are countered.

The Security Target then divides these countermeasures in two groups:

a) the security objectives for the TOE: these describe the countermeasure(s) for which correctness will be determined in the evaluation;

b) the security objectives for the Operational Environment: these describe the countermeasures for which correctness will not be determined in the evaluation.

The reasons for this division are:

- ISO/IEC 15408 is only suitable for assessing the correctness of IT countermeasures. Therefore the non-IT countermeasures (e.g. human security guards, procedures) are always in the Operational Environment.
- Assessing correctness of countermeasures costs time and money, possibly making it infeasible to assess the correctness of all IT countermeasures.
- The correctness of some IT countermeasures may already have been assessed in another evaluation. It is therefore not cost-effective to assess this correctness again.

For the TOE (the IT countermeasures whose correctness will be assessed during the evaluation), the Security Target requires a further detailing of the security objectives for the TOE in Security Functional Requirements (SFRs). These SFRs are formulated in a standardised language (described in ISO/IEC 15408-2) to ensure exactness and facilitate comparability.

In summary, the Security Target demonstrates that:

- The SFRs meet the security objectives for the TOE;
- The security objectives for the TOE and the security objectives for the operational environment counter the threats;
- And therefore, the SFRs and the security objectives for the operational environment counter the threats.

From this it follows that a correct TOE (meeting the SFRs) in combination with a correct operational environment (meeting the security objectives for the operational environment) will counter the threats. In the next two subclauses correctness of the TOE and correctness of the operational environment are discussed separately.

6.2.2 Correctness of the TOE

A TOE may be incorrectly designed and implemented, and may therefore contain errors that lead to vulnerabilities. By exploiting these vulnerabilities, attackers may still damage and/or abuse the assets.

These vulnerabilities may arise from accidental errors made during development, poor design, intentional addition of malicious code, poor testing etc.

To determine correctness of the TOE, various activities can be performed such as:

- testing the TOE;
- examining various design representations of the TOE;
- examining the physical security of the development environment of the TOE.

The Security Target provides a structured description of these activities to determine correctness in the form of Security Assurance Requirements (SARs). These SARs are formulated in a standardised language (described in ISO/IEC 15408-3) to ensure exactness and facilitate comparability.

If the SARs are met, there exists assurance in the correctness of the TOE and the TOE is therefore less likely to contain vulnerabilities that can be exploited by attackers. The amount of assurance that exists in the correctness of the TOE is determined by the SARs themselves: a few “weak” SARs will lead to a little assurance, a lot of “strong” SARs will lead to a lot of assurance.

6.2.3 Correctness of the Operational Environment

The operational environment may also be incorrectly designed and implemented, and may therefore contain errors that lead to vulnerabilities. By exploiting these vulnerabilities, attackers may still damage and/or abuse the assets.

However, in ISO/IEC 15408, no assurance is obtained regarding the correctness of the operational environment. Or, in other words, the operational environment is not evaluated (see the next subclause).

As far as the evaluation is concerned, the operational environment is assumed to be a 100% correct instantiation of the security objectives for the operational environment.

This does not preclude a consumer of the TOE from using other methods to determine the correctness of his operational environment, such as:

- If, for an OS TOE, the security objectives for the operational environment state “The operational environment shall ensure that entities from an untrusted network (e.g. the Internet) can only access the TOE by ftp”, the consumer could select an evaluated firewall, and configure it to only allow ftp access to the TOE;

- If the security objectives for the operational environment state “The operational environment shall ensure that all administrative personnel will not behave maliciously”, the consumer could adapt his contracts with administrative personnel to include punitive sanctions for malicious behaviour, but this determination is not part of an ISO/IEC 15408 evaluation.

6.3 Evaluation

ISO/IEC 15408 recognises two types of evaluation: an ST/TOE evaluation, which is described below, and an evaluation of PPs, which is defined in ISO/IEC 15408-3. In many places, ISO/IEC 15408 uses the term evaluation (without qualifiers) to refer to an ST/TOE evaluation.

In ISO/IEC 15408 an ST/TOE evaluation proceeds in two steps:

a) An ST evaluation: where the sufficiency of the TOE and the operational environment are determined;

b) A TOE evaluation: where the correctness of the TOE is determined. As said earlier, the TOE evaluation does not assess correctness of the operational environment.

The ST evaluation is carried out by applying the Security Target evaluation criteria (which are defined in ISO/IEC 15408-3) to the Security Target. The precise method to apply the ASE criteria is determined by the evaluation methodology that is used.

The TOE evaluation is more complex. The principal inputs to a TOE evaluation are: the evaluation evidence, which includes the TOE and ST, but will usually also include input from the development environment, such as design documents or developer test results.

The TOE evaluation consists of applying the SARs (from the Security Target) to the evaluation evidence. The precise method to apply a specific SAR is determined by the evaluation methodology that is used.

How the results of applying the SARs are documented, and what reports need to be generated and in what detail, is determined by both the evaluation methodology that is used and the evaluation scheme under which the evaluation is carried out.

The result of the TOE evaluation process is either:

- A statement that not all SARs have been met and that therefore there is not the specified level of assurance that the TOE meets the SFRs as stated in the ST;

- A statement that all SARs have been met, and that therefore there is the specified level of assurance that the TOE meets the SFRs as stated in the ST.

The TOE evaluation may be carried out after TOE development has finished, or in parallel with TOE development.

The method of stating ST/TOE evaluation results is described in Clause 9. These results also identify the PP(s) and package(s) to which the TOE claims conformance, and these constructs are described in the next Clause.

7 Tailoring Security Requirements

7.1 Operations

ISO/IEC 15408 functional and assurance components may be used exactly as defined in ISO/IEC 15408-2 and ISO/IEC 15408-3, or they may be tailored through the use of permitted operations. When using

operations, the PP/ST author should be careful that the dependency needs of other requirements that depend on this requirement are satisfied. The permitted operations are selected from the following set:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

The assignment and selection operations are permitted only where specifically indicated in a component. Iteration and refinement are permitted for all components. The operations are described in more detail below.

The ISO/IEC 15408-2 Annexes provide the guidance on the valid completion of selections and assignments. This guidance provides normative instructions on how to complete operations, and those instructions shall be followed unless the PP/ST author justifies the deviation:

a) "None" is only available as a choice for the completion of a selection if explicitly provided.

   The lists provided for the completion of selections must be non-empty. If a "None" option is chosen, no additional selection options may be chosen. If "None" is not given as an option in a selection, it is permissible to combine the choices in a selection with "and"s and "or"s, unless the selection explicitly states "choose one of".

   Selection operations may be combined by iteration where needed. In this case, the applicability of the option chosen for each iteration should not overlap the subject of the other iterated selection, since they are intended to be exclusive.

b) For the completion of assignments, ISO/IEC 15408-2 Annexes shall be consulted in order to determine when "None" would be a valid completion.

7.1.1 The iteration operation

The iteration operation may be performed on every component. The PP/ST author performs an iteration operation by including multiple requirements based on the same component. Each iteration of a component shall be different from all other iterations of that component, which is realised by completing assignments and selections in a different way, or by applying refinements to it in a different way.

Different iterations should be uniquely identified to allow clear rationales and tracings to and from these requirements.

It is important to note that sometimes an iteration operation can be used with components where could also be possible to perform an assignment operation with a range or list of values instead of iterate them. In that case the author can select the most appropriate alternative, considering if there is a necessity of providing a whole rationale for the range of values or if it is necessary to have a separate one for each of them. The author should also keep in mind if individual traces are required for those values.

7.1.2 The assignment operation

An assignment operation occurs where a given component contains an element with a parameter that may be set by the PP/ST author. The parameter may be an unrestricted variable, or a rule that narrows the variable to a specific range of values.

Whenever an element in a PP contains an assignment, a PP author shall do one of four things:

a) leave the assignment uncompleted. The PP author could include FIA_AFL.1.2 "When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: list of actions]**." in the PP.

b) complete the assignment. As an example, the PP author could include FIA_AFL.1.2 “When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **prevent that external entity from binding to any subject in the future**.” in the PP.

c) narrow the assignment, to further limit the range of values that is allowed. As an example, the PP author could include FIA_AFL.1.1 “The TSF shall **detect when [assignment: positive integer between 4 and 9] unsuccessful authentication attempts occur ...”** in the PP.

d) transform the assignment to a selection, thereby narrowing the assignment. As an example, the PP author could include FIA_AFL.1.2 “When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[selection: prevent that user from binding to any subject in the future, notify the administrator]**.” in the PP.

Whenever an element in an ST contains an assignment, an ST author shall complete that assignment, as indicated in b) above. Options a), c) and d) are not allowed for STs.

The values chosen in options b), c) and d) shall conform to the indicated type required by the assignment.

When an assignment is to be completed with a set (e.g. subjects), one may list a set of subjects, but also some description of the set from which the elements of the set can be derived such as:

- all subjects
- all subjects of type X
- all subjects except subject a
- as long as it is clear which subjects are meant.

7.1.3 The selection operation

The selection operation occurs where a given component contains an element where a choice from several items has to be made by the PP/ST author.

Whenever an element in a PP contains a selection, the PP author may do one of three things:

a) leave the selection uncompleted.

b) complete the selection by choosing one or more items.

c) restrict the selection by removing some of the choices, but leaving two or more.

Whenever an element in an ST contains a selection, an ST author shall complete that selection, as indicated in b) above. Options a) and c) are not allowed for STs.

The item or items chosen in b) and c) shall be taken from the items provided in the selection.

7.1.4 The refinement operation

The refinement operation can be performed on every requirement. The PP/ST author performs a refinement by altering that requirement. The first rule for a refinement is that a TOE meeting the refined requirement also meets the unrefined requirement in the context of the PP/ST (i.e. a refined requirement must be “stricter” than the original requirement). If a refinement does not meet this rule, the resulting refined requirement is considered to be an extended requirement and shall be treated as such.

The only exception to this rule is that a PP/ST author is allowed to refine a SFR to apply to some but not all subjects, objects, operations, security attributes and/or external entities.

However, this exception does not apply to refining SFRs that are taken from PPs that compliance is being claimed to; these SFRs may not be refined to apply to fewer subjects, objects, operations, security attributes and/or external entities than the SFR in the PP.

The second rule for a refinement is that the refinement shall be related to the original component.

A special case of refinement is an editorial refinement, where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar, or to make it more understandable to the reader. This change is not allowed to modify the meaning of the requirement in any way.

7.2 Dependencies between components

Dependencies may exist between components. Dependencies arise when a component is not self sufficient and relies upon the presence of another component to provide security functionality or assurance.

The functional components in ISO/IEC 15408-2 typically have dependencies on other functional components as do some of the assurance components in ISO/IEC 15408-3 which may have dependencies on other ISO/IEC 15408-3 components. ISO/IEC 15408-2 dependencies on ISO/IEC 15408-3 components may also be defined. However, this does not preclude extended functional components having dependencies on assurance components or vice versa.

Component dependency descriptions are determined by consulting ISO/IEC 15408-2 and ISO/IEC 15408-3 component definitions. In order to ensure completeness of the TOE security requirements, dependencies should be satisfied when requirements based on components with dependencies are incorporated into PPs and STs. Dependencies should also be considered when constructing packages.

In other words: if component A has a dependency on component B, this means that whenever a PP/ST contains a security requirement based on component A, the PP/ST shall also contain one of :

a) a security requirement based on component B, or

b) a security requirement based on a component that is hierarchically higher than B, or

c) a justification why the PP/ST does not contain a security requirement based on component B.

In cases a) and b), when a security requirement is included because of a dependency, it may be necessary to complete operations (assignment, iteration, refinement, selection) on that security requirement in a particular manner to make sure that it actually satisfies the dependency.

In case c), the justification that a security requirement is not included should address either:

- why the dependency is not necessary or useful, or
- that the dependency has been addressed by the operational environment of the TOE, in which case the justification should describe how the security objectives for the operational environment address this dependency, or
- that the dependency has been addressed by the other SFRs in some other manner (extended SFRs, combinations of SFRs etc.)

7.3 Extended components

In ISO/IEC 15408 it is mandatory to base requirements on components from ISO/IEC 15408-2 or ISO/IEC 15408-3 with two exceptions:

a) there are security objectives for the TOE that can not be translated to Part 2 SFRs, or there are third party requirements (e.g., laws, standards) that can not be translated to Part 3 SARs (e.g. regarding evaluation of cryptography);

b) a security objective can be translated, but only with great difficulty and/or complexity based on components in ISO/IEC 15408-2 and/or ISO/IEC 15408-3.

In both cases the PP/ST author is required to define his own components. These newly defined components are called extended components. A precisely defined extended component is needed to provide context and meaning to the extended SFRs and SARs based on that component.

After the new components have been defined correctly, the PP/ST author can then base one or more SFRs or SARs on these newly defined extended components and use them in the same way as the other SFRs and SARs. From this point on, there is no further distinction between SARs and SFRs based on ISO/IEC 15408 and SARs and SFRs based on extended components. Refer to ISO/IEC 15408-3 Extended components definition (APE_ECD) and Extended components definition (ASE_ECD) for further requirements on extended components.

8 Protection Profiles and Packages

8.1 Introduction

To allow consumer groups and communities of interest to express their security needs, and to facilitate writing STs, this part of ISO/IEC 15408 provides two special constructs: packages and Protection Profiles (PPs). In the following two subclauses these constructs are described in more detail, followed by a subclause on how these constructs can be used.

8.2 Packages

A package is a named set of security requirements. A package is either

- a functional package, containing only SFRs, or
- an assurance package, containing only SARs.

Mixed packages containing both SFRs and SARs are not allowed.

A package can be defined by any party and is intended to be re-usable. To this goal it should contain requirements that are useful and effective in combination. Packages can be used in the construction of larger packages, PPs and STs. At present there are no criteria for the evaluation of packages, therefore any set of SFRs or SARs can be a package.

Examples of assurance packages are the evaluation assurance levels (EALs) that are defined in ISO/IEC 15408-3. At the time of writing there are no functional packages for this version of ISO/IEC 15408.

8.3 Protection Profiles

Whereas an ST always describes a specific TOE (e.g. the MinuteGap v18.5 Firewall), a PP is intended to describe a TOE type (e.g. firewalls). The same PP may therefore be used as a template for many different STs to be used in different evaluations. A detailed description of PPs is given in Annex B.

In general an ST describes requirements for a TOE and is written by the developer of that TOE, while a PP describes the general requirements for a TOE type, and is therefore typically written by:

- A user community seeking to come to a consensus on the requirements for a given TOE type;
- A developer of a TOE, or a group of developers of similar TOEs wishing to establish a minimum baseline for that type of TOE;
- A government or large corporation specifying its requirements as part of its acquisition process.

The PP determines the allowed type of conformance of the ST to the PP. That is, the PP states (in the PP conformance statement, see B.5) what the allowed types of conformance for the ST are:

- if the PP states that strict conformance is required, the ST shall conform to the PP in a strict manner;
- if the PP states that demonstrable conformance is required, the ST shall conform to the PP in a strict or demonstrable manner.

Restating this in other words, an ST is only allowed to conform in a PP in a demonstrable manner, if the PP explicitly allows this.

If an ST claims conformance to multiple PPs, it shall conform (as described above) to each PP in the manner ordained by that PP. This may mean that the ST conforms strictly to some PPs and demonstrably to other PPs.

Note that either the ST conforms to the PP in question or it does not. ISO/IEC 15408 does not recognise "partial" conformance. It is therefore the responsibility of the PP author to ensure the PP is not overly onerous, prohibiting PP/ST authors in claiming conformance to the PP.

An ST is equivalent or more restrictive than a PP if:

- all TOEs that meet the ST also meet the PP, and
- all operational environments that meet the PP also meet the ST.

or, informally, the ST shall levy the same or more, restrictions on the TOE and the same or less restrictions on the operational environment of the TOE.

This general statement can be made more specific for various subclauses of the ST:

a) **Security problem definition**: The conformance rationale in the ST shall demonstrate that the security problem definition in the ST is equivalent (or more restrictive) than the security problem definition in the PP. This means that:

   - all TOEs that would meet the security problem definition in the ST also meet the security problem definition in the PP;
   - all operational environments that would meet the security problem definition in the PP would also meet the security problem definition in the ST.

b) **Security objectives**: The conformance rationale in the ST shall demonstrate that the security objectives in the ST is equivalent (or more restrictive) than the security objectives in the PP. This means that:

   - all TOEs that would meet the security objectives for the TOE in the ST also meet the security objectives for the TOE in the PP;
   - all operational environments that would meet the security objectives for the operational environment in the PP would also meet the security objectives for the operational environment in the ST.

If strict conformance for protection profiles is specified then the following requirements apply:

a) **Security problem definition**:

   - The ST shall contain the security problem definition of the PP and may specify additional threats and OSPs; it shall contain all assumptions as defined in the PP, with two possible exceptions as explained in the next two bullets;
   - an assumption (or a part of an assumption) specified in the PP may be omitted from the ST, if all security objectives for the operational environment defined in the PP addressing this assumption (or this part of an assumption) are replaced by security objectives for the TOE in the ST;

- a new assumption may be added in the ST to the set of assumptions defined in the PP, if this new assumption does not mitigate a threat (or part of a threat) meant to be addressed by security objectives for the TOE in the PP and if this assumption doesn't fulfil an OSP (or a part of an OSP) meant to be addressed by security objectives for the TOE in the PP;

b) **Security objectives**: The ST:

- shall contain all security objectives for the TOE of the PP but may specify additional security objectives for the TOE;
- shall contain all security objectives for the operational environment as defined in the PP with two exceptions as explained in the next two bullet points;
- may specify that certain objectives for the operational environment in the PP are security objectives for the TOE in the ST. This is called re-assigning a security objective. If a security objective is re-assigned to the TOE the security objectives justification has to make clear which assumption or part of the assumption may not be necessary any more;
- may specify additional objectives for the operational environment, if these new objectives do not mitigate a threat (or part of a threat) meant to be addressed by security objectives of the TOE in the PP and if these new objectives do not fulfil an OSP (or a part of an OSP) meant to be addressed by security objectives of the TOE in the PP

c) **Security requirements**: The ST shall contain all SFRs and SARs in the PP, but may claim additional or hierarchically stronger SFRs and SARs. The completion of operations in the ST must be consistent with that in the PP; either the same completion will be used in the ST as that in the PP or one that makes the requirement more restrictive (the rules of refinement apply).

If demonstrable conformance for protection profiles is specified then the following requirements apply:

- the ST shall contain a rationale on why the ST is considered to be “equivalent or more restrictive” than the PP.
- Demonstrable conformance allows a PP author to describe a common security problem to be solved and provide generic guidelines to the requirements necessary for its resolution, in the knowledge that there is likely to be more than one way of specifying a resolution.

PP evaluation is optional. Evaluation is performed by applying the APE criteria to them as listed in ISO/IEC 15408-3. The goal of such an evaluation is to demonstrate that the PP is complete, consistent, and technically sound and suitable for use as a template on which to build another PP or an ST.

Basing a PP/ST on an evaluated PP has two advantages:

- There is much less risk that there are errors, ambiguities or gaps in the PP. If any problems with a PP (that would have been caught by evaluating that PP) are found during the writing or evaluation of the new ST, significant time may elapse before the PP is corrected.
- Evaluation of the new PP/ST may often re-use evaluation results of the evaluated PP, resulting in less effort for evaluating the new PP/ST.

8.4 Using PPs and packages

If an ST claims to be conformant to one or more packages and/or Protection Profiles, the evaluation of that ST will (among other properties of that ST) demonstrate that the ST actually conforms to these packages and/or PPs that they claim conformance to. Details of this determination of conformance can be found in Annex A.

This allows the following process:

a) An organisation seeking to acquire a particular type of IT security product develops their security needs into a PP, then has this evaluated and publishes it;

b) A developer takes this PP, writes an ST that claims conformance to the PP and has this ST evaluated;

c) The developer then builds a TOE (or uses an existing one) and has this evaluated against the ST.

The result is that the developer can prove that his TOE is conformant to the security needs of the organisation: the organisation can therefore acquire that TOE. A similar line of reasoning applies to packages.

8.5 Using Multiple Protection Profiles

ISO/IEC 15408 also allows PPs to conform to other PPs, allowing chains of PPs to be constructed, each based on the previous one(s).

For instance, one could take a PP for an Integrated Circuit and a PP for a Smart Card OS, and use these to construct a Smart Card PP (IC and OS) that claims conformance to the other two. One could then write a PP on Smart Cards for Public Transport based on the Smart Card PP and a PP on Applet Loading. Finally, a developer could then construct an ST based on this Smart Cards for Public Transport PP.

9 Evaluation results

9.1 Introduction

This clause presents the expected results from PP and ST/TOE evaluations performed according to ISO/IEC 18045.

PP evaluations lead to catalogues of evaluated PPs.

An ST evaluation leads to intermediate results that are used in the frame of a TOE evaluation.

ST/TOE evaluations lead to catalogues of evaluated TOEs. In many cases these catalogues will refer to the IT products that the TOEs are derived from rather than the specific TOE. Therefore, the existence of an IT product in a catalogue should not be construed as meaning that the whole IT product has been evaluated; instead the actual extent of the ST/TOE evaluation is defined by the ST. Refer to the bibliography for examples of such catalogues.

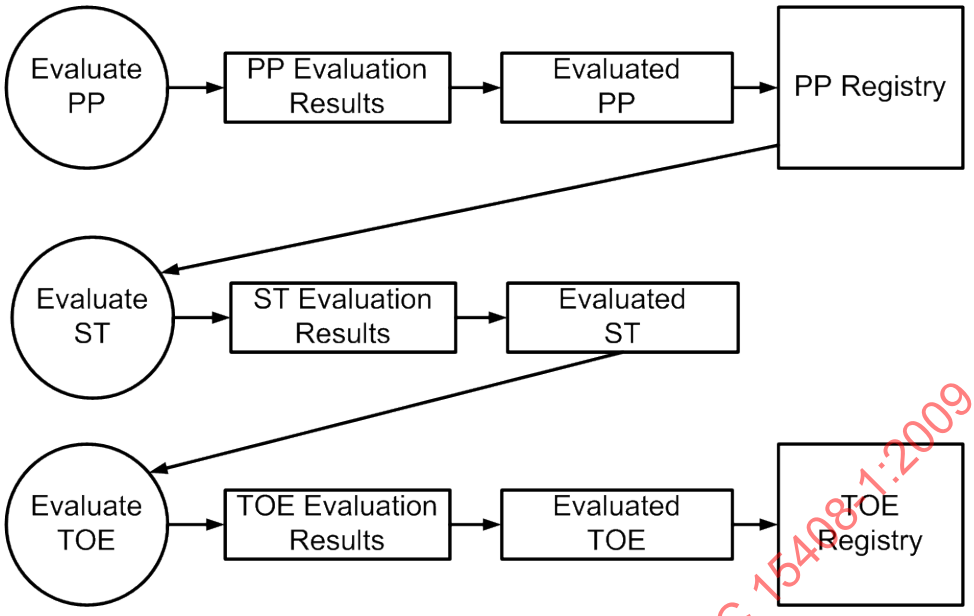

Figure 4 - Evaluation results

STs may be based on packages, evaluated PPs or non-evaluated PPs - however this is not mandatory, as STs do not have to be based on anything at all.

Evaluation should lead to objective and repeatable results that can be cited as evidence, even if there is no absolute objective scale for representing the results of a security evaluation. The existence of a set of evaluation criteria is a necessary pre-condition for evaluation to lead to a meaningful result and provides a technical basis for mutual recognition of evaluation results between evaluation authorities.

An evaluation result represents the findings of a specific type of investigation of the security properties of a TOE. Such a result does not automatically guarantee fitness for use in any particular application environment. The decision to accept a TOE for use in a specific application environment is based on consideration of many security issues including the evaluation findings.

9.2 Results of a PP evaluation

ISO/IEC 15408-3 contains the evaluation criteria that an evaluator is obliged to consult in order to state whether a PP is complete, consistent, and technically sound and hence suitable for use in developing an ST.

The results of the evaluation shall also include a “Conformance Claim” (see 9.4)).

9.3 Results of an ST/TOE evaluation

ISO/IEC 15408-3 contains the evaluation criteria that an evaluator is obliged to consult in order to determine whether sufficient assurance exists that the TOE satisfies the SFRs in the ST. Evaluation of the TOE shall therefore result in a pass/fail statement for the ST. If both the ST and the TOE evaluation have resulted in a pass statement, the underlying product is eligible for inclusion in a registry. The results of evaluation shall also include a “Conformance Claim” as defined in the next subclause.

It may be the case that the evaluation results are subsequently used in a certification process, but this certification process is outside the scope of ISO/IEC 15408.

9.4 Conformance claim

The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains an ISO/IEC 15408 conformance claim that:

a) describes the version of ISO/IEC 15408 to which the PP or ST claims conformance.

b) describes the conformance to ISO/IEC 15408-2 (security functional requirements) as either:

- **ISO/IEC 15408-2 conformant** - A PP or ST is ISO/IEC 15408-2 conformant if all SFRs in that PP or ST are based only upon functional components in ISO/IEC 15408-2, or
- **ISO/IEC 15408-2 extended** - A PP or ST is ISO/IEC 15408-2 extended if at least one SFR in that PP or ST is not based upon functional components in ISO/IEC 15408-2.

c) describes the conformance to ISO/IEC 15408-3 (security assurance requirements) as either:

- **ISO/IEC 15408-3 conformant** - A PP or ST is ISO/IEC 15408-3 conformant if all SARs in that PP or ST are based only upon assurance components in ISO/IEC 15408-3, or
- **ISO/IEC 15408-3 extended** - A PP or ST is ISO/IEC 15408-3 extended if at least one SAR in that PP or ST is not based upon assurance components in ISO/IEC 15408-3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- *Package name Conformant* - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- *Package name Augmented* - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. ISO/IEC 15408-2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

a) *PP Conformant* - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.

b) *Conformance Statement* (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex B.

9.5 Use of ST/TOE evaluation results

Once an ST and a TOE have been evaluated, asset owners can have the assurance (as defined in the ST) that the TOE, together with the operational environment, counters the threats. The evaluation results may be used by the asset owner in deciding whether to accept the risk of exposing the assets to the threats.

However, the asset owner should carefully check whether:

a) the Security Problem Definition in the ST matches the security problem of the asset owner;

b) the Operational Environment of the asset owner conforms (or can be made to conform) to the security objectives for the Operational Environment described in the ST.

If either of these is not the case, the TOE may not be suitable for the purposes of the asset owner.

Additionally, once an evaluated TOE is in operation, it is still possible that previously unknown errors or vulnerabilities in the TOE may surface. In that case, the developer may correct the TOE (to repair the vulnerabilities) or change the ST to exclude the vulnerabilities from the scope of the evaluation. In either case, the old evaluation results may no longer be valid.

If it is deemed necessary that confidence is regained, re-evaluation is needed. ISO/IEC 15408 may be used for this re-evaluation, but detailed procedures for re-evaluation are outside the scope of this part of ISO/IEC 15408.

Annex A
(informative)

Specification of Security Targets

A.1 Goal and structure of this Annex

The goal of this annex is to explain the Security Target (ST) concept. This annex does not define the ASE criteria; this definition can be found in ISO/IEC 15408-3 and is supported by the documents given in the bibliography.

This annex consists of four major parts:

a) *What an ST must contain*. This is summarised in A.2, and described in more detail in A.4 - A.10. These subclauses describe the mandatory contents of the ST, the interrelationships between these contents, and provide examples.

b) *How an ST should be used*. This is summarised in A.3, and described in more detail in A.11. These subclauses describe how an ST should be used, and some of the questions that can be answered with an ST.

c) *Low Assurance STs*. Low Assurance STs are STs with reduced content. They are described in detail in A.12.

d) *Claiming compliance with standards*. A.13 describes how an ST writer can claim that the TOE meets a particular standard.

A.2 Mandatory contents of an ST

Figure A.1 portrays the mandatory contents of an ST that are given in ISO/IEC 15408-3. Figure A.1 may also be used as a structural outline of the ST, though alternative structures are allowed. For instance, if the security requirements rationale is particularly bulky, it could be included in an appendix of the ST instead of in the security requirements subclause. The separate subclauses of an ST and the contents of those subclauses are briefly summarised below and explained in much more detail in A.4 to A.10. An ST normally contains:

a) *an ST introduction* containing three narrative descriptions of the TOE on different levels of abstraction;

b) *a conformance claim*, showing whether the ST claims conformance to any PPs and/or packages, and if so, to which PPs and/or packages;

c) *a security problem definition*, showing threats, OSPs and assumptions;

d) *security objectives*, showing how the solution to the security problem is divided between security objectives for the TOE and security objectives for the operational environment of the TOE;

e) *extended components definition* (optional), where new components (i.e. those not included in ISO/IEC 15408-2 or ISO/IEC 15408-3) may be defined. These new components are needed to define extended functional and extended assurance requirements;

f) *security requirements*, where a translation of the security objectives for the TOE into a standardised language is provided. This standardised language is in the form of SFRs. Additionally this subclause defines the SARs;

g) *a TOE summary specification*, showing how the SFRs are implemented in the TOE.

There also exists low assurance STs which have reduced contents; these are described in detail in A.12. All other parts of this Annex assume an ST with full contents.

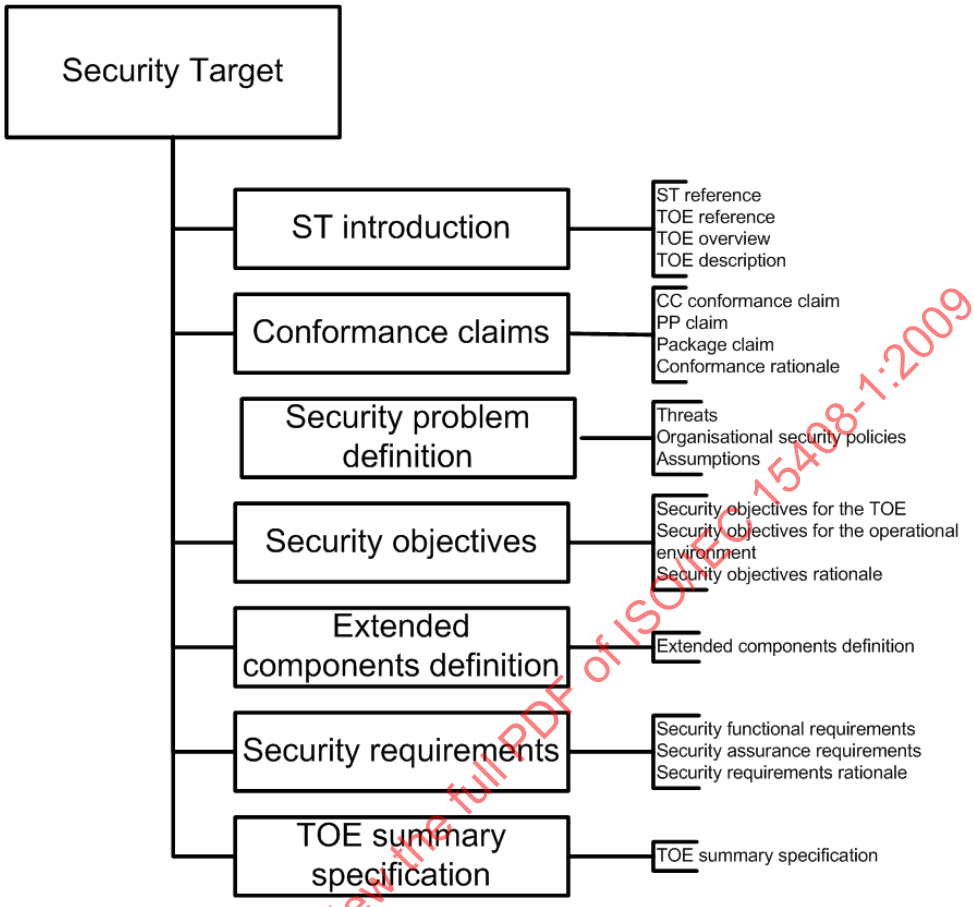

Figure A.1 - Security Target contents

A.3 Using an ST

A.3.1 How an ST should be used

A typical ST fulfils two roles:

- Before and during the evaluation, the ST specifies “what is to be evaluated”. In this role, the ST serves as a basis for agreement between the developer and the evaluator on the exact security properties of the TOE and the exact scope of the evaluation. Technical correctness and completeness are major issues for this role. A.7 describes how the ST should be used in this role.

- After the evaluation, the ST specifies “what was evaluated”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST describes the exact security properties of the TOE in an abstract manner, and the potential consumer can rely on this description because the TOE has been evaluated to meet the ST. Ease of use and understandability are major issues for this role. A.11 describes how the ST should be used in this role.

A.3.2 How an ST should not be used

Two roles (among many) that an ST should not fulfil are:

- *a detailed specification*: An ST is designed to be a security specification on a relatively high level of abstraction. An ST should, in general, not contain detailed protocol specifications, detailed descriptions of algorithms and/or mechanisms, long description of detailed operations etc.

- *a complete specification*: An ST is designed to be a security specification and not a general specification. Unless security-relevant, properties such as interoperability, physical size and weight, required voltage etc. should not be part of an ST. This means that in general an ST may be a part of a complete specification, but not a complete specification itself.

A.4 ST Introduction (ASE_INT)

The ST introduction describes the TOE in a narrative way on three levels of abstraction:

a) the ST reference and the TOE reference, which provide identification material for the ST and the TOE that the ST refers to;

b) the TOE overview, which briefly describes the TOE;

c) the TOE description, which describes the TOE in more detail.

A.4.1 ST reference and TOE reference

An ST contains a clear ST reference that identifies that particular ST. A typical ST reference consists of title, version, authors and publication date. An example of an ST reference is “MauveRAM Database ST, version 1.3, MauveCorp Specification Team, 11 October 2002”.

An ST also contains a TOE reference that identifies the TOE that claims conformance to the ST. A typical TOE reference consists of developer name, TOE name and TOE version number. An example of a TOE reference is “MauveCorp MauveRAM Database v2.11”. As a single TOE may be evaluated multiple times, for instance by different consumers of that TOE, and therefore have multiple STs, this reference is not necessarily unique.

If the TOE is constructed from one or more well-known products, it is allowed to reflect this in the TOE reference, by referring to the product name(s). However, this should not be used to mislead consumers: situations where major parts or security functionalities were not considered in the evaluation, yet the TOE reference does not reflect this are not allowed.

The ST reference and the TOE reference facilitate indexing and referencing the ST and TOE and their inclusion in summaries of lists of evaluated TOEs/Products.

A.4.2 TOE overview

The TOE overview is aimed at potential consumers of a TOE who are looking through lists of evaluated TOEs/Products to find TOEs that may meet their security needs, and are supported by their hardware, software and firmware. The typical length of a TOE overview is several paragraphs.

To this end, the TOE overview briefly describes the usage of the TOE and its major security features, identifies the TOE type and identifies any major non-TOE hardware/software/firmware required by the TOE.

A.4.2.1 Usage and major security features of a TOE

The description of the usage and major security features of the TOE is intended to give a very general idea of what the TOE is capable of in terms of security, and what it can be used for in a security context. This subclause should be written for (potential) TOE consumers, describing TOE usage and major security features in terms of business operations, using language that TOE consumers understand.

An example of this is “The MauveCorp MauveRAM Database v2.11 is a multi-user database intended to be used in a networked environment. It allows 1024 users to be active simultaneously. It allows password/token and biometric authentication, protects against accidental data corruption, and can roll-back ten thousand transactions. Its audit features are highly configurable, so as to allow detailed audit to be performed for some users and transactions, while protecting the privacy of other users and transactions.”

A.4.2.2 TOE type

The TOE overview identifies the general type of TOE, such as: firewall, VPN-firewall, smart card, crypto-modem, intranet, web server, database, web server and database, LAN, LAN with web server and database, etc.

It may be the case that the TOE is not of a readily available type, in which case “none” would be acceptable.

In some cases, a TOE type can mislead consumers. Examples include:

- certain functionality can be expected of the TOE because of its TOE type, but the TOE does not have this functionality. Examples include:
  - an ATM-card type TOE, which does not support any identification/authentication functionality;
  - a firewall type TOE, which does not support protocols that are almost universally used;
  - a PKI-type TOE, which has no certificate revocation functionality.
- the TOE can be expected to operate in certain operational environments because of its TOE type, but it cannot do so. Examples include:
  - a PC-operating system type TOE, which is unable to function securely unless the PC has no network connection, floppy drive, and CD/DVD-player;
  - a firewall, which is unable to function securely unless all users that can connect through that firewall are benign.

A.4.2.3 Required non-TOE hardware/software/firmware

While some TOEs do not rely upon other IT, many TOEs (notably software TOEs) rely on additional, non-TOE, hardware, software and/or firmware. In the latter case, the TOE overview is required to identify such non-TOE hardware,software and/or firmware . A complete and fully detailed identification of the additional hardware, software and/or firmware is not necessary, but the identification should be complete and detailed enough for potential consumers to determine the major hardware,software and/or firmware needed to use the TOE.

Example hardware/software/firmware identifications are:

- a standard PC with a 1GHz or faster processor and 512MB or more RAM, running version 3.0 Update 6b, c, or 7, or version 4.0 of the Yaiza operating system;
- a standard PC with a 1GHz or faster version processor and 512MB or more RAM, running version 3.0 Update 6d of the Yaiza operating system and the WonderMagic 1.0 Graphics card with the 1.0 WM Driver Set;
- a standard PC with version 3.0 of the Yaiza OS (or higher);
- a CleverCard SB2067 integrated circuit;
- a CleverCard SB2067 integrated circuit running v2.0 of the QuickOS smart card operating system;
- the December 2002 installation of the LAN of the Director-General's Office of the Department of Traffic.

A.4.3 TOE description

A TOE description is a narrative description of the TOE, likely to run to several pages. The TOE description should provide evaluators and potential consumers with a general understanding of the security capabilities of the TOE, in more detail than was provided in the TOE overview. The TOE description may also be used to describe the wider application context into which the TOE will fit.

The TOE description discusses the physical scope of the TOE: a list of all hardware, firmware, software and guidance parts that constitute the TOE. This list should be described at a level of detail that is sufficient to give the reader a general understanding of those parts.

The TOE description should also discuss the logical scope of the TOE: the logical security features offered by the TOE at a level of detail that is sufficient to give the reader a general understanding of those features. This description is expected to be in more detail than the major security features described in the TOE overview.

An important property of the physical and logical scopes is that they describe the TOE in such a way that there remains no doubt on whether a certain part or feature is in the TOE or whether this part or feature is outside the TOE. This is especially important when the TOE is intertwined with and cannot be easily separated from non-TOE entities.

Examples where the TOE is intertwined with non-TOE entities are:

- the TOE is a cryptographic co-processor of a smart card IC, instead of the entire IC;
- the TOE is a smart card IC, except for the cryptographic processor;
- the TOE is the Network Address Translation part of the MinuteGap Firewall v18.5.

A.5 Conformance claims (ASE_CCL)

This subclause of an ST describes how the ST conforms with:

- Part 2 and Part 3 of this International Standard;
- Protection Profiles (if any);
- Packages (if any).

The description of how the ST conforms to ISO/IEC 15408 consists of two items: the version of ISO/IEC 15408 that is used and whether the ST contains extended security requirements or not (see A.8).

The description of conformance of the ST to Protection Profiles means that the ST lists the packages that conformance is being claimed to. For an explanation of this, see 9.4.

The description of conformance of the ST to packages means that the ST lists the packages that conformance is being claimed to. For an explanation of this, see 9.4.

A.6 Security problem definition (ASE_SPD)

A.6.1 Introduction

The security problem definition defines the security problem that is to be addressed. The security problem definition is, as far as ISO/IEC 15408 is concerned, axiomatic. That is, the process of deriving the security problem definition falls outside the scope of ISO/IEC 15408.

However, it should be noted that the usefulness of the results of an evaluation strongly depends on the ST, and the usefulness of the ST strongly depends on the quality of the security problem definition. It is therefore

often worthwhile to spend significant resources and use well-defined processes and analyses to derive a good security problem definition.

Note that according to ISO/IEC 15408-3 it is not mandatory to have statements in all subclauses, an ST with threats does not need to have OSPs and vice versa. Also, any ST may omit assumptions.

Also note that where the TOE is physically distributed, it may be better to discuss the relevant threats, OSPs and assumptions separately for distinct domains of the TOE operational environment.

A.6.2 Threats

This subclause of the security problem definition shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

A threat consists of an adverse action performed by a threat agent on an asset.

Adverse actions are actions performed by a threat agent on an asset. These actions influence one or more properties of an asset from which that asset derives its value.

Threat agents may be described as individual entities, but in some cases it may be better to describe them as types of entities, groups of entities etc.

Examples of threat agents are hackers, users, computer processes, and accidents. Threat agents may be further described by aspects such as expertise, resources, opportunity and motivation.

Examples of threats are:

- a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network;
- a worm seriously degrading the performance of a wide-area network;
- a system administrator violating user privacy;
- someone on the Internet listening in on confidential electronic communication.

A.6.3 Organisational security policies (OSPs)

This subclause of the security problem definition shows the OSPs that are to be enforced by the TOE, its operational environment, or a combination of the two.

OSPs are security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment. OSPs may be laid down by an organisation controlling the operational environment of the TOE, or they may be laid down by legislative or regulatory bodies. OSPs can apply to the TOE and/or the operational environment of the TOE.

Examples of OSPs are:

- All products that are used by the Government must conform to the National Standard for password generation and encryption;
- Only users with System Administrator privilege and clearance of Department Secret shall be allowed to manage the Department Fileserver.

A.6.4 Assumptions

This subclause of the security problem definition shows the assumptions that are made on the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security

functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment.

Examples of assumptions are:

- Assumptions on physical aspects of the operational environment:
  - It is assumed that the TOE will be placed in a room that is designed to minimise electromagnetic emanations;
  - It is assumed that the administrator consoles of the TOE will be placed in a restricted access area.
- Assumptions on personnel aspects of the operational environment:
  - It is assumed that users of the TOE will be trained sufficiently in order to operate the TOE;
  - It is assumed that users of the TOE are approved for information that is classified as National Secret;
  - It is assumed that users of the TOE will not write down their passwords.
- Assumptions on connectivity aspects of the operational environment:
  - It is assumed that a PC workstation with at least 10GB of disk space is available to run the TOE on;
  - It is assumed that the TOE is the only non-OS application running on this workstation;
  - It is assumed that the TOE will not be connected to an untrusted network.

Note that during the evaluation these assumptions are considered to be true: they are not tested in any way. For these reasons, assumptions can only be made on the operational environment. Assumptions can never be made on the behaviour of the TOE because an evaluation consists of evaluating assertions made about the TOE and not by assuming that assertions on the TOE are true.

A.7 Security objectives (ASE_OBJ)

The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition. The role of the security objectives is threefold:

- provide a high-level, natural language solution of the problem;
- divide this solution into two part wise solutions, that reflect that different entities each have to address a part of the problem;
- demonstrate that these part wise solutions form a complete solution to the problem.

A.7.1 High-level solution

The security objectives consist of a set of short and clear statements without overly much detail that together form a high-level solution to the security problem. The level of abstraction of the security objectives aims at being clear and understandable to knowledgeable potential consumers of the TOE. The security objectives are in natural language.

A.7.2 Part wise solutions

In an ST the high-level security solution, as described by the security objectives, is divided into two part wise solutions. These part wise solutions are called the security objectives for the TOE and the security objectives for the operational environment. This reflects that these part wise solutions are to be provided by two different entities: the TOE, and the operational environment.

A.7.2.1 Security objectives for the TOE

The TOE provides security functionality to solve a certain part of the problem defined by the security problem definition. This part wise solution is called the security objectives for the TOE and consists of a set of objectives that the TOE should achieve in order to solve its part of the problem.

Examples of security objectives for the TOE are:

- The TOE shall keep confidential the content of all files transmitted between it and a Server;
- The TOE shall identify and authenticate all users before allowing them access to the Transmission Service provided by the TOE;
- The TOE shall restrict user access to data according to the Data Access policy described in Annex 3 of the ST.

If the TOE is physically distributed, it may be better to subdivide the ST subclause containing the security objectives for the TOE into several sub-subclauses to reflect this.

A.7.2.2 Security objectives for the operational environment

The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). This part wise solution is called the security objectives for the operational environment and consists of a set of statements describing the goals that the operational environment should achieve.

Examples of security objectives for the operational environment are:

- The operational environment shall provide a workstation with the OS Inux version 3.01b to execute the TOE on;
- The operational environment shall ensure that all human TOE users receive appropriate training before allowing them to work with the TOE;
- The operational environment of the TOE shall restrict physical access to the TOE to administrative personnel and maintenance personnel accompanied by administrative personnel;
- The operational environment shall ensure the confidentiality of the audit logs generated by the TOE before sending them to the central Audit Server.

If the operational environment of the TOE consists of multiple sites, each with different properties, it may be better to subdivide the ST subclause containing the security objectives for the operational environment into several sub-subclauses to reflect this.

A.7.3 Relation between security objectives and the security problem definition

The ST also contains a security objectives rationale containing two subclauses:

- a tracing that shows which security objectives address which threats, OSPs and assumptions;
- a set of justifications that shows that all threats, OSPs, and assumptions are effectively addressed by the security objectives.

A.7.3.1 Tracing between security objectives and the security problem definition

The tracing shows how the security objectives trace back to the threats, OSPs and assumptions as described in the security problem definition.

a) *No spurious objectives*: Each security objective traces to at least one threat, OSP or assumption.

b) *Complete with respect to the security problem definition*: Each threat, OSP and assumption has at least one security objective tracing to it.

c) *Correct tracing*: Since assumptions are always made by the TOE on the operational environment, security objectives for the TOE do not trace back to assumptions. The tracings allowed by ISO/IEC 15408-3 are depicted in Figure A.2.

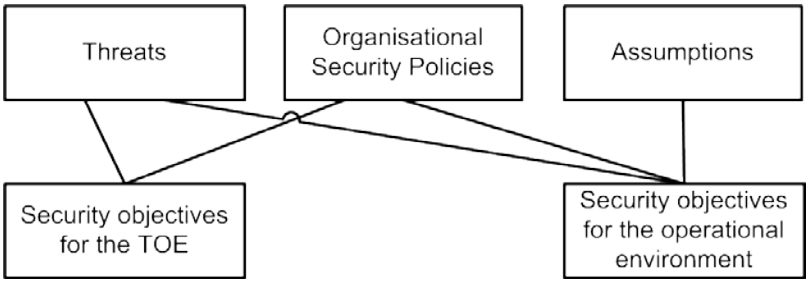

Figure A.2 - Tracings between security objectives and security problem definition

Multiple security objectives may trace to the same threat, indicating that the combination of those security objectives counters that threat. A similar argument holds for OSPs and assumptions.

A.7.3.2 Providing a justification for the tracing

The security objectives rationale also demonstrates that the tracing is effective: All the given threats, OSPs and assumption are addressed (i.e. countered, enforced and upheld respectively) if all security objectives tracing to a particular threat, OSP or assumption are achieved.

This demonstration analyses the effect of achieving the relevant security objectives on countering the threats, enforcing the OSPs and upholding the assumptions and leads to the conclusion that this is indeed the case.

In some cases, where parts of the security problem definition very closely resemble some security objectives, the demonstration can be very simple. An example is: a threat “T17: Threat agent X reads the Confidential Information in transit between A and B”, a security objective for the TOE: “OT12: The TOE shall ensure that all information transmitted between A and B is kept confidential”, and a demonstration “T17 is directly countered by OT12”.

A.7.3.3 On countering threats

Countering a threat does not necessarily mean removing that threat, it can also mean sufficiently diminishing that threat or sufficiently mitigating that threat.

Examples of removing a threat are:

- removing the ability to execute the adverse action from the threat agent;
- moving, changing or protecting the asset in such a way that the adverse action is no longer applicable to it;
- removing the threat agent (e.g. removing machines from a network that frequently crash that network).

Examples of diminishing a threat are:

- restricting the ability of a threat agent to perform adverse actions;
- restricting the opportunity to execute an adverse action of a threat agent;
- reducing the likelihood of an executed adverse action being successful;
- reducing the motivation to execute an adverse action of a threat agent by deterrence;

- requiring greater expertise or greater resources from the threat agent.

Examples of mitigating the effects of a threat are:

- making frequent back-ups of the asset;
- obtaining spare copies of an asset;
- insuring an asset;
- ensuring that successful adverse actions are always timely detected, so that appropriate action can be taken.

A.7.4 Security objectives: conclusion

Based on the security objectives and the security objectives rationale, the following conclusion can be drawn: if all security objectives are achieved then the security problem as defined in Security problem definition (ASE_SPD) is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

A.8 Extended Components Definition (ASE_ECD)

In many cases the security requirements (see the next subclause) in an ST are based on components in ISO/IEC 15408-2 or ISO/IEC 15408-3. However, in some cases, there may be requirements in an ST that are not based on components in ISO/IEC 15408-2 or ISO/IEC 15408-3. In this case, new components (extended components) must be defined, and this definition should be done in the Extended Components Definition. For more information on this, see Annex C.4.

Note that this subclause is intended to contain only the extended components and not the extended requirements (requirements based on extended components). The extended requirements should be included in the security requirements (see the next subclause) and are for all purposes the same as requirements based on components in ISO/IEC 15408-2 or ISO/IEC 15408-3.

A.9 Security requirements (ASE_REQ)

The security requirements consist of two groups of requirements:

a) *the security functional requirements* (SFRs): a translation of the security objectives for the TOE into a standardised language;

b) *the security assurance requirements* (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

These two groups are discussed in the following two subclauses:

A.9.1 Security functional requirements (SFRs)

The SFRs are a translation of the security objectives for the TOE. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives must be completely addressed) and be independent of any specific technical solution (implementation). ISO/IEC 15408 requires this translation into a standardised language for several reasons:

- to provide an exact description of what is to be evaluated. As security objectives for the TOE are usually formulated in natural language, translation into a standardised language enforces a more exact description of the functionality of the TOE.
- to allow comparison between two STs. As different ST authors may use different terminology in describing their security objectives, the standardised language enforces using the same terminology and concepts. This allows easy comparison.

There is no translation required in ISO/IEC 15408 for the security objectives for the operational environment, because the operational environment is not evaluated and does therefore not require a description aimed at its evaluation. See the bibliography for items relevant to the security assessment of operational systems.

It may be the case that parts of the operational environment are evaluated in another evaluation, but this is out of scope for the current evaluation. For example: an OS TOE may require a firewall to be present in its operational environment. Another evaluation may subsequently evaluate the firewall, but this evaluation has nothing to do with the evaluation of the OS TOE.

A.9.1.1 How ISO/IEC 15408 supports this translation

ISO/IEC 15408 supports this translation in three ways:

a) by providing a predefined precise “language” designed to describe exactly what is to be evaluated. This language is defined as a set of components defined in ISO/IEC 15408-2. The use of this language as a well-defined translation of the security objectives for the TOE to SFRs is mandatory, though some exceptions exist (see 7.3).

b) by providing operations: mechanisms that allow the ST writer to modify the SFRs to provide a more accurate translation of the security objectives for the TOE. This part of ISO/IEC 15408 defines the four allowed operations: assignment, selection, iteration, and refinement. These are described further in 7.1.

c) by providing dependencies: a mechanism that supports a more complete translation to SFRs. In ISO/IEC 15408-2 language, an SFR can have a dependency on other SFRs. This signifies that if an ST uses that SFR, it generally needs to use those other SFRs as well. This makes it much harder for the ST writer to overlook including necessary SFRs and thereby improves the completeness of the ST. Dependencies are described further in 7.2.

A.9.1.2 Relation between SFRs and security objectives

The ST also contains a security requirements rationale, consisting of two subclauses about SFRs:

- a tracing that shows which SFRs address which security objectives for the TOE;
- a set of justifications that shows that all security objectives for the TOE are effectively addressed by the SFRs.

A.9.1.2.1 Tracing between SFRs and the security objectives for the TOE

The tracing shows how the SFRs trace back to the security objectives for the TOE as follows:

a) *No spurious SFRs*: Each SFR traces back to at least one security objective.

b) *Complete with respect to the security objectives for the TOE*: Each security objective for the TOE has at least one SFR tracing to it.

Multiple SFRs may trace to the same security objective for the TOE, indicating that the combination of those security requirements meets that security objective for the TOE.

A.9.1.2.2 Providing a justification for the tracing

The security requirements rationale demonstrates that the tracing is effective: if all SFRs tracing to a particular security objective for the TOE are satisfied, that security objective for the TOE is achieved.

This demonstration should analyse the effects of satisfying the relevant SFRs on achieving the security objective for the TOE and lead to the conclusion that this is indeed the case.

In cases where SFRs very closely resemble security objectives for the TOE, the demonstration can be very simple.

A.9.2 Security assurance requirements (SARs)

The SARs are a description of how the TOE is to be evaluated. This description uses a standardised language for two reasons:

- to provide an exact description of how the TOE is to be evaluated. Using a standardised language assists in creating an exact description and avoids ambiguity.

- to allow comparison between two STs. As different ST authors may use different terminology in describing the evaluation, the standardised language enforces using the same terminology and concepts. This allows easy comparison.

This standardised language is defined as a set of components defined in ISO/IEC 15408-3. The use of this language is mandatory, though some exceptions exist. ISO/IEC 15408 enhances this language in two ways:

a) by providing operations: mechanisms that allow the ST writer to modify the SARs. ISO/IEC 15408 has four operations: assignment, selection, iteration, and refinement. These are described further in 7.1.

b) by providing dependencies: a mechanism that supports a more complete translation to SARs. In ISO/IEC 15408-3 language, an SAR can have a dependency on other SARs. This signifies that if an ST uses that SAR, it generally needs to use those other SARs as well. This makes it much harder for the ST writer to overlook including necessary SARs and thereby improves the completeness of STs. Dependencies are described further in 7.2.

A.9.3 SARs and the security requirement rationale

The ST also contains a security requirements rationale that explains why this particular set of SARs was deemed appropriate. There are no specific requirements for this explanation. The goal for this explanation is to allow the readers of the ST to understand the reasons why this particular set was chosen.

An example of an inconsistency is if the security problem description mentions threats where the threat agent is very capable, and a low (or no) Vulnerability analysis (AVA_VAN) is included in the SARs.

A.9.4 Security requirements: conclusion

In the security problem definition of the ST, the security problem is defined as consisting of threats, OSPs and assumptions. In the security objectives subclause of the ST, the solution is provided in the form of two sub-solutions:

- security objectives for the TOE;

- security objectives for the operational environment.

Additionally, a security objectives rationale is provided showing that if all security objectives are achieved, the security problem is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

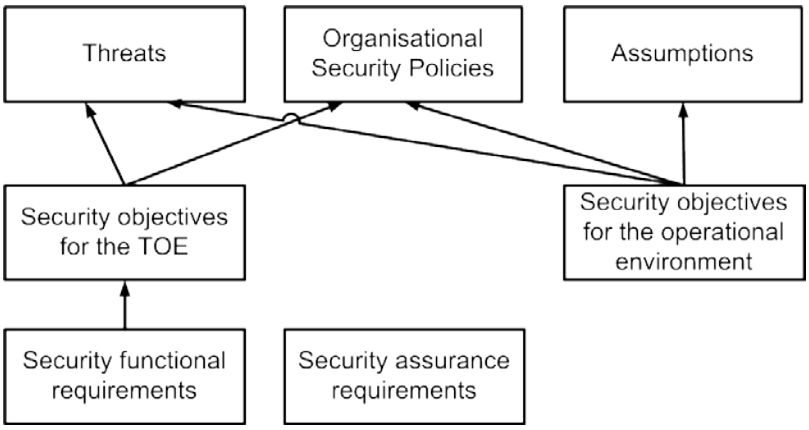

Figure A.3 - Relations between the security problem definition, the security objectives and the security requirements

In the security requirements subclause of the ST, the security objectives for the TOE are translated to SFRs and a security requirements rationale is provided showing that if all SFRs are satisfied, all security objectives for the TOE are achieved.

Additionally, a set of SARs is provided to show how the TOE is evaluated, together with an explanation for selecting these SARs.

All of the above can be combined into the statement: If all SFRs and SARs are satisfied and all security objectives for the operational environment are achieved, then there exists assurance that the security problem as defined in ASE_SPD is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld. This is illustrated in Figure A.3.

The amount of assurance obtained is defined by the SARs, and whether this amount of assurance is sufficient is defined by the explanation for choosing these SARs.

A.10 TOE summary specification (ASE_TSS)

The objective for the TOE summary specification is to provide potential consumers of the TOE with a description of how the TOE satisfies all the SFRs. The TOE summary specification should provide the general technical mechanisms that the TOE uses for this purpose. The level of detail of this description should be enough to enable potential consumers to understand the general form and implementation of the TOE.

For instance if the TOE is an Internet PC and the SFRs contain FIA_UAU.1 to specify authentication, the TOE summary specification should indicate how this authentication is done: password, token, iris scanning etc. More information, like applicable standards that the TOE uses to meet SFRs, or more detailed descriptions may also be provided.

A.11 Questions that may be answered with an ST

After the evaluation, the ST specifies “what was evaluated”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST can therefore answer the following questions (and more):

a) *How can I find the ST/TOE that I need given the multitude of existing STs/TOEs?* This question is addressed by the TOE overview, which gives a brief (several paragraphs) summary of the TOE;

b) *Does this TOE fit in with my existing IT-infrastructure?* This question is addressed by the TOE overview, which identifies the major hardware/firmware/software elements needed to run the TOE;

c) *Does this TOE fit in with my existing operational environment?* This question is addressed by the security objectives for the operational environment, which identifies all constraints the TOE places on the operational environment in order to function;

d) *What does the TOE do (interested reader)?* This question is addressed by the TOE overview, which gives a brief (several paragraphs) summary of the TOE;

e) *What does the TOE do (potential consumer)?* This question is addressed by the TOE description, which gives a less brief (several pages) summary of the TOE;

f) *What does the TOE do (technical)?* This question is addressed by the TOE summary specification which provides a high-level description of the mechanisms the TOE uses;

g) *What does the TOE do (expert)?* This question is addressed by the SFRs which provide an abstract highly technical description, and the TOE summary specification which provide additional detail;

h) *Does the TOE address the problem as defined by my government/organisation?* If your government/organisation has defined packages and/or PPs to define this solution, then the answer can be found in the Conformance Claims subclause of the ST, which lists all packages and PPs that the ST conforms to

i) *Does the TOE address my security problem (expert)?* What are the threats countered by the TOE? What organisational security policies does it enforce? What assumptions does it make about the operational environment? These questions are addressed by the security problem definition;

j) *How much trust can I place in the TOE?* This can be found in the SARs in the security requirements subclause, which provide the assurance level that was used to evaluate the TOE, and hence the trust that the evaluation provides in the correctness of the TOE.

A.12 Low assurance Security Targets

Writing an ST is not a trivial task, and may, especially in low assurance evaluations, be a major part of the total effort expended by the developer and the evaluator in the whole of the evaluation. For this reason, it is also possible to write a low assurance ST.

ISO/IEC 15408 allows the use of a low assurance ST for an EAL 1 evaluation, but not for EAL 2 and up. A low-assurance ST may only claim conformance to a low-assurance PP (see Annex B). A regular ST (i.e., one with full contents) may claim conformance with a low assurance PP.

A low assurance ST has a significantly reduced content compared to a regular ST:

- there is no need to describe the security problem definition;
- there is no need to describe the security objectives for the TOE. The security objectives for the operational environment must still be described;
- there is no need to describe the security objectives rationale as there is no security problem definition in the ST;
- the security requirements rationale only needs to justify (any) dependencies not being satisfied as there are no security objectives for the TOE in the ST.

All that remains are:

a) the references to TOE and ST;

b) a conformance claim;

c) the various narrative descriptions;