



BSI Standards Publication

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security

Part 1: Introduction and general model

National foreword

This British Standard is the UK implementation of EN ISO/IEC 15408-1:2023. It is identical to ISO/IEC 15408-1:2022. It supersedes BS EN ISO/IEC 15408-1:2020, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 28228 3

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2022.

Amendments/corrigenda issued since publication

Date	Text affected
31 December 2023	Correction to designator, supersession details and addition of CEN-CENELEC title page and foreword.

English version

Information security, cybersecurity and privacy protection
- Evaluation criteria for IT security - Part 1: Introduction
and general model (ISO/IEC 15408-1:2022)

Sécurité de l'information, cybersécurité et protection
de la vie privée - Critères d'évaluation pour la sécurité
des technologies de l'information - Partie 1:
Introduction et modèle général (ISO/IEC 15408-
1:2022)

Informationssicherheit, Cybersicherheit und Schutz
der Privatsphäre - Evaluationskriterien für IT-
Sicherheit - Teil 1: Einführung und allgemeines Modell
(ISO/IEC 15408-1:2022)

This European Standard was approved by CEN on 20 November 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

European foreword

The text of ISO/IEC 15408-1:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 15408-1:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2024, and conflicting national standards shall be withdrawn at the latest by June 2024.

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

This document supersedes EN ISO/IEC 15408-1:2020.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 15408-1:2022 has been approved by CEN-CENELEC as EN ISO/IEC 15408-1:2023 without any modification.

Contents

Page

Foreword	vi
Introduction	viii
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviated terms	13
5 Overview	15
5.1 General	15
5.2 ISO/IEC 15408 series description	15
5.2.1 General	15
5.2.2 Audience	16
5.3 Target of evaluation (TOE)	19
5.3.1 General	19
5.3.2 TOE boundaries	19
5.3.3 Different representations of the TOE	20
5.3.4 Different configurations of the TOE	20
5.3.5 Operational environment of the TOE	20
5.4 Presentation of material in this document	21
6 General model	21
6.1 Background	21
6.2 Assets and security controls	21
6.3 Core constructs of the paradigm of the ISO/IEC 15408 series	24
6.3.1 General	24
6.3.2 Conformance types	24
6.3.3 Communicating security requirements	24
6.3.4 Meeting the needs of consumers (risk owners)	27
7 Specifying security requirements	29
7.1 Security problem definition (SPD)	29
7.1.1 General	29
7.1.2 Threats	29
7.1.3 Organizational security policies (OSPs)	30
7.1.4 Assumptions	30
7.2 Security objectives	31
7.2.1 General	31
7.2.2 Security objectives for the TOE	31
7.2.3 Security objectives for the operational environment	31
7.2.4 Relation between security objectives and the SPD	32
7.2.5 Tracing between security objectives and the SPD	32
7.2.6 Providing a justification for the tracing	33
7.2.7 On countering threats	33
7.2.8 Security objectives: conclusion	33
7.3 Security requirements	33
7.3.1 General	33
7.3.2 Security Functional Requirements (SFRs)	34
7.3.3 Security assurance requirements (SARs)	36
7.3.4 Security requirements: conclusion	37
8 Security components	38
8.1 Hierarchical structure of security components	38
8.1.1 General	38
8.1.2 Class	38
8.1.3 Family	39

8.1.4	Component.....	39
8.1.5	Element.....	39
8.2	Operations.....	39
8.2.1	General.....	39
8.2.2	Iteration.....	40
8.2.3	Assignment.....	40
8.2.4	Selection.....	41
8.2.5	Refinement.....	43
8.3	Dependencies between components.....	44
8.4	Extended components.....	44
8.4.1	General.....	44
8.4.2	Defining extended components.....	45
9	Packages.....	45
9.1	General.....	45
9.2	Package types.....	46
9.2.1	General.....	46
9.2.2	Assurance packages.....	46
9.2.3	Functional packages.....	47
9.3	Package dependencies.....	47
9.4	Evaluation method(s) and activities.....	47
10	Protection Profiles (PPs).....	48
10.1	General.....	48
10.2	PP introduction.....	48
10.3	Conformance claims and conformance statements.....	48
10.4	Security assurance requirements (SARs).....	51
10.5	Additional requirements common to strict and demonstrable conformance.....	51
10.5.1	Conformance claims and conformance statements.....	51
10.5.2	Security problem definition (SPD).....	51
10.5.3	Security objectives.....	52
10.6	Additional requirements specific to strict conformance.....	52
10.6.1	Requirements for the security problem definition (SPD).....	52
10.6.2	Requirements for the security objectives.....	52
10.6.3	Requirements for the security requirements.....	52
10.7	Additional requirements specific to demonstrable conformance.....	53
10.8	Additional requirements specific to exact conformance.....	53
10.8.1	General.....	53
10.8.2	Conformance claims and statements.....	53
10.9	Using PPs.....	54
10.10	Conformance statements and claims in the case of multiple PPs.....	54
10.10.1	General.....	54
10.10.2	Where strict or demonstrable conformance is specified.....	54
10.10.3	Where exact conformance is specified.....	54
11	Modular requirements construction.....	54
11.1	General.....	54
11.2	PP-Modules.....	55
11.2.1	General.....	55
11.2.2	PP-Module Base.....	55
11.2.3	Requirements for PP-Modules.....	55
11.3	PP-Configurations.....	59
11.3.1	General.....	59
11.3.2	Requirements for PP-Configurations.....	59
11.3.3	Usage of PP-Configurations.....	65
12	Security Targets (STs).....	68
12.1	General.....	68
12.2	Conformance claims and statements.....	68
12.3	Assurance requirements.....	71

12.4	Additional requirements in the exact conformance case.....	71
12.4.1	Additional requirements for the conformance claim	71
12.4.2	Additional requirements for the SPD	71
12.4.3	Additional requirements for the security objectives.....	72
12.4.4	Additional requirements for the security requirements	72
12.5	Additional requirements in the multi-assurance case.....	72
13	Evaluation and evaluation results	74
13.1	General.....	74
13.2	Evaluation context	76
13.3	Evaluation of PPs and PP-Configurations.....	77
13.4	Evaluation of STs.....	77
13.5	Evaluation of TOEs.....	77
13.6	Evaluation methods and evaluation activities.....	78
13.7	Evaluation results.....	78
13.7.1	Results of a PP evaluation.....	78
13.7.2	Results of a PP-Configuration evaluation	78
13.7.3	Results of a ST/TOE evaluation.....	78
13.8	Multi-assurance evaluation.....	79
14	Composition of assurance	80
14.1	General.....	80
14.2	Composition models	81
14.2.1	Layered composition model	81
14.2.2	Network or bi-directional composition model	82
14.2.3	Embedded composition model.....	82
14.3	Evaluation techniques for providing assurance in composition models.....	83
14.3.1	General	83
14.3.2	ACO class for composed TOEs.....	83
14.3.3	Composite evaluation for composite products.....	84
14.4	Requirements for evaluations using composition techniques.....	95
14.4.1	Re-use of evaluation results.....	95
14.4.2	Composition evaluation issues	96
14.5	Evaluation by composition and multi-assurance.....	97
	Annex A (normative) Specification of packages	98
	Annex B (normative) Specification of Protection Profiles (PPs)	102
	Annex C (normative) Specification of PP-Modules and PP-Configurations.....	112
	Annex D (normative) Specification of Security Targets (STs) and Direct Rationale STs.....	125
	Annex E (normative) PP/PP-Configuration conformance.....	136
	Bibliography.....	141

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <https://patents.iec.ch>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 15408-1:2009), which has been technically revised.

The main changes are as follows:

- the document has been restructured;
- technical changes have been introduced:
 - the terminology has been reviewed and updated;
 - the exact conformance type has been introduced;
 - low assurance protection profiles (PPs) have been removed and direct rationale PPs have been introduced;
 - PP-Modules and PP-Configurations for modular evaluations have been introduced;
 - multi-assurance evaluation has been introduced.

A list of all parts in the ISO/IEC 15408 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Legal notice

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

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale de la Sécurité des Systèmes d'Information
Germany	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Netherlands	Netherlands National Communications Security Agency
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Ministerio de Asuntos Económicos y Transformación Digital
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations 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.

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

The ISO/IEC 15408 series is intentionally flexible, enabling a range of evaluation approaches 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 the ISO/IEC 15408 series in conjunction with unsuitable evaluation methods/activities, irrelevant security properties, or inappropriate IT products, can 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 provides 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.

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

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

- a) the ISO/IEC 15408 series does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognized that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls;
- b) the ISO/IEC 15408 series does not address the evaluation methodology under which the criteria should be applied;

NOTE 1 The baseline methodology is defined in ISO/IEC 18045. ISO/IEC 15408-4 can be used to further derive evaluation activities and methods from ISO/IEC 18045.

- c) the ISO/IEC 15408 series does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the ISO/IEC 15408 series is intended to be used for evaluation purposes in the context of such a framework;
- d) the procedures for use of evaluation results in accreditation are outside the scope of the ISO/IEC 15408 series. 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 must make separate provisions for those aspects;

- e) the subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the ISO/IEC 15408 series. In the case that independent assessment of mathematical properties of cryptography is required, the evaluation scheme under which the ISO/IEC 15408 series is applied shall make provision for such assessments.

NOTE 2 This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 1: Introduction and general model

1 Scope

This document 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.

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

This document introduces:

- the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types;
- a description of the organization of security components throughout the model;
- the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations;
- general information about the evaluation methods given in ISO/IEC 18045;
- guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;
- general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5;
- information in regard to the scope of evaluation schemes.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

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

ISO/IEC IEEE 24765, *Systems and software engineering — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 18045 and ISO/IEC IEEE 24765 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 action

documented activity of the *evaluator* (3.45) or *developer* (3.33)

Note 1 to entry: Evaluator actions and developer actions are required by ISO/IEC 15408-3.

3.2 administrator

entity (3.36) that has a level of trust with respect to all policies implemented by the *TOE security functionality (TSF)* (3.92)

Note 1 to entry: Not all *protection profiles (PPs)* (3.68) or security targets (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 *target of evaluation (TOE)* (3.90). Some of these policies can be related to the functionality of the TOE, while others can be related to the *operational environment* (3.63).

3.3 adverse action

action (3.1) performed by a *threat agent* (3.91) on an *asset* (3.4)

3.4 asset

entity (3.36) that the owner of the *target of evaluation (TOE)* (3.90) presumably places value on

3.5 assignment

specification of an identified parameter in a functional or assurance component

3.6 assurance

grounds for confidence that a *target of evaluation (TOE)* (3.90) meets the *security functional requirements (SFRs)* (3.78)

3.7 assurance package

named set of *security assurance requirements* (3.76)

EXAMPLE "EAL 3".

3.8 attack potential

measure of the effort needed to exploit a vulnerability in a *target of evaluation (TOE)* (3.90)

Note 1 to entry: The effort is expressed as a function of properties related to the attacker (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

3.9**attack surface**

set of logical or physical interfaces to a target, consisting of points through which access to the target and its functions may be attempted

EXAMPLE 1 The casing of a payment terminal is a part of physical attack surface for that device.

EXAMPLE 2 The communications protocols available for connection to a network device are part of the logical attack surface for that network device.

3.10**augmentation**

addition of one or more requirements to a package

Note 1 to entry: In case of a *functional package* (3.51), such an augmentation is considered only in the context of one package and is not considered in the context with other packages or *protection profiles (PPs)* (3.68) or *security targets (STs)* (3.82).

Note 2 to entry: In case of an *assurance package* (3.7), augmentation refers to one or more *security assurance requirements (SARs)* (3.76).

3.11**authorized user**

entity (3.36) who may, in accordance with the *security functional requirements (SFRs)* (3.78), perform an operation on the *target of evaluation (TOE)* (3.90)

3.12**base component**

independent entity (3.36) in a multi-component product that provides services and resources to one or more *dependent component(s)* (3.31)

Note 1 to entry: This applies in particular to 'composed TOEs' (3.21) and 'composite products / composite TOEs' (3.25).

3.13**base Protection Profile****base PP**

Protection Profile (3.68) specified in a *PP-Module* (3.71), as part of that PP-Module's *PP-Module Base* (3.72), used as a basis to build a *PP-Configuration* (3.69)

3.14**base PP-Module**

PP-Module (3.71) specified in a different PP-Module, as part of that PP-Module's *PP-Module Base* (3.72), used as a basis to build a *PP-Configuration* (3.69)

Note 1 to entry: Specifying a base PP-Module in a PP-Module implicitly includes the base PP-Module's PP-Module Base.

3.15**base target of evaluation****base TOE**

base component (3.12) which is itself the subject of an evaluation

Note 1 to entry: This applies in particular to 'composed TOEs' (3.21) and 'composite products/composite TOEs' (3.25).

3.16**class**

<taxonomy> set of families that share a common focus

Note 1 to entry: Class is further defined in ISO/IEC 15408-2, which defines security functional classes and ISO/IEC 15408-3, which defines security assurance classes.

3.17

component

<taxonomy> smallest selectable set of elements on which requirements may be based

3.18

component

<composition> *entity* (3.36) which provides resources and services in a product

3.19

component target of evaluation

component TOE

(evaluated) *target of evaluation (TOE)* (3.90) that is a component of another *composed TOE* (3.21)

3.20

composed assurance package

CAP

assurance package (3.7) consisting of components drawn predominately from the *ACO class* (3.16), representing a point on the pre-defined scale for composition assurance

3.21

composed target of evaluation

composed TOE

target of evaluation (TOE) (3.90) comprising solely two or more separately identified components with a security relationship between their *TOE security functionality (TSFs)* (3.92)

Note 1 to entry: Each of the separately identified components is itself a TOE.

3.22

composed evaluation

evaluation of a *composed TOE* (3.21) using the specific evaluation technique applicable to composed TOEs

Note 1 to entry: This evaluation technique refers to the *ACO assurance class* (3.16) that is defined in ISO/IEC 15408-3.

3.23

composite evaluation

evaluation of a *composite TOE/product* (3.25) using the specific composite evaluation technique

Note 1 to entry: This evaluation technique refers to the COMP related assurance families that are specified in ISO/IEC 15408-3 for the ADV, ALC, ASE, ATE and AVA classes (3.16).

3.24

composite product

product comprised of two or more components which can be organized in two layers: a layer of one already evaluated *base component (base TOE)* (3.15) and a layer of one *dependent component* (3.31)

3.25

composite target of evaluation

composite TOE

part of a *composite product* (3.24) including the *base TOE* (3.15) and the *dependent component* (3.31)

Note 1 to entry: A dependent component in a composite TOE can consist of one or more dependent components. For simplification, they are considered as 'one dependent component'.

Note 2 to entry: A composite TOE can contain parts that are independent from the *base component* (3.12) or *base TOE* respectively. For simplification, such parts are considered as belonging to the dependent component.

Note 3 to entry: The *composite evaluation* (3.23) can be applied as many times as necessary to a multi-component/multi-layered product, in an incremental approach.

3.26**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

[SOURCE: ISO/IEC IEEE 24765:2017, 3.779 1]

3.27**configuration management system**

set of procedures and tools (including their documentation) used by a *developer* (3.33) to develop and maintain configurations of their products during their life-cycles

Note 1 to entry: Configuration management systems can have varying degrees of rigour and function. At higher levels, configuration management systems can be automated, with flaw remediation, change controls, and other tracking mechanisms.

3.28**counter, verb**

act on or respond to a particular threat so that the threat is eradicated or mitigated

3.29**demonstrable conformance****DC**

relation between a *protection profile (PP)* (3.68)/*security target (ST)* (3.82) (PP/ST) and a PP, or an ST and a *PP-Configuration* (3.69), where the PP/ST provides an equivalent or more restrictive solution that solves the generic security problem in the PP/PP-Configuration

3.30**dependency**

relationship between components such that a *protection profile (PP)* (3.68), *security target (ST)* (3.82), *functional package* (3.51) or *assurance package* (3.7) including a component also includes any other components that are identified as being depended upon or include a rationale as to why they are not

3.31**dependent component**

dependent entity (3.36) in a multi-component product that relies on the provision of services and resources by one or more *base components* (3.12)

Note 1 to entry: This applies in particular to '*composed TOEs*' (3.21) and '*composite products / composite TOE*' (3.25).

3.32**dependent target of evaluation****dependent TOE**

dependent component (3.31) which is itself the subject of an evaluation

Note 1 to entry: This applies only to '*composed TOEs*' (3.21) and not to '*composite products / composite TOEs*' (3.25).

3.33**developer**

organization responsible for the development of the *target of evaluation (TOE)* (3.90)

3.34

direct rationale

type of *Protection Profile* (3.68), *PP-Module* (3.71) or *Security Target* (3.82) in which the *security problem definition (SPD)* (3.80) elements are mapped directly to the *security functional requirements (SFRs)* (3.78) and possibly to the *security objectives* (3.79) for the *operational environment* (3.63)

Note 1 to entry: Direct rationale does not include security objectives for the *target of evaluation (TOE)* (3.90).

3.35

element

⟨taxonomy⟩ self-contained description of a security need assigned to *security assurance requirement (SAR)* (3.76) or *security functional requirement (SFR)* (3.78)

3.36

entity

identifiable item that is described by a set or collection of properties

Note 1 to entry: Entities include subjects, users (including external IT products), objects, information, sessions and/or resources.

3.37

evaluation

assessment of a *PP-Configuration* (3.69), *protection profile (PP)* (3.68), a *security target (ST)* (3.82), or a *target of evaluation (TOE)* (3.90), against defined criteria

3.38

evaluation activity

EA

activity derived from one or more work units

Note 1 to entry: Work units are defined in ISO/IEC 18045.

Note 2 to entry: Derivation mechanisms are defined in ISO/IEC 15408-4.

3.39

evaluation assurance level

EAL

well-formed package of *security assurance requirements* (3.76) representing a point on the pre-defined assurance scale

Note 1 to entry: EALs are defined in ISO/IEC 15408-5.

3.40

evaluation authority

body operating an *evaluation scheme* (3.42)

Note 1 to entry: By applying the evaluation scheme, the evaluation authority sets the standards and monitors the quality of evaluations conducted by bodies within a specific community.

3.41

evaluation method

EM

set of one or more *evaluation activities* (3.38) for application in a specific context

3.42

evaluation scheme

rules, procedures and management to carrying evaluations of IT product security

Note 1 to entry: An evaluation scheme implements all parts of the ISO/IEC 15408 series.

3.43**evaluation technical report****ETR**

documentation of the *overall verdict* (3.66) and its justification, produced by the *evaluator* (3.45), and submitted to an *evaluation authority* (3.40)

3.44**evaluation technical report for composite evaluation****ETR for composite evaluation****ETR_COMP**

documentation intended to be used within the *composite evaluation* (3.23) approach and derived by the *base component* (3.12) *evaluator* (3.45) from the full *evaluation technical report (ETR)* (3.43) for the evaluated base component

Note 1 to entry: The ETR for composite evaluation belongs to the base component and its evaluation and is used for the evaluation of a composite product with such base component when using the composite evaluation approach.

Note 2 to entry: The ETR for composite evaluation related to a base component is set up to provide sufficient information for a composite evaluation of a composite product that integrates such already evaluated base component. It enables the composite product *evaluator* (3.45) and the respective composite product *evaluation authority* (3.40) to understand the attack paths and the tests that have been considered and performed for the base component and the effectiveness of the countermeasures implemented by the base component.

3.45**evaluator**

individual assigned to perform evaluations in accordance with a given evaluation standard and associated evaluation methodology

Note 1 to entry: An example of evaluation standards is the ISO/IEC 15408 series with the associated evaluation methodology given in ISO/IEC 18045.

[SOURCE: ISO/IEC 19896-1:2018, 3.5]

3.46**exact conformance****EC**

hierarchical relationship between a *protection profile (PP)* (3.68) or *PP Configuration* (3.69) and a *security target (ST)* (3.82) where all the requirements in the ST are drawn only from the PP/PP-Configuration

Note 1 to entry: An ST is allowed to claim exact conformance to one or more PPs but only to one PP-Configuration.

3.47**exploitable vulnerability**

weakness in the *target of evaluation (TOE)* (3.90) that can be used to violate the *security functional requirements (SFRs)* (3.78) in the *operational environment* (3.63) for the TOE

3.48**extended security requirement**

security requirement developed according to the rules in this document, but which are not listed in any part of the ISO/IEC 15408 series

Note 1 to entry: An extended security requirement preserves the form and syntax described in ISO/IEC 15408-2.

Note 2 to entry: Extended security requirements can be defined by authors of *security target (ST)* (3.82) or *protection profile (PP)* (3.68) or *PP-Module* (3.71).

3.49**external entity****user**

human technical system or one of its components interacting with the *target of evaluation (TOE)* (3.90) from outside of the TOE boundary

3.50

family

⟨taxonomy⟩ set of components that shares a similar goal but differs in emphasis or rigour

3.51

functional package

named set of *security functional requirements* (3.78) that may be accompanied by a *security problem definition (SPD)* (3.80) and *security objectives* (3.79) derived from that SPD

3.52

global assurance package

assurance package (3.7) that applies to the entire *target of evaluation (TOE)* (3.90) in a *multi-assurance evaluation* (3.60)

Note 1 to entry: Global assurance package can contain extended assurance components.

3.53

guidance documentation

documentation that describes the delivery, preparation, operation, management and/or use of the *target of evaluation (TOE)* (3.90)

3.54

implementation representation

least abstract representation of the *TOE security functionality (TSF)* (3.92), specifically the one that is used to create the TSF itself without further design *refinement* (3.73)

Note 1 to entry: 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.

3.55

internally consistent, adj.

no apparent contradictions exist between any aspects of an *entity* (3.36)

Note 1 to entry: In terms of documentation, this means that there can be no statements within the documentation that can be taken to contradict each other.

3.56

interpretation

clarification or amplification of a standard or an evaluation scheme requirement

3.57

iteration

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

3.58

layering

design technique where separate groups of components are hierarchically organized to have separate responsibilities such that a group of components depends on groups of components below it in the hierarchy for services, and provides its services to the groups of components above it

3.59

module

architectural unit specified at a level suitable for implementation of the unit

Note 1 to entry: Properties related to division of a *target of evaluation (TOE)* (3.90) into modules are described in ISO/IEC 15408-3, in the ADV_TDS and ADV_INT families.

3.60**multi-assurance evaluation**

evaluation of a *target of evaluation (TOE)* (3.90) using a *PP-Configuration* (3.68) where each PP-Configuration component is associated with its own set of assurance requirements

Note 1 to entry: At least one of the PP-Configuration components contains a different set of assurance requirements to the others.

3.61**object**

entity (3.36) in the *target of evaluation (TOE)* (3.90) that contains or receives information, and upon which subjects perform operations

3.62**operation**

(on an object) specific type of *action* (3.1) performed by a subject on an object

3.63**operational environment**

environment in which the *target of evaluation (TOE)* (3.90) is operated, consisting of everything that is outside the TOE boundary

3.64**optional Security Functional Requirement****optional SFR**

security functional requirement (SFR) (3.78) in a *Protection Profile (PP)* (3.68), *functional package* (3.51), or *PP-Module* (3.71) that contributes to a stated aspect of the PP's security problem description but whose inclusion in a conformant PP's or *security target (ST's)* (3.82) list of SFRs is not mandatory

Note 1 to entry: An optional SFR can address appropriate *security problem definition (SPD)* (3.80) elements threat(s) and/or organizational security policies (OSPs) stated in the main body of the PP, functional package, or PP-Module, or reference associated SPD elements/objectives that themselves are optional (in that they are addressed solely by the optional SFR).

3.65**organizational security policy****OSP**

set of security rules, procedures, or guidelines for an organization

Note 1 to entry: A policy can pertain to a specific *operational environment* (3.63).

3.66**overall verdict**

statement issued by an *evaluator* (3.45) with respect to the result of an evaluation

Note 1 to entry: The statement can be expressed as “pass” or “fail”.

3.67**potential vulnerability**

suspected, but not confirmed, weakness

Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the *security functional requirements (SFRs)* (3.78).

3.68**Protection Profile****PP**

implementation-independent statement of security needs for a *target of evaluation (TOE)* (3.90) type

3.69

Protection Profile Configuration

PP-Configuration

implementation-independent statement of security needs for a *target of evaluation (TOE)* (3.90) type containing at least one *protection profile (PP)* (3.68) and an additional non-empty set of PPs and *PP-Modules* (3.71) (with the associated PP-Modules Bases)

3.70

Protection Profile Configuration component

PP-Configuration component

Protection Profile (PP) (3.68) or *PP-Module* (3.71) included in a *PP-Configuration* (3.69)

3.71

Protection Profile module

PP-Module

implementation-independent statement of security needs for a *target of evaluation (TOE)* (3.90) type complementary to one or more base *Protection Profiles* (3.68) and possibly some *base PP-Modules* (3.14)

3.72

Protection Profile Module Base

PP-Module Base

set of either *PP-Modules* (3.71) or *Protection Profiles (PPs)* (3.68) or both, specified by a PP-Module as a basis for building a *PP-Configuration* (3.69)

Note 1 to entry: The notion of a PP-Module Base is iterative in that the base of a PP-Module can contain another PP-Module with its own base, with that base containing a PP-Module. However, this “chain” terminates with a PP-Module that has only PP(s) as its base.

3.73

refinement

addition of details to a security component

3.74

residual vulnerability

weakness that cannot be exploited in the *operational environment* (3.63) for the *target of evaluation (TOE)* (3.90), but that can be used to violate the *security functional requirements (SFRs)* (3.78) by an attacker with greater *attack potential* (3.8) than is anticipated in the operational environment for the TOE

3.75

role

pre-defined set of rules establishing the allowed interactions between a user and the *target of evaluation (TOE)* (3.90)

3.76

security assurance requirement

SAR

security requirement that refers to the conditions and processes for the development and delivery of the *target of evaluation (TOE)* (3.90), and the *actions* (3.1) required of *evaluators* (3.45) with respect to evidence produced from these conditions and processes

3.77

security attribute

property of subjects, users, objects, information, sessions and/or resources that is used in defining the *security functional requirements (SFRs)* (3.78) and whose values are used in enforcing the SFRs

Note 1 to entry: Users can include external IT products.

3.78**security functional requirement****SFR**

security requirement, which contributes to fulfil the *target of evaluation (TOE)* (3.90) *security problem definition (SPD)* (3.80) as defined in a specific *security target (ST)* (3.82) or in a *protection profile (PP)* (3.68)

Note 1 to entry: A security functional requirement can be addressed directly as in the *direct rationale* (3.34) model, or indirectly, through the *security objectives* (3.79) for the TOE, as in the general model.

3.79**security objective**

statement of an intent to *counter* (3.28) identified threats and/or satisfy identified organization security policies and/or assumptions

3.80**security problem****security problem definition****SPD**

statement, which in a formal manner defines the nature and scope of the security that the *target of evaluation (TOE)* (3.90) is intended to address

Note 1 to entry: This statement consists of a combination of: threats to be countered by the TOE and its *operational environment* (3.63), the organizational security policies (OSPs) enforced by the TOE and its operational environment, and the assumptions that are upheld for the operational environment of the TOE.

Note 2 to entry: SPD-elements include threats, OSPs, and assumptions.

3.81**security requirement**

requirement, which is part of a *target of evaluation (TOE)* (3.90) security specification as defined in a specific *security target (ST)* (3.82) or in a *protection profile (PP)* (3.68) Note 1 to entry:

Requirements are stated in a language, i.e. form and syntax, specified in the ISO/IEC 15408 series.

3.82**Security Target****ST**

implementation-dependent statement of security requirements for a *target of evaluation (TOE)* (3.90) based on a *security problem definition* (3.80)

3.83**selection**

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

3.84**selection-based security functional requirement****selection-based SFR**

security functional requirement (SFR) (3.78) in a *Protection Profile (PP)* (3.78), *PP-Module* (3.71), or *functional package* (3.51) that contributes to a stated aspect of the PP's, PP-Module's or functional package's *security problem definition* (3.80) that is to be included in a conformant PP or ST if a selection choice identified in the PP/PP-Module/functional package indicates that it has an associated selection-based SFR

3.85**single-assurance evaluation**

evaluation of a *target of evaluation (TOE)* (3.90) using one set of assurance requirements

3.86

strict conformance

SC

hierarchical relationship between a *protection profile (PP)* (3.68) and a *PP/security target (ST)* (3.92) where all the requirements in the PP also exist in the PP/ST

Note 1 to entry: This relation can be paraphrased as “the ST contains all statements that are in the PP but can contain more”. Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner.

3.87

sub-TOE security functionality

sub-TSF

combined functionality of all hardware, software, and firmware of a *target of evaluation (TOE)* (3.90) that is relied upon for the correct enforcement of the security functional requirements (SFRs) defined in one *PP-Configuration* (3.69) component

Note 1 to entry: This set of SFRs is closed by dependencies, objectives, and *security problem definition (SPD)* (3.80) elements in the PP-Configuration component.

Note 2 to entry: The notion of sub-TSF is applied in relationship with the specification and evaluation of PP-Configurations and conformant security targets (STs). It can be used in the single-assurance approach, but it has to be used in the multi-assurance approach: sub-TSFs have to be defined in a multi-assurance PP-Configuration and in conformant multi-assurance STs.

Note 3 to entry: Each sub-TSF is associated with its own set of security assurance requirements (SARs) in a multi-assurance PP-Configuration/ST. In the rest of the document, a set of SARs can be an *assurance package* (3.7).

Note 4 to entry: A sub-TSF has the characteristics of a TSF.

3.88

subject

entity (3.36) in the *target of evaluation (TOE)* (3.90) that performs operations on objects

3.89

tailoring

addition of one or more functional requirements to a *functional package* (3.51), and/or the addition of one or more selections to a *security functional requirement (SFR)* (3.78) in a functional package

Note 1 to entry: Such tailoring is considered only in the context of one package and is not considered in the context with other packages, *protection profiles (PPs)* (3.68), or PP-Modules.

Note 2 to entry: The selections in the SFR can be replaced by the additional selections.

Note 3 to entry: Selections can only be added for packages claimed by PPs or PP-Modules. STs cannot claim package-name tailored conformance to the package.

3.90

target of evaluation

TOE

set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation

3.91

threat agent

entity (3.36) that has potential to exercise adverse *actions* (3.3) on *assets* (3.4) protected by the *target of evaluation (TOE)* (3.90)

3.92**TOE security functionality****TSF**

combined functionality of all hardware, software, and firmware of a *target of evaluation (TOE)* ([3.90](#)) that is relied upon for the correct enforcement of the *security functional requirements (SFRs)* ([3.78](#))

3.93**TOE type**

set of characteristics common to a group of *target of evaluations (TOEs)* ([3.90](#))

Note 1 to entry: The TOE type can be more explicitly defined in a *protection profile (PP)* ([3.68](#)).

3.94**translation**

process of describing security requirements in a standardized language

Note 1 to entry: Use of the term translation in this context is not literal and does not imply that every *security functional requirement (SFR)* ([3.78](#)) expressed in standardized language can also be translated back to the *security objectives* ([3.79](#)).

3.95**vulnerability**

weakness in the *target of evaluation (TOE)* ([3.90](#)) that can be used to violate the *security functional requirements (SFRs)* ([3.78](#)) in some environment

4 Abbreviated terms

AP	assurance package
API	application programming interface
CAP	composition assurance package
CD	compact disk
CM	configuration management
COMP	composite product assurance package
DAC	discretionary access control
DC	demonstrable conformance
DPA	differential power analysis
DRBG	deterministic random bit generator
EA	evaluation activity
EAL	evaluation assurance level
EC	exact conformance
EM	evaluation method
EMS	electromagnetic spectrum
ETR	evaluation technical report
GAP	global assurance package

GB	gigabyte
GHz	gigahertz
GUI	graphical user interface
HSM	hardware security module
HTTPS	hypertext transfer protocol secure
IC	integrated circuit
IOCTL	input output control
IP	internet protocol
IPsec	IP security (protocol)
IT	information technology
LDAP	lightweight directory access protocol
MAC	mandatory access control
MB	megabyte
MBps	megabytes per second
OR	observation report
OS	operating system
OSP	organizational security policy
OTP	one-time programmable
PC	personal computer
PCI	peripheral component interconnect
PKI	public key infrastructure
PP	protection profile
PPA	protection profile assurance package
RAM	random access memory
RBG	random bit generator
RNG	random number generator
RPC	remote procedure call
SAR	security assurance requirement
SC	strict conformance
SFP	security function policies
SFR	security functional requirement

SPA	simple power analysis
SPD	security problem definition
SSH	secure shell
ST	security target
STA	security target assurance package
TCP	transmission control protocol
TLS	transport layer security
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TSF interface
USB	universal serial bus
VPN	virtual private network

5 Overview

5.1 General

This clause introduces the main concepts of the ISO/IEC 15408 series. It identifies the concept of the Target of Evaluation (TOE), the target audience of the ISO/IEC 15408 series, and the approach taken to present the material in the ISO/IEC 15408 series.

5.2 ISO/IEC 15408 series description

5.2.1 General

The ISO/IEC 15408 series is presented as a set of distinct but related parts as identified below:

- a) **ISO/IEC 15408-1, Introduction, and general model** is the introduction to the ISO/IEC 15408 series. It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation;
- b) **ISO/IEC 15408-2, Security functional components** establishes a set of functional components that serve as standard templates upon which security functional requirements (SFRs) for TOEs are based. ISO/IEC 15408-2 catalogues the set of security functional components and organizes them in families and classes;
- c) **ISO/IEC 15408-3, Security assurance components** establishes a set of assurance components that serve as standard templates upon which security assurance requirements for TOEs are based. ISO/IEC 15408-3 catalogues the set of security assurance components and organizes them into families and classes. ISO/IEC 15408-3 also defines evaluation criteria for PPs, STs and TOEs;
- d) **ISO/IEC 15408-4, Framework for the specification of evaluation methods and activities** provides a standardized framework for the specification of evaluation methods and activities that may be included in PPs, STs and any documents supporting them, to be used by evaluators in support of evaluations using the model described in the other parts of the ISO/IEC 15408 series. ISO/IEC 18045 is fundamental to ISO/IEC 15408-4;

- e) **ISO/IEC 15408-5, Pre-defined packages of security requirements** provides packages of security assurance and SFRs that have been identified as useful in support of common usage by stakeholders. Examples of provided packages include the evaluation assurance levels (EAL) and the composed assurance packages (CAPs).

In the application of the ISO/IEC 15408 series, a justification shall be provided whenever the recommended option is not chosen.

In support of the ISO/IEC 15408 series, other documents have been published. The Bibliography provides a list of supportive documents.

NOTE ISO/IEC 18045 provides the baseline methodology for IT security evaluations performed in accordance with the ISO/IEC 15408 series.

5.2.2 Audience

5.2.2.1 General

There are five main groups with a general interest in evaluation of the security properties of TOEs: consumers (risk owners), developers, technical working groups, evaluators and others. The information presented in the ISO/IEC 15408 series has been structured to support the needs of all of these groups which are considered to be the principal users of the ISO/IEC 15408 series. The groups can benefit from the criteria as explained in [5.2.2.2](#) through [5.2.2.6](#).

5.2.2.2 Consumers (Risk owners)

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

Risk owners 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. Risk owners can also use the evaluation results to compare different TOEs.

The ISO/IEC 15408 series gives risk owners, especially those in consumer groups and communities of interest, an implementation-independent structure, termed the PP, in which to express their security requirements in an unambiguous manner.

5.2.2.3 Developers

The ISO/IEC 15408 series is intended to support IT product 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 conform to one or more PPs to show that the TOE meets the security requirements from consumers as laid down in those PPs.

The ISO/IEC 15408 series 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.

5.2.2.4 Technical working groups

The ISO/IEC 15408 series is intended to support technical working groups in preparing and developing PPs, PP-Modules, PP-Configurations, packages and supporting documents or guidance. Technical working groups can be composed of stakeholders including consumers (risk owners), developers, evaluators, and academics.

5.2.2.5 Evaluators

The ISO/IEC 15408 series contains criteria to be used by evaluators when forming judgements about the conformance of TOEs, STs, PPs and PP-Configurations to their security requirements. The ISO/IEC 15408 series describes the general set of actions the evaluator is to carry out.

NOTE The ISO/IEC 15408 series does not specify procedures to be followed in carrying out those actions. More information on these procedures can be found in [Clause 13](#).

5.2.2.6 Others

While the ISO/IEC 15408 series is oriented towards specification and evaluation of the IT security properties of TOEs, it can 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 the ISO/IEC 15408 series are:

- a) system custodians and system security officers responsible for determining and meeting organizational IT security policies and requirements;
- b) auditors, both internal and external, responsible for assessing the adequacy of the security of an IT solution (which can 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;
- f) evaluation authorities responsible for the management and oversight of IT security evaluation programs;
- g) academia who perform research on the topic of IT security.

[Table 1](#) presents the interest of each part of ISO/IEC 15408 series to each of the audience groupings.

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

ISO/IEC 15408 parts	Consumers (Risk owners)	Developers	Technical working groups	Evaluators	Others
Part 1	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications and security problem definitions (SPDs) for TOEs.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications for TOEs.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications for packages, PPs, PP-Modules and PP-Configurations.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use when evaluating PPs, PP-Configurations and STs.	May use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition.

Table 1 (continued)

ISO/IEC 15408 parts	Consumers (Risk owners)	Developers	Technical working groups	Evaluators	Others
Part 2	Shall use for guidance and reference when formulating statements of security functional components for their risk-environment.	Shall use for reference when interpreting statements of security functional components in packages, PPs and PP-Modules. Shall use when developing STs. May use when formulating security functionality for IT products.	Shall use for reference when formulating statements of security functional components in packages, PPs and PP-Modules.	Shall use for reference when evaluating security functional components given in packages, PPs and PP-Modules or security functional requirements (SFRs) in STs.	May use for reference when reviewing security functional components given in packages, PPs and PP-Modules or security functional requirements (SFRs) in STs.
Part 3	Shall use for guidance and reference when determining the security assurance required for their risk-environment.	Shall use for reference when interpreting statements of security assurance components in packages, PPs, PP-Modules and PP-Configurations. Shall use when developing STs May use when formulating or improving development processes.	Shall use for reference when formulating statements of security assurance components in packages, PPs, PP-Modules and PP-Configurations.	Shall use for reference when evaluating security functional components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.	May use for reference when reviewing security functional components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.
Part 4	Should use for reference and background information in the structure of evaluation method(s) and/or activities.	Should use for reference purposes and for guidance in the structure of evaluation method(s) and/or activities.	Should use for reference purposes and for guidance in the structure of evaluation methods and activities.	Should use for reference purposes and for guidance in the structure of evaluation methods and activities. Should use when formulating specific evaluation methods and activities.	May use for reference purposes and for guidance in the structure of evaluation methods and activities.
Part 5	Should use for reference in determining the contents of any claimed pre-defined packages of security requirements.	Shall use when developing STs claiming conformance to pre-defined packages of security requirements. Shall use for reference when preparing a TOE for evaluation conformant to pre-defined packages of security requirements.	Shall use when developing PPs, PP-Modules and PP-Configurations claiming conformance to pre-defined packages of security requirements.	Shall use for reference when evaluating PPs, PP-Modules and PP-Configurations or STs claiming conformance to pre-defined packages of security requirements.	May use for reference in determining the contents of any claimed pre-defined packages of security requirements.

5.3 Target of evaluation (TOE)

5.3.1 General

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

While there are cases where a TOE consists of a complete 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 can never be made into a product, or a combination of these.

As far as the ISO/IEC 15408 series 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.

EXAMPLE Examples of TOEs include devices characterized by few interfaces, reduced attack surface, and a well-known supply chain:

- a network device;
- a software application;
- an operating system;
- a virtualization system;
- an integrated circuit;
- the cryptographic co-processor of an integrated circuit;
- an application for a mobile device;
- a database application excluding the remote client software normally associated with that database application.

TOEs can also be more complex, characterized by a large interface/large interfaces and/or number of components, multiple manufacturing/integration phases, field upgradeable products such as:

- a Local Area Network (LAN) including all terminals, servers, network equipment and software;
- a mobile device;
- gateways and hubs;
- a software application in combination with an operating system;
- a multi-function device, such as a multi-function printer;
- a Hardware Security Module (HSM).

5.3.2 TOE boundaries

The concept of a TOE boundary is fundamental to the specification of the ST.

A TOE may be a complete IT product (or products), a part of an IT product, or made up of various components. The ST shall clearly outline the physical and logical scope of the TOE as it is delivered to the customer.

Any parts of an IT product that are not within the TOE boundary are outside the scope of the evaluation and are called *non-TOE parts of the IT product*.

5.3.3 Different representations of the TOE

In the ISO/IEC 15408 series, a TOE can occur in several representations in relationship with the assurance criteria:

NOTE These assurance criteria include testing (ATE) and vulnerability analysis (AVA), which require TOE samples, some design (ADV_IMP), which require an implementation representation, e.g. source code, and lifecycle (ALC), which requires the TOE's configuration list.

EXAMPLE TOE representations for a software TOE:

- a list of files in a configuration management system;
- a single master copy that has just been compiled;
- the source code for a specific version of an open-source distribution;
- a box containing physical media and a manual, ready to be shipped to a customer;
- a binary file available for secure download;
- an installed and operational version.

TOE representations for a hardware TOE:

- integrated circuit layout;
- memory mappings;
- wafers;
- modules.

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

5.3.4 Different configurations of the TOE

In general, IT products can be configured in many ways with different options enabled or disabled. During an evaluation performed in accordance with the ISO/IEC 15408 series, it will be determined whether a TOE meets certain requirements. It is often the case that the guidance part of the TOE constrains the possible configurations of the TOE, i.e. the guidance for the TOE can be different from the general guidance of the IT product.

EXAMPLE An operating system IT product: This product can be configured in many ways including, e.g. the types of users, number of users, types of external connections allowed/disallowed, options enabled/disabled.

In general, if an IT product contains or is a TOE then the configuration of the product will need to be much more tightly controlled, since some configuration options can lead to a TOE not meeting the requirements.

For this reason, there would be an expected difference between the guidance documentation for the general IT product, that can allow many configurations; and the guidance documentation for the TOE, that may allow only one or only a set of configurations that do not differ in security-relevant ways.

If the guidance documentation for the TOE allows more than one configuration, these configurations are collectively called “the TOE” and each configuration shall meet the requirements levied on the TOE.

5.3.5 Operational environment of the TOE

Everything outside the TOE boundary belongs to the TOE operational environment. In the case where the TOE is part of an IT product the IT product can have non-TOE parts. Such non-TOE parts are also part of the operational environment of the TOE.

The ST shall describe assumptions and define security objectives for the operational environment which together with the security functionality provided by the TOE itself are necessary to mitigate the threats, and to enforce organizational security policies (OSPs).

The security objectives for the operational environment may support the TOE security functionality.

The ST shall formulate clear requirements for the TOE environment in order to provide the user with sufficient information to use the evaluated TOE properly.

EXAMPLE Secure key generation and injection premises and processes is an example of a security objective for the operational environment which supports the TOE cryptographic services specified using FCS components from ISO/IEC 15408-2.

5.4 Presentation of material in this document

The general model is presented in [Clause 6](#), which explains the concepts relating to the evaluation of the security functionality of IT products, the definition of the security problem and the specification of security requirements addressing the security problem. Concepts relating to the specification of security requirements, packages, PPs, PP-Modules and PP-Configurations, that relate to the needs of risk-owners with similar security problems are introduced.

The means of specifying security requirements and the completion of security components provided in ISO/IEC 15408-2 and ISO/IEC 15408-3 are explained in [Clauses 7](#) and [8](#).

The requirements and recommendations for the core constructs of packages, PPs, PP-Modules, PP-Configurations and ST s, are explained in [Clauses 9, 10, 11](#) and [11.3.3](#).

The requirements and recommendations for evaluation and evaluation results for TOEs, STs, PPs and PP-Configurations are found in [Clause 13](#).

Finally, the topic of composing assurance is found in [Clause 14](#).

6 General model

6.1 Background

This clause presents the general concepts used throughout the ISO/IEC 15408 series, including the context in which the concepts are to be used and the approach for applying the concepts. ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 15408-4, and ISO/IEC 15408-5 expand on the use of these concepts and assume that the approach described here is used. Further, for users of the ISO/IEC 15408 series who intend to perform evaluation activities, ISO/IEC 18045 is applicable.

The ISO/IEC 15408 series 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 the ISO/IEC 15408 series. However, the concepts themselves are not intended to restrict the class of IT security problems to which the ISO/IEC 15408 series is applicable. [Clause 6](#) assumes that the reader has knowledge of IT security and it is not intended to act as a tutorial in this area.

6.2 Assets and security controls

Security is concerned with the protection of assets within the operational environment.

EXAMPLE 1 An example of an asset is the contents of a file or a server.

Examples of operational environments in the context of such an asset are:

- a data centre where the server is installed;
- a computer network connected to the Internet which connects the server to the world;
- a LAN which connects the server to other servers and/or workstations;

- the every-day environment of a user who uses information from the server or a particular file;
- a general office environment which provides communication facilities to the server and/or a particular file.

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 can require that availability, dissemination, and modification of any such information are strictly controlled and that the assets are protected from threats by security controls implemented in the operational environment. [Figure 1](#) illustrates these high-level concepts and relationships.

NOTE ISO/IEC 27001 provides requirements for establishing, implementing, maintaining and continually improving an information security management system including the specification of controls.

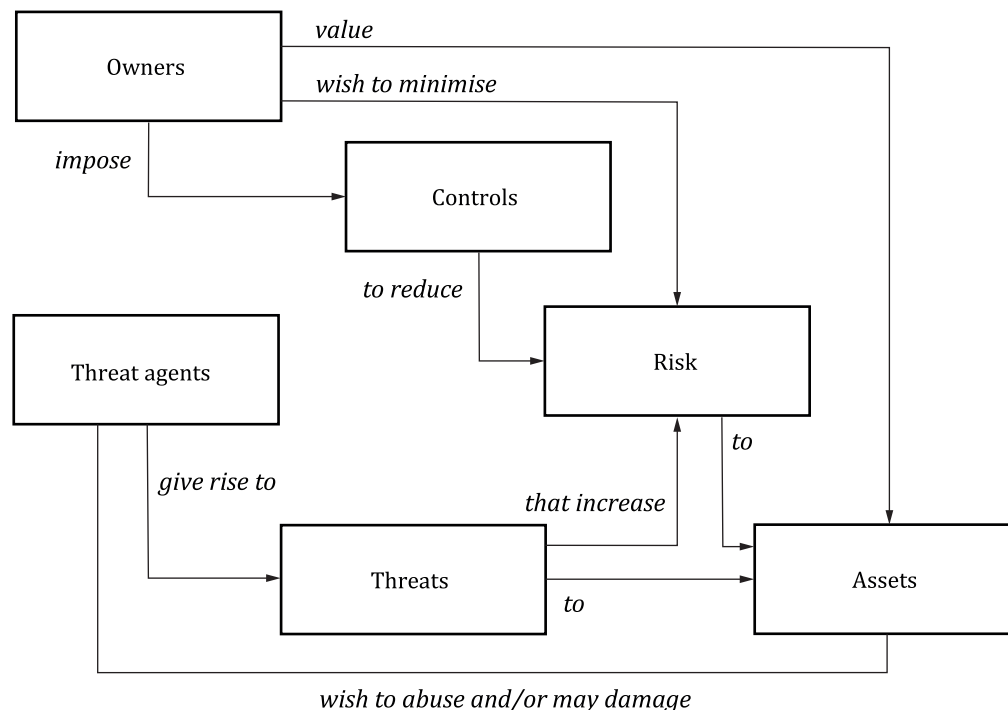


Figure 1 — Security concepts and relationships

Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents can also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner.

EXAMPLE 2 Examples of threat agents include hackers, malicious users, non-malicious users, who sometimes make errors, computer processes and accidents.

The owners of the assets can perceive such threats as a potential source of impairment of the assets, leading to a decrease of their value. 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 realized and the impact on the assets when that threat is realized. Subsequently controls are imposed to reduce the risks to assets. These controls can consist of IT-related controls (e.g. firewalls and smart cards) and non-IT controls (e.g. guards and procedures). See also ISO/IEC 27001 and ISO/IEC 27002 for a more general discussion on security controls and how to implement and manage them.

Owners of assets can 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 controls are sufficient: if the applied controls do what they claim to do, the threats to the assets are countered;
- the controls are correct: if the applied controls do what they claim to do.

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

[Figure 2](#) describes the evaluation concepts and relationships discussed in this clause.

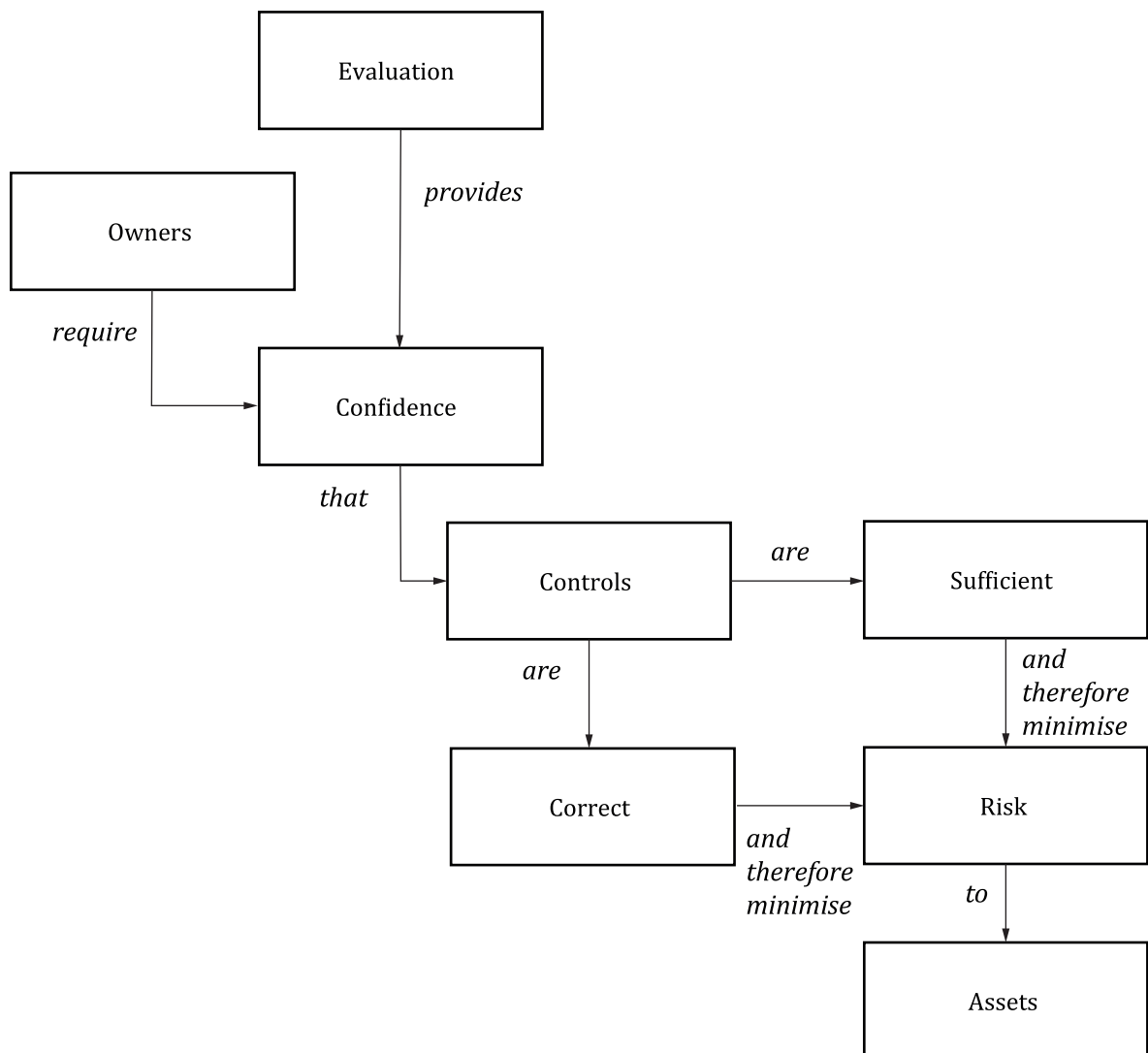


Figure 2 — Evaluation concepts and relationships

In an evaluation, the sufficiency of the security controls is analysed through a construct called the security target (ST).

6.3 Core constructs of the paradigm of the ISO/IEC 15408 series

6.3.1 General

The ISO/IEC 15408 series defines a flexible framework for the evaluation of IT products.

To allow consumer groups and technical communities to express their security needs, and to facilitate authoring appropriate documents that express these needs, five constructs are provided in the paradigm: package, PP, PP-Module, PP-Configuration and ST.

As an evaluation can need to meet varying assurance needs of consumers (risk owners), the ISO/IEC 15408 series provides different tools including well-formed security assurance components (ISO/IEC 15408-3) as well as a mechanism to define extended assurance components (ISO/IEC 15408-1).

Users of ISO/IEC 15408 series may also choose from pre-defined packages including those for EALs (based on ISO/IEC 15408-5), or from a framework for defining evaluation methods and activities (ISO/IEC 15408-4), and the associated evaluation methodology (based on ISO/IEC 18045).

6.3.2 Conformance types

Three different types of conformance to PPs and PP-Configurations have been defined to meet the needs of consumers (risk owners). These are exact, strict and demonstrable conformance. They are described in detail in [Annex E](#).

PPs, PP-Modules and PP-Configurations shall specify a conformance type.

STs claim conformance to PPs and PP-Configurations according to their conformance types. PPs can also claim conformance to other PPs according to their conformance type.

Conformance types, conformance claims, and relationships of conformance types of PPs, PP-Modules and PP-Configurations are described in [Annex E](#) and shall be used in conjunction with the clauses of this document.

6.3.3 Communicating security requirements

6.3.3.1 Packages

Packages describe a set of related security requirements that are frequently used together. Packages are often designed to be re-used bringing some comparability between those PPs, PP-Modules and STs that use them.

Security functional packages may be used to define security protocols, or other security functional concepts.

Security assurance packages may be used to define the conditions and processes such as specification, design, development, testing and delivery under which the TOE is developed and configured.

Core requirements for packages can be found in [Clause 9](#). [Annex A](#) provides additional information and requirements about packages that shall be used in conjunction with the clauses of this document.

ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for STs, PPs and PP-Modules undergoing evaluation that may use packages and ISO/IEC 15408-5 provides some pre-defined assurance packages that may be used by PP, PP-Module, PP-Configuration and ST authors.

6.3.3.2 Protection Profiles (PPs)

PPs describe a TOE type and the security assurance requirements (SARs) and security functional requirements (SFRs) expected to be provided for that type of TOE.

PPs based on other PPs may be used to further refine a TOE type.

PPs may take either a standard or a direct rationale approach.

Core requirements for PPs can be found in [Clause 10](#) and further information is found in [Annex B](#) that shall be used in conjunction with the clauses of this document.

ISO/IEC 15408-3 provides evaluation criteria for PPs.

6.3.3.3 PP-Modules and PP-Configurations

PP-Configurations build upon the concepts of PP and PP-Module.

A PP-Module may be used to refine the generic TOE type of a base PP, or to add security requirements for particular technologies which may be optionally associated with the TOE type defined in the base PPs. PP-Modules may also be based on other PP-Modules. Further, PP-Configurations consist of a TOE type and set of requirements specified in several PPs and possibly PP-Modules (these are the PP-Configuration components).

This concept is described in more detail in [Clause 11](#) and [Annex C](#).

EXAMPLE A PP-Module describes the SFRs for Bluetooth technology. Another PP-Module describes the SFRs for wireless LAN clients. Using a PP-Configuration, the SFRs for each of these technologies can be combined with PPs describing a TOE type, such as an operating system PP, or a mobile device PP. In this context the PP describing the TOE type is referred to as a base PP. A PP-Configuration describes which PPs and PP-Modules are combined to present a specification that includes all the requirements given in the appropriate PPs and PP-Modules.

In this example it would be possible to specify six PP-Configurations:

- a) operating system with Bluetooth,
- b) operating system with Wireless client,
- c) operating system with Bluetooth and Wireless client,
- d) mobile device with Bluetooth,
- e) mobile device with Wireless client,
- f) mobile device with Bluetooth and Wireless client.

6.3.3.4 Security Targets (STs)

6.3.3.4.1 General

The clause presents a simplified view of the ST construct. A more detailed and complete description of the ST concept and the content requirements can be found in [11.3.3](#) and [Annex D](#) which shall be used in conjunction with the clauses of this document.

ISO/IEC 15408-3 provides evaluation criteria and specific requirements for STs undergoing evaluation.

6.3.3.4.2 Purpose of a ST

The ST is a key document that begins with determining the security problem definition (SPD) for the TOE. This includes specifying the assets to be protected and the threats to those assets. The ST then considers any relevant assumptions and describes the security controls that need to be in place in order to demonstrate that these threats are countered. If the security controls do what they claim to do, the threats are countered.

The two groups of security controls are:

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

- b) the security objectives for the operational environment: these describe the security controls for which correctness will not be determined in the evaluation.

The reasons for this division are:

- the ISO/IEC 15408 series is suitable for assessing the correctness of IT development and production environments and product life cycle management. Security controls required from the operational environment are out of the scope of the evaluation according to the ISO/IEC 15408 series.
- assessing the correctness of security controls costs time and money, possibly making it infeasible to assess the correctness of all security controls.
- the correctness of some security controls can already have been assessed in another evaluation. It is therefore not cost-effective to assess this correctness again.

The ST further details the security objectives for the TOE by means of specifying SFRs. These SFRs shall be formulated in a standardized language, described in ISO/IEC 15408-2, to ensure precision and facilitate comparability.

In summary, the ST 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 address the SPD and, in particular, counter the threats;
- and therefore, the SFRs and the security objectives for the operational environment address the SPD and, in particular, counter the threats.

From this it follows that a correct TOE, i.e. a TOE that meets the SFRs in combination with a correct operational environment that meets the security objectives for the operational environment, will counter the threats. In [6.3.3.4.3](#) and [6.3.3.4.4](#) correctness of the TOE and correctness of the operational environment are discussed separately.

In some cases, defining a ST that omits security objectives for the TOE and directly maps the SFRs to the SPD is appropriate. This is a “Direct Rationale” ST, and is explained in detail in [11.3.3](#) and [Annex D](#).

A ST may be defined as standalone document for a specific TOE or may conform with a pre-existent PP-Configuration or one or several pre-existent PP(s). These documents allow for generic definitions of a TOE type to be made allowing for comparability in evaluation results between TOEs as well as efficiencies to be made.

Packages, PPs, PP-Modules and PP-Configurations that may contribute to the specification of a ST are introduced in [6.3.3.1](#), [6.3.3.2](#) and [6.3.3.3](#).

6.3.3.4.3 Correctness of the TOE

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

These vulnerabilities can arise from, e.g. poor design, accidental errors made during development, intentional addition of malicious code, poor configuration management.

To determine the correctness of the TOE, various activities may 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 ST provides a structured description of these activities to determine correctness in the form of SARs. These SARs shall be formulated in a standardized language described in ISO/IEC 15408-3 to ensure precision 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.

6.3.3.4.4 Correctness of the operational environment

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

However, in the ISO/IEC 15408 series, no assurance is obtained regarding the correctness of the operational environment, i.e. the operational environment is not evaluated.

As far as the evaluation is concerned, the operational environment is assumed to be a 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 this operational environment.

EXAMPLE 1 If, for an Operating System TOE, the security objectives for the operational environment state “The operational environment ensure that entities from an untrusted network can only access the TOE using the FTP protocol”, the consumer can select an evaluated firewall, and configure it to only allow FTP access to the TOE.

EXAMPLE 2 If the security objectives for the operational environment state: “The operational environment shall ensure that all administrative personnel do not behave maliciously”, the consumer can adapt their contracts with administrative personnel to include punitive sanctions for malicious behaviour, but this determination is not part of an evaluation using the ISO/IEC 15408 series as a basis.

NOTE The Internet is an example of an untrusted network.

6.3.4 Meeting the needs of consumers (risk owners)

6.3.4.1 General

Consumers (risk owners) can have different approaches for obtaining the assurance that the products they use to address the SPD. [6.3.4.2](#) and [6.3.4.3](#) introduce these approaches. Moreover, ISO/IEC 15408-4 provides methods to define specific evaluation activities for the assurance requirements.

6.3.4.2 Single assurance evaluation

Single assurance evaluation is the type of evaluation that has been specified in previous revisions of the ISO/IEC 15408 series. In single assurance evaluation a single set of SARs are applied to the entire TOE.

The single assurance evaluation paradigm:

- requires that the entire TOE has been subject to the same SARs;
- is used when a single set of SARs are commensurate with the security needs for the TOE.

A single assurance evaluation is based on an ST that may claim conformance with PP(s), or a PP-Configuration but is reliant on all claimed PPs or PP-Configuration components specifying identical sets or supersets of security assurance components. An evaluation based on an ST that does not make any conformance claim with PPs or a PP-Configuration is by its nature a single-assurance evaluation.

6.3.4.3 Multi-assurance evaluation

The multi-assurance evaluation paradigm consists in applying different assurance requirements to different parts of the TSF (sub-TSFs), while enforcing a global set of SARs for the entire TOE.

The multi-assurance evaluation paradigm:

- addresses heterogeneous IT products where different security needs require a different assurance within a single evaluation;
- ensures that the multiple assurance requirements are sound with regard to the security needs for the IT product.

Technically, a multi-assurance evaluation is driven by a ST that conforms with one (and only one) multi-assurance PP-Configuration. The multi-assurance PP-Configuration ensures that applying different assurance requirements to different parts of the TSF is consistent with their security needs. In this evaluation approach, each sub-TSF enforces some security functionality, e.g. an authentication protocol, a firewall policy, the boot process, encryption/decryption operations, and in some cases, the sub-TSF may be associated with a subset of TOE components, for instance a TPM, a cryptographic library or a card reader.

The multi-assurance paradigm is relevant, in particular, in the following situations:

- a product where some security functionality requires a higher assurance than the rest, e.g. a key storage and processing unit, a secure boot module;
- a product where some parts of the security functionality do not require the same high evaluation assurance as other more exposed parts, for instance an internet gateway with support for personal area network protocols;
- a family of products where some security functionality is shared across all the products with the same assurance, and some security functionality is implemented in different ways for different use cases, for instance in a tamper-resistant module or in a software module or through COTS, requiring a different assurance;

An example is a family of biometric authentication devices, with either match-on-device or match-on-SE, or both. This can give rise to a PP for the authentication device excluding the matching function, and two PP-Modules for the different types of matching functions, each with a dedicated set of assurance requirements. Three PP-Configurations can be defined for the device: PP with each of the PP-Modules, PP with both PP-Modules. A similar situation arises, for instance, for a family of mobile applications which uses either software crypto library secured by with-box techniques or a hardware-based crypto library, or for a family of payment terminals with either IC and/or magstripe readers;

Multi-assurance is also relevant for products claiming conformance to different PPs with different assurance packages: by defining and evaluating a PP-Configuration, the multi-assurance paradigm allows better control over possible inconsistencies between these PPs. The evaluation of electronic passports implementing both Basic Access Control and Extended Access Control constitutes a typical example, as these access control mechanisms are subject to different security problems and assurance requirements.

7 Specifying security requirements

7.1 Security problem definition (SPD)

7.1.1 General

The SPD defines the security problem that is to be addressed and may appear in PPs, PP-Modules and STs. The SPD is, as far as the ISO/IEC 15408 series is concerned, axiomatic, i.e. the process of deriving the SPD falls outside the scope of the ISO/IEC 15408 series.

SPD elements can be associated with configurations or requirements that are optional for the given TOE type, for example, in a case where the TOE is distributed, or where optional functional requirements (as outlined in 7.3.2.6) are specified. This is allowed as long as the optional nature of the SPD elements (and any associated objectives and functional requirements) are identified as specified in this document.

NOTE 1 The usefulness of the results of an evaluation strongly depends on the quality of the SPD. It is therefore often worthwhile to spend significant resources and use well-defined processes and analyses to derive a good SPD. ISO/IEC 15446 presents guidance in regard to deriving an SPD.

NOTE 2 According to ISO/IEC 15408-3, it is not mandatory to have statements in all sections. A PP with threats does not need to have OSPs and vice versa. Also, any PP can omit assumptions.

NOTE 3 Where the TOE is physically distributed, it is preferable to discuss the relevant threats, OSPs and assumptions separately for distinct domains of the TOE operational environment.

7.1.2 Threats

The SPD describes 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 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 is preferable to describe them as, e.g. types of entities, groups of entities.

EXAMPLE 1

Examples of threat agents are:

- hackers;
- users;
- computer processes;
- accidents.

Threat agents can be further described by attributes such as expertise, resources, opportunity, and motivation.

EXAMPLE 2

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.

7.1.3 Organizational security policies (OSPs)

The SPD describes 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 in the operational environment. OSPs can be made by an organization controlling the operational environment of the TOE, or they can be made by legislative or regulatory bodies. OSPs can apply to the TOE and/or the operational environment of the TOE.

EXAMPLE Examples of OSPs are:

- “All products that are used by the government shall 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”.

7.1.4 Assumptions

The SPD describes 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, there is a possibility that the TOE will be unable to provide all of its security functionality. Assumptions may be on physical, personnel and connectivity of the operational environment.

EXAMPLE Examples of assumptions are:

- assumptions on the non-TOE part of the product;
 - it is assumed that the TOE will be integrated into a device that provides a hardware-based root of trust.
- assumptions on physical aspects of the operational environment;
 - it is assumed that the TOE will be placed in a room that is designed to minimize 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 During an 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. Nevertheless, the ST, PP and PP-Configuration evaluations help detect unrealistic assumptions for the type of TOE and operational environment, which can become unacceptable.

7.2 Security objectives

7.2.1 General

The security objectives are a concise statement of the intended solution to the security problem. The role of the security objectives is threefold:

- a) provide a high-level, natural language solution of the problem. The security objectives consist of a set of 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;
- b) divide this solution into two part-wise solutions, that reflect the roles of the TOE and its operational environment to address each part of the problem. In a 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;
- c) demonstrate that these part-wise solutions form a complete solution to the problem.

7.2.2 Security objectives for the TOE

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

EXAMPLE 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 PP”.

If the TOE is physically distributed, it is preferable to subdivide the section containing the security objectives for the TOE into several subsections to reflect this.

NOTE In Direct Rationale STs security objectives for the TOE are not included: See [D.4](#).

7.2.3 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 pair-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 shall achieve.

EXAMPLE

Examples of security objectives for the operational environment are:

- “The operational environment shall provide a workstation with the OS Linux 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 received from the TOE on the Audit Server”.

If the operational environment of the TOE consists of multiple physical sites, each with different properties, it is preferable to subdivide the section containing the security objectives for the operational environment into several sub-sections to reflect this.

Third party components that shall not be evaluated due to unavailability of evaluation evidence are included in the operational environment, and the security objectives for the operational environment shall include that the third-party component works as intended.

7.2.4 Relation between security objectives and the SPD

STs, PPs, PP-Modules and packages also contain a security objectives rationale containing two sections:

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

NOTE In Direct Rationale PPs a rationale for security objectives in the TOE is not included. See [D.4](#).

EXAMPLE 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”.

7.2.5 Tracing between security objectives and the SPD

The tracing shows how the security objectives trace back to the SPD-elements and that:

- a) *there are no spurious objectives;*

Each security objective traces to at least one SPD-element.

- b) *the security problem definition is completely covered;*

Each SPD-element has at least one security objective tracing to it;

- c) *the tracing is correct.*

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 3](#).

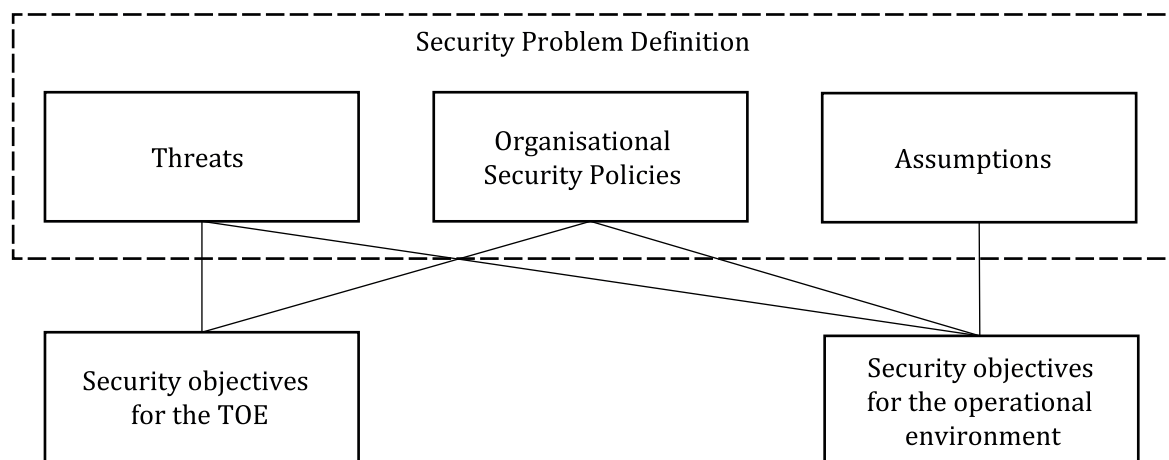


Figure 3 — Tracings between security objectives and the SPD

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.

7.2.6 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 SPD very closely resemble some security objectives, the demonstration can be straightforward.

7.2.7 On countering threats

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

EXAMPLE 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.

7.2.8 Security objectives: conclusion

Based on the security objectives and the security objectives rationale, the following conclusion is drawn: If all security objectives are achieved then the security problem as defined in SPD is solved. All threats are countered, all OSPs are enforced, and all assumptions are upheld.

NOTE The ASE_SPD family in ISO/IEC 15408-3 supports this determination.

7.3 Security requirements

7.3.1 General

As mentioned in [6.3.3.4](#) and [6.3.3](#), packages, PPs, PP-Modules, PP-Configurations and STs specify the detailed security requirements applicable to a TOE that have been derived from the stated SPD. SFRs and SARs shall be drawn from security components defined in ISO/IEC 15408-2 and ISO/IEC 15408-3

respectively, which are a template for security requirements written in a standardized language. The process of deriving a security requirement from a security component involves digesting the components and is known as “completion”.

NOTE 1 In [Clause 7](#), the term “author” includes authors of STs, PPs, PP-Modules, PP-Configurations and packages.

Security requirements are specified as a result of the description of the in a ST and possibly PP, PP-Module, and packages. Security requirements are specified by a choosing the components given in ISO/IEC 15408-2, ISO/IEC 15408-3 or that have been defined as extended components in accordance with [8.4](#). The tailoring process uses the operations in [8.2](#).

NOTE 2 Since a ST specifies the security requirements for a specific TOE it presents only fully completed components. PPs, PP-Modules and packages often present uncompleted security components allowing authors basing documents upon them appropriate flexibility.

The security requirements consist of two groups of requirements:

- a) **the security functional requirements** (SFRs): a description of how the TOE addresses the SPD in a standardized language;
- b) **the security assurance requirements** (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

NOTE 3 SARs concern the adherence of the TOE to the ST. SARs play no role in the coverage of the SPD, which is covered by security objectives and SFRs.

These two groups are discussed in [7.3.2](#) and [7.3.3](#).

7.3.2 Security Functional Requirements (SFRs)

7.3.2.1 General

The SFRs contribute to fulfil the TOE’s SPD and address the security objectives defined for the TOE. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives for the TOE shall be completely addressed). The ISO/IEC 15408 series requires this translation into a standardized language for the following reasons:

- to provide a precise description of what is to be evaluated. As security objectives for the TOE are usually formulated in natural language, translation into a standardized language enforces a more precise description of the functionality of the TOE;
- to allow comparison between two STs. The standardized language enforces using the same terminology and concepts. This allows comparison of STs even when authors use different terminology in describing their SPD and security objectives (this situation does not arise when the STs conform to the same PPs or PP-Configuration).

In the context of PPs and PP-Modules, the SFRs shall be independent of any specific technical solution (implementation).

There is no translation required in this document 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.

NOTE 1 See the Bibliography for items relevant to the security assessment of operational systems.

NOTE 2 It can be the case that parts of the operational environment are evaluated in another evaluation, but this is not within the scope of the ISO/IEC 15408 series.

EXAMPLE An operating system TOE can require a firewall to be present in its operational environment. Another evaluation can subsequently evaluate the firewall, but this evaluation has nothing to do with the evaluation of the OS TOE.

7.3.2.2 How this translation is supported

The ISO/IEC 15408 series supports this translation in three ways:

- a) By providing a pre-defined “language” designed to describe precisely 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 and are given in [8.4](#);
- b) By providing operations: mechanisms that allow the author of the package, ST, PP or PP-Module to complete and modify the SFRs to provide a more accurate translation of the security objectives for the TOE or TOE type. This document defines the four allowed operations: assignment, selection, iteration, and refinement. These are described further in [8.2](#);
- c) By providing dependencies: a mechanism that supports a more complete translation to SFRs. In ISO/IEC 15408-2 language, an SFR may have a dependency on other SFRs. This signifies that if a ST uses that SFR, it generally needs to use those other SFRs as well. This makes it much harder for the ST author to overlook including necessary SFRs and thereby improves the completeness of the ST. Dependencies are described further in [8.3](#).

7.3.2.3 Relation between SFRs and security objectives

Packages, PPs, PP-Modules and STs contain a SFRs rationale, consisting of two sections:

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

NOTE In the Direct Rationale approach the tracing and rationale is provided between the SFRs and the SPD.

7.3.2.4 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.

7.3.2.5 Providing a justification for the tracing

The SFRs 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 analyses 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.

7.3.2.6 Special types of SFR

SFRs can be designated in packages, PPs and PP-Modules as optional requirements or selection-based requirements.

A. Optional requirements

Optional requirements are “optional” in the sense that they do not need to be included in a PP/ST in order for the PP/ST to claim conformance (of any type) to a PP or PP-Configuration.