REPLACES:

ISO/IEC JTC 1/SC 27/WG 3

Information technology - Security techniques - Security evaluation, testing and specification

Convenorship: AENOR, Spain, Vice-convenorship: JISC, Japan

DOC TYPE: Call for contributions

TITLE: Terms of reference and Call for Contributions for an ISO/IEC JTC 1/SC 27/WG 3 Study Period on The concept hierarchy for terminology used in SC27/WG3 projects in particular focused on the ISO/IEC 15408 and ISO/IEC 18045 projects

SOURCE: JTC 1/SC 27/WG 3 Secretariat

DATE: 2019-07-11

PROJECT: Study Period

STATUS: As per WG 3 recommendation 10 (contained in SC 27 N19523/WG 3 N1676) of the 58th SC 27/WG 3 meeting held in Tel-Aviv, Israel, April 1st – 5th 2019, this document provides Terms of Reference for a Study Period on Evaluation criteria for connected vehicle information security based on ISO/IEC 15408 starting in April 2019.

As per WG 3 recommendation 10 experts and Liaison Organizations of SC 27/WG 3 are requested to contribute by 2019-09-10.

PLEASE submit your contribution on the hereby attached document via the SC 27/WG 3 Consultations at: **http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg3**

ACTION: ACT

DUE DATE: 2019-09-10

DISTRIBUTION: M. Bañón, N. Kai, WG 3 Experts

MEDIUM: **http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg3**

NO. OF PAGES: 1 + attachment

Study Period on the concept hierarchy for terminology used in SC27/WG3 projects in particular focused on the ISO/IEC 15408 and ISO/IEC 18045 projects

Motivation

ISO/IEC JTC1 Directives, Part 2, Clause 16.4, say "*Terms and definitions should preferably be listed according to the hierarchy of the concepts (i.e. systematic order). Alphabetical order is the least preferred order.*"

The current versions of all projects developed by SC27/WG3, including ISO/IEC 15408 series of standards and ISO/IEC 18045 being currently under development, have all their terms presented in alphabetical order, which works in English only. Such approach presents several disadvantages including, but not limited to:

- all translated versions do not follow even the least preferable order as dictated by the Directives,
- presenting hundreds of terms in alphabetical order does not help users to understand the idea behind since definitions of adjacent terms can refer to completely different concepts,
- using different concepts and different perspectives without sufficient synchronization among projects leads to different definitions for the same term, unnecessary repetitions instead of referencing sources, differences in wording even where the same idea is developed, and thus creating confusion to users.

Works on hierarchy of concepts leading to the systematic order presentation of terms with regards to current revision of ISO/IEC 15408 and ISO/IEC 18045 had been started during the meeting held in Berlin, October 2017 and continued till the meeting in Tel-Aviv, April 2019. Current results of these efforts are registered in WG3 N1651, and modified version of preliminary systematic order for ISO/IEC 15408 and ISO/IEC 18045 resulted from comments submitted to N1651 and resolved during the meeting are included in Annex 1 to this ToR.

By the decision of editing group further works on the hierarchy of concept and systematic order of terms should be continued in this Study Period to achieve the following:

- Consistent and mature hierarchy of concepts and concept maps of terms for ISO/IEC 15408 and ISO/IEC 18045
- Creating the inventory of terms used in WG3 projects, identifying apparent inconsistencies, redundancies, obsolete terms,
- Identify preliminary hierarchy of concepts for projects other than ISO/IEC 15408 and ISO/IEC 18045

Experts, and in particular Project Editors of WG3 are motivated to consult with terminology experts in their countries/communities.

References

[1] SC27 N 18803 ISO/IEC 2nd CD 15408-1

[2] WG3 N 1633 ISO/IEC TR 4th WD 22216

[3] WG3 N 1651 Expert contribution on concept approach to the ISO/IEC 15408 & 18045 Terminology

[4] Other relevant standards and projects developed or being under development by WG3

[5] Generic terminology standards indicated in Annex 1 of this ToR, and other relevant international standards regarding terminology

Contributions are requested on the following topics:

– Further development hierarchy of concepts and concept maps of terms for ISO/IEC 15408 and 18045

– Providing information necessary for creating inventory of terms related to projects other than ISO/IEC 15408 and 18045

– Proposing new concepts to create the hierarchy of concepts for WG3 projects

Terms of Reference

The rapporteurs will examine contributions provided during the study period and present the results to interested WG 3 experts during the next WG 3 meeting which will be held in Paris, France according to the SC 27 calendar.

Annex no 1 - Concept approach to the ISO/IEC 15408 & 18045 Terminology

2019-06-18

Table of content

Background

According to the ISO/IEC JTC1 Directives, Part 2, Clause 16.4, "*Terms and definitions should preferably be listed according to the hierarchy of the concepts (i.e. systematic order). Alphabetical order is the least preferred order.*"

The current version of ISO/IEC 15408 series of standards and ISO/IEC 18045 have all their terms presented in alphabetical order, which works in English only. Hence all translated versions do not follow even the least preferable order as dictated by the Directives. Additionally, presenting hundreds of terms in alphabetical order does not help users understanding the idea behind since definitions of adjacent terms can refer to completely different concepts.

Further, by the decision taken at the Berlin meeting (October 2017) ALL terms related to the ICT security evaluation are to be gathered in one document, ie. ISO/IEC 15408-1. This means special attention should be paid to Clause 3 to present terms in a clear and easy-to-follow way for all potential users of the series of the 15408 standards.

Concept approach is described in several international standards related to terminology developed by the ISO Technical Committee TC37 *Language and terminology*.

A basic principle for this approach is that one term corresponds to one concept and only one concept corresponds to one term in a given domain or subject in a given language.

For the purpose of this document relevant terms are defined as follows[1]:

- **concept** means a unit of knowledge created by a unique combination of *characteristics*
- **term** means a verbal designation of a general concept in a specific domain or subject
- **designation** means a representation of a concept by a sign which denotes it
- **definition** means a representation of a concept by a descriptive statement which serves to differentiate it from related concepts.

Systematic order requires identification of distinguished concepts and further determining terms which relate to the concept and provide necessary characteristics. The concept can have its definition, but it is not always the case. Systematic order is achieved by proper numbering in the hierarchy of terms (see Fig.1). However, it is common to apply another style of numbering (see Fig. 2). The only condition is to use one style consistently.

---

[1] Adopted from ISO/IEC 10241-1:2011 Terminological entries in standards — Part 1: General requirements and examples of presentation
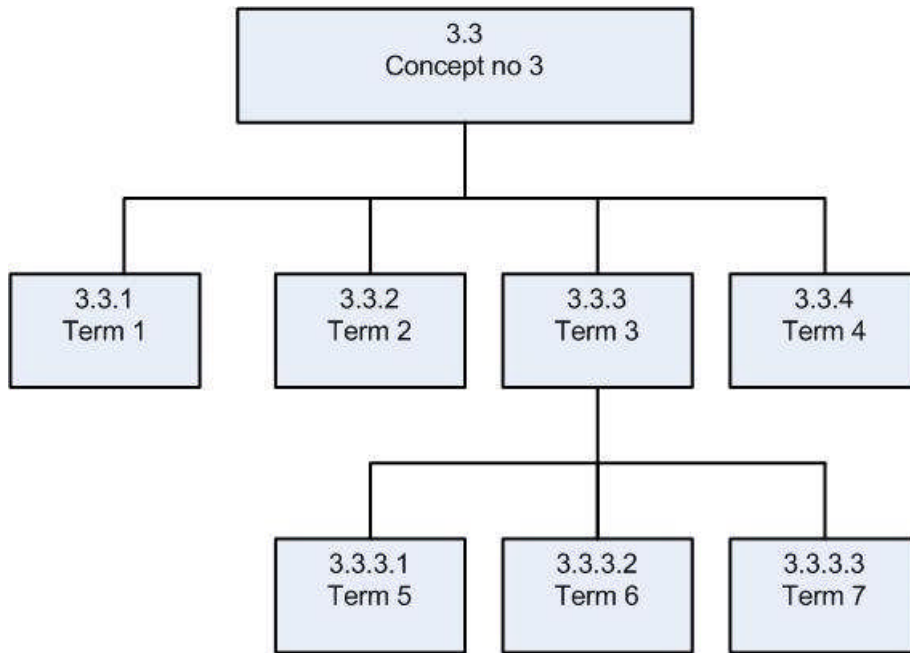
```
          ┌─────────────────┐
          │      3.3        │
          │  Concept no 3   │
          └────────┬────────┘
     ┌─────────┬───┴────┬──────────┐
┌────┴───┐ ┌───┴───┐ ┌──┴───┐ ┌────┴───┐
│ 3.3.1  │ │3.3.2  │ │3.3.3 │ │ 3.3.4  │
│ Term 1 │ │Term 2 │ │Term 3│ │ Term 4 │
└────────┘ └───────┘ └──┬───┘ └────────┘
           ┌────────────┼────────────┐
      ┌────┴────┐  ┌────┴────┐  ┌────┴────┐
      │ 3.3.3.1 │  │ 3.3.3.2 │  │ 3.3.3.3 │
      │ Term 5  │  │ Term 6  │  │ Term 7  │
      └─────────┘  └─────────┘  └─────────┘
```

Fig. 1 Numbering of terms within the concept (example)

```
          ┌─────────────────┐
          │      3.3        │
          │  Concept no 3   │
          └────────┬────────┘
     ┌─────────┬───┴────┬──────────┐
┌────┴───┐ ┌───┴───┐ ┌──┴───┐ ┌────┴───┐
│ 3.3.1  │ │3.3.2  │ │3.3.3 │ │ 3.3.7  │
│ Term 1 │ │Term 2 │ │Term 3│ │ Term 7 │
└────────┘ └───────┘ └──┬───┘ └────────┘
           ┌────────────┼────────────┐
      ┌────┴────┐  ┌────┴────┐  ┌────┴────┐
      │ 3.3.4   │  │ 3.3.5   │  │ 3.3.6   │
      │ Term 4  │  │ Term 5  │  │ Term 6  │
      └─────────┘  └─────────┘  └─────────┘
```
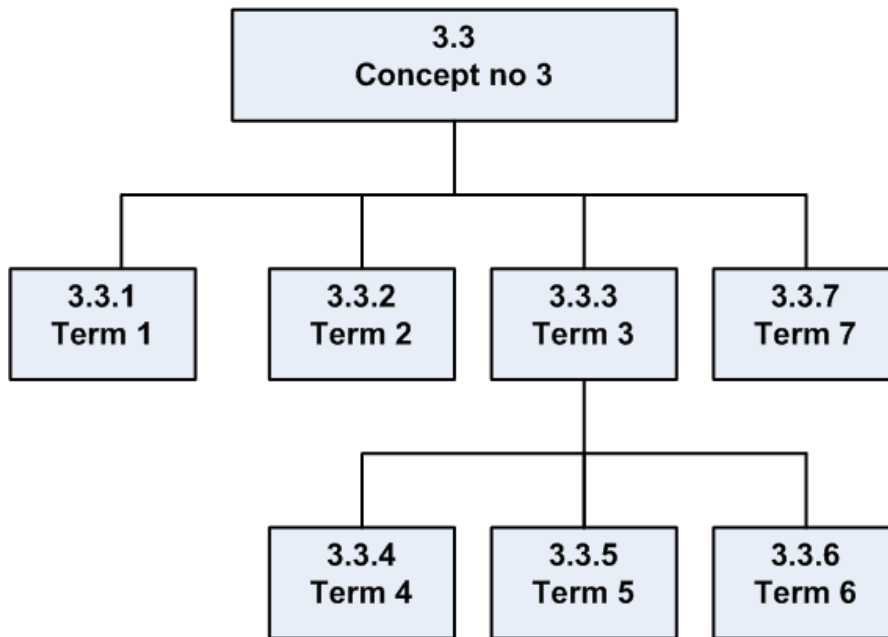
Fig. 2 Numbering of terms within the concept (2. example)

It is recommended[2] to minimize the number of concepts to produce a clear picture of relationships inside one concept map and limit cross-relations between concepts.

Although the systematic approach is used in ISO standards for terminology presentation for many years (see, for example, ISO/IEC 9000, to name the most eminent one, in my opinion) it has not been applied in SC27 documents yet. However, when one considers:

---

[2] ISO/IEC 704:2009, Principles and methods

- the complexity of the IT security evaluation domain which resulted in hundreds of terms, often used in a different context than usual dictionary meaning,
- deep revision of 15408 & 18045 set of standards currently underway,
- needs for opening the Common Criteria world for new users, new applications, new technologies, and new evaluation techniques, and simultaneously, legacy needs for preserving current applications (existing evaluation and certification schemes with their practices, skills and experience),
- new regulatory/ legal frameworks, like European cybersecurity certification framework[3],

clear request for working out the terminology issue is emerging (if not now – when?, In not us – who?).

Therefore, by identifying concepts and re-arrange the current presentation of terms in ISO/IEC 15408 part 1 we could meet the challenges as described above and:

- fulfil the ISO requirements for correct presentation of terms,
- clarify terms and their definitions in the ICT security evaluation context, and consequently
  o identify and then remove from Clause 3 these terms which are not necessary to define,
  o improve current definitions (e.g. shortening them or removing circular references among several definitions).

Concept approach introduction to ISO/IEC 15408-1/18045

To achieve a complete systematic order with regards to all terms finally included in Clause 3 of ISO/IEC 15408-1 an action plan is proposed with the following prerequisites:

1. Clause 3 of ISO/IEC CD 15408-1 contains all terms in alphabetical order; experts can comment on the content, and regular housekeeping work is being done;
2. In parallel, a Study Period is set up for developing the concept system and reordering the set of terms by assigning them to relevant concepts;

Identification of concepts and terms mapping

A set of concepts has been evaluated to encompass potentially all terms defined currently in ISO/IEC 3rd CD 15408-1. Following concepts have been established:

1. Security model
2. Target ofevaluation, TOE
3. Assurance
4. Evaluation verb
5. Lifecycle
6. Vulnerability
7. Composition
8. Taxonomy

---

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505737096808&uri=CELEX:52017PC0477

Relevant terms have been assigned to concepts by analyzing respective definitions. As a result, several maps of relationships between terms are presented in following subchapters. Each map is accompanied by the table containing terms and their definitions.

The complete list of terms, their definitions and current status with regards to the concept assignments are presented in the table located at the end of this Annex.

It is worth to note some maps contain not defined terms. It is not necessary a fault, nor a proof of incompleteness. The term is not to be defined if used in common, dictionary meaning however it could be indispensable for completeness of the concept map. Such terms are indicated in red font. Finally, if we have any doubt with assigning particular terms, it appears in a yellow box.

Request for comments

It is not claimed the maps for the respective concepts are complete and fully correct. All presented concepts and their maps are subject to modifications and improvements.

Experts are requested to provide their comments on concepts identification, terms assigning and consistency of all maps.

Concept approach to he ISO/IEC 3rdCD 15408 (all parts) & ISO/IEC 3rdCD 18045 Terminology

Concept maps

1. Security model
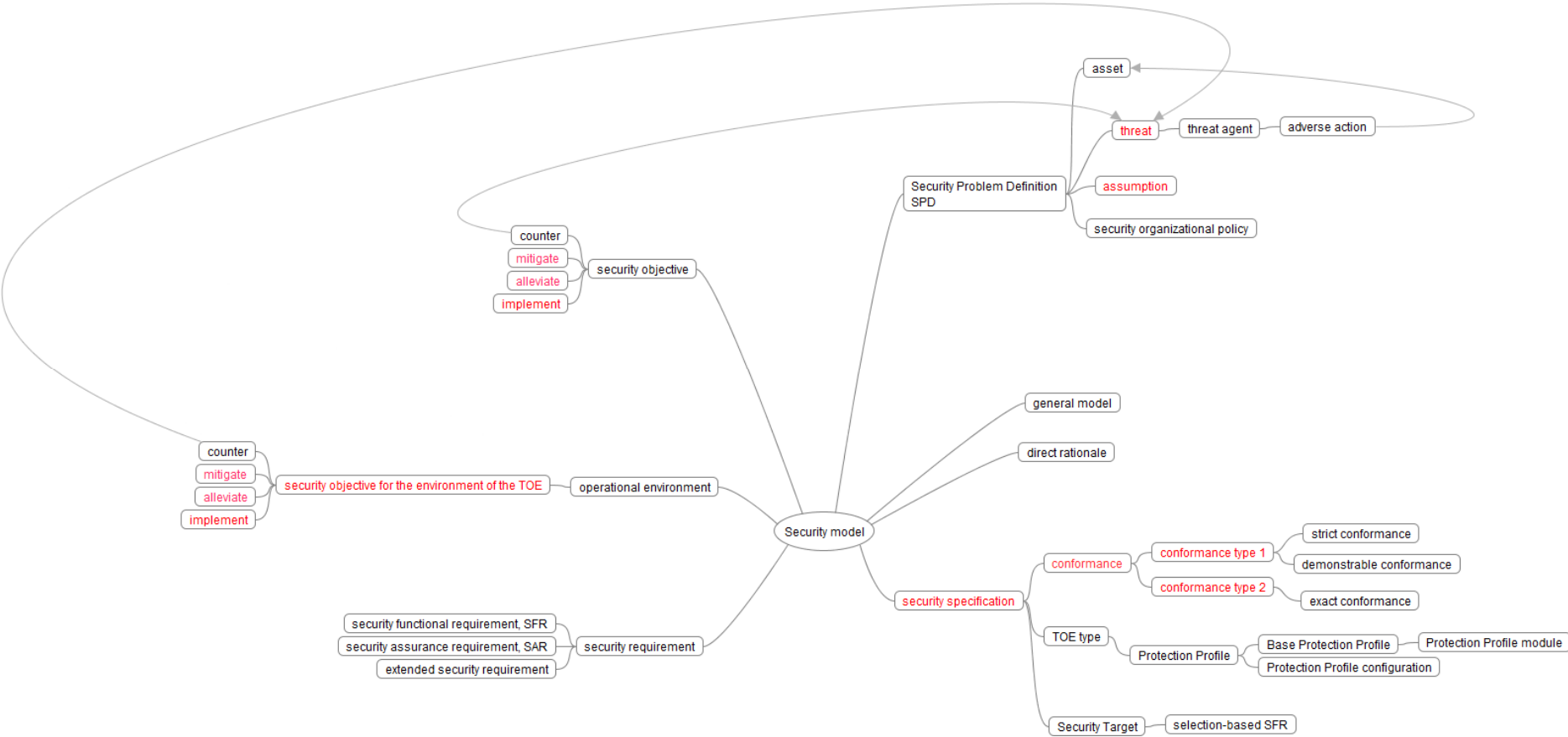
Fig. 3 Concept map for 'security model'

2. Target of Evaluation, TOE
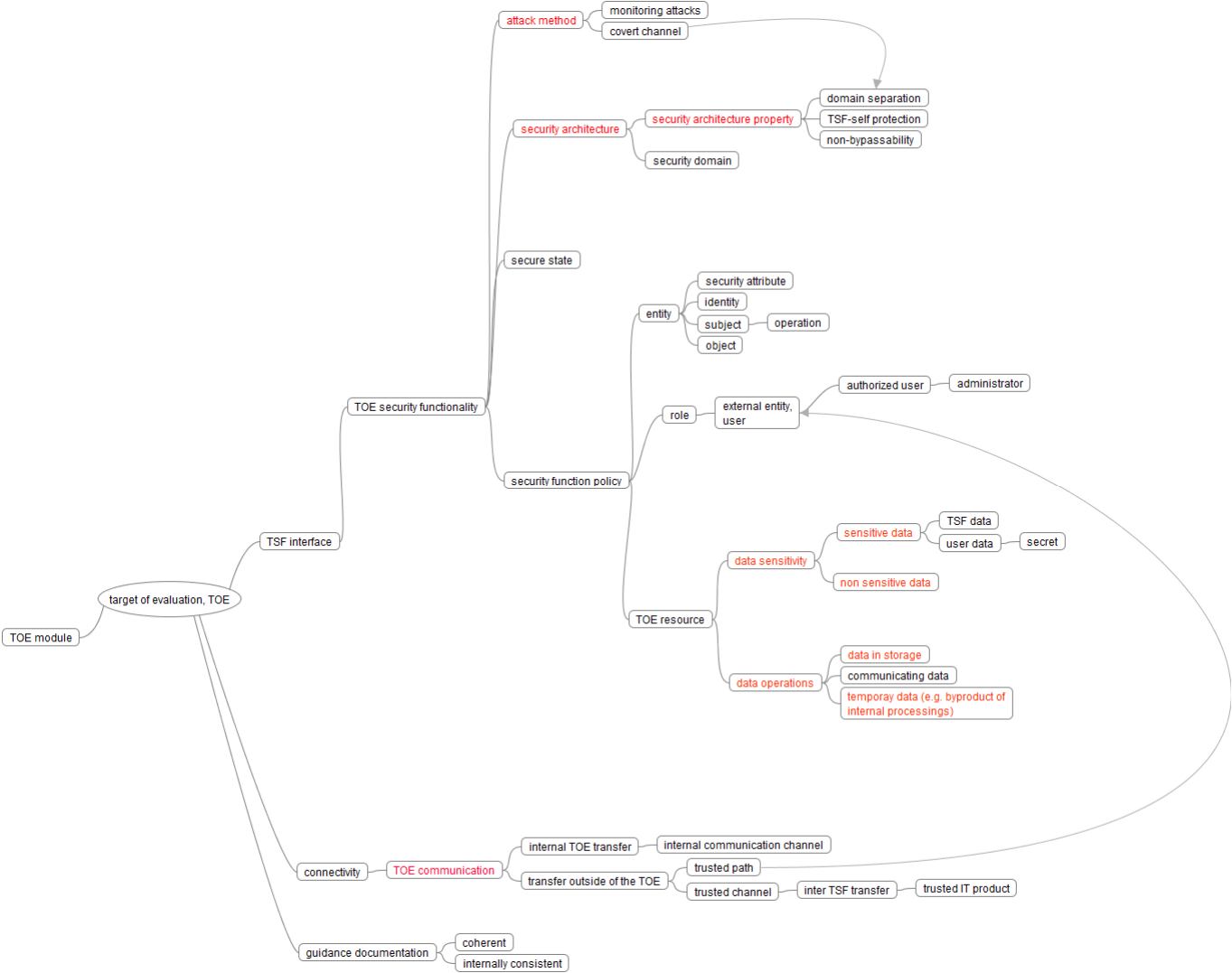
Fig. 4 Concept map for 'TOE'

3. Assurance
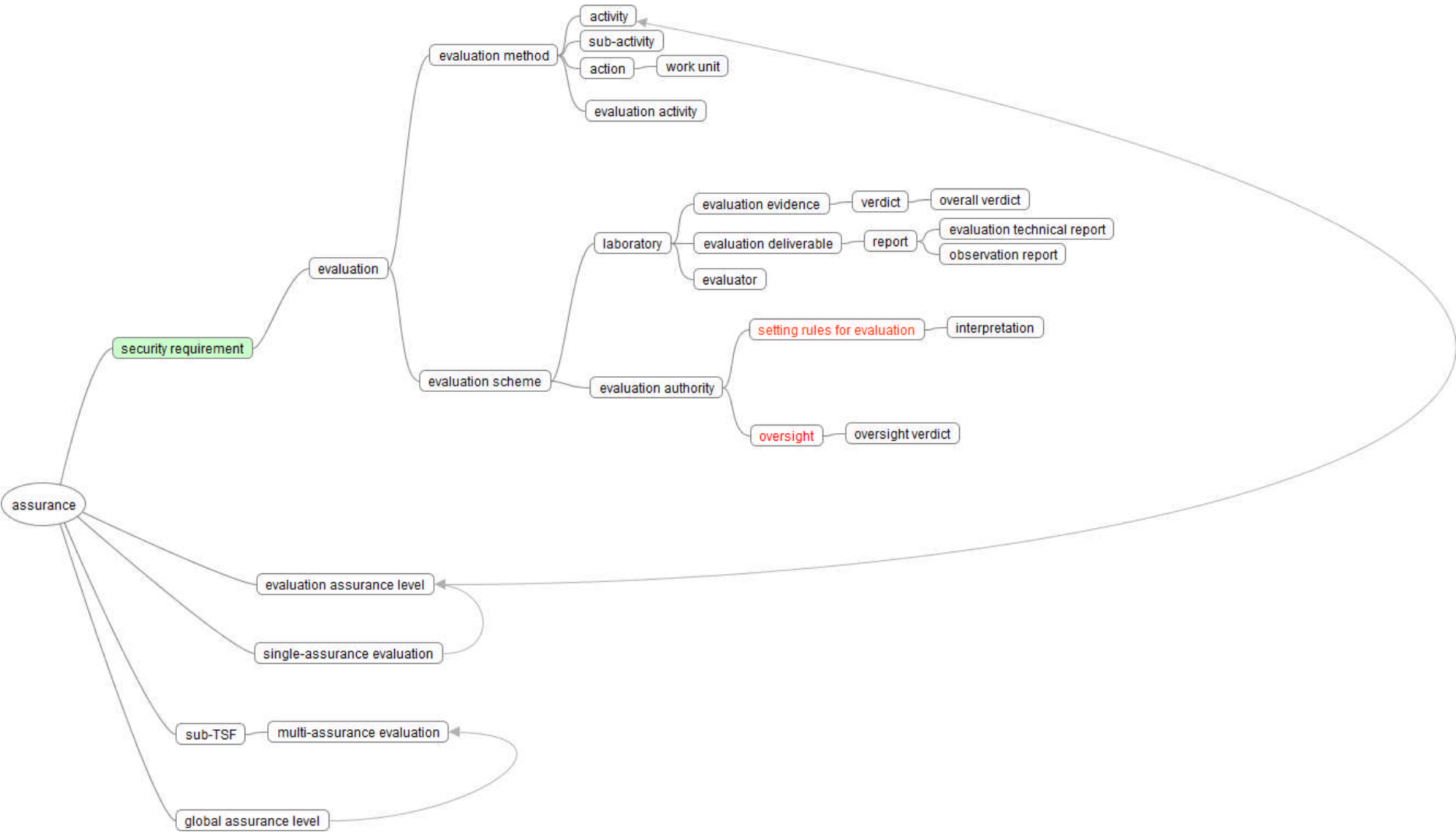
Fig. 5 Concept map for 'assurance'

4. Evaluation verb

Fig. 6 Concept map for 'evaluation verb'

5. Life cycle

Fig. 7 Concept map 'life cycle'

6. Vulnerability analysis

Fig. 8 Concept map for 'vulnerability analysis'

7. Composite evaluation

Fig. 9 Concept map for 'composite evaluation'

8. Taxonomy
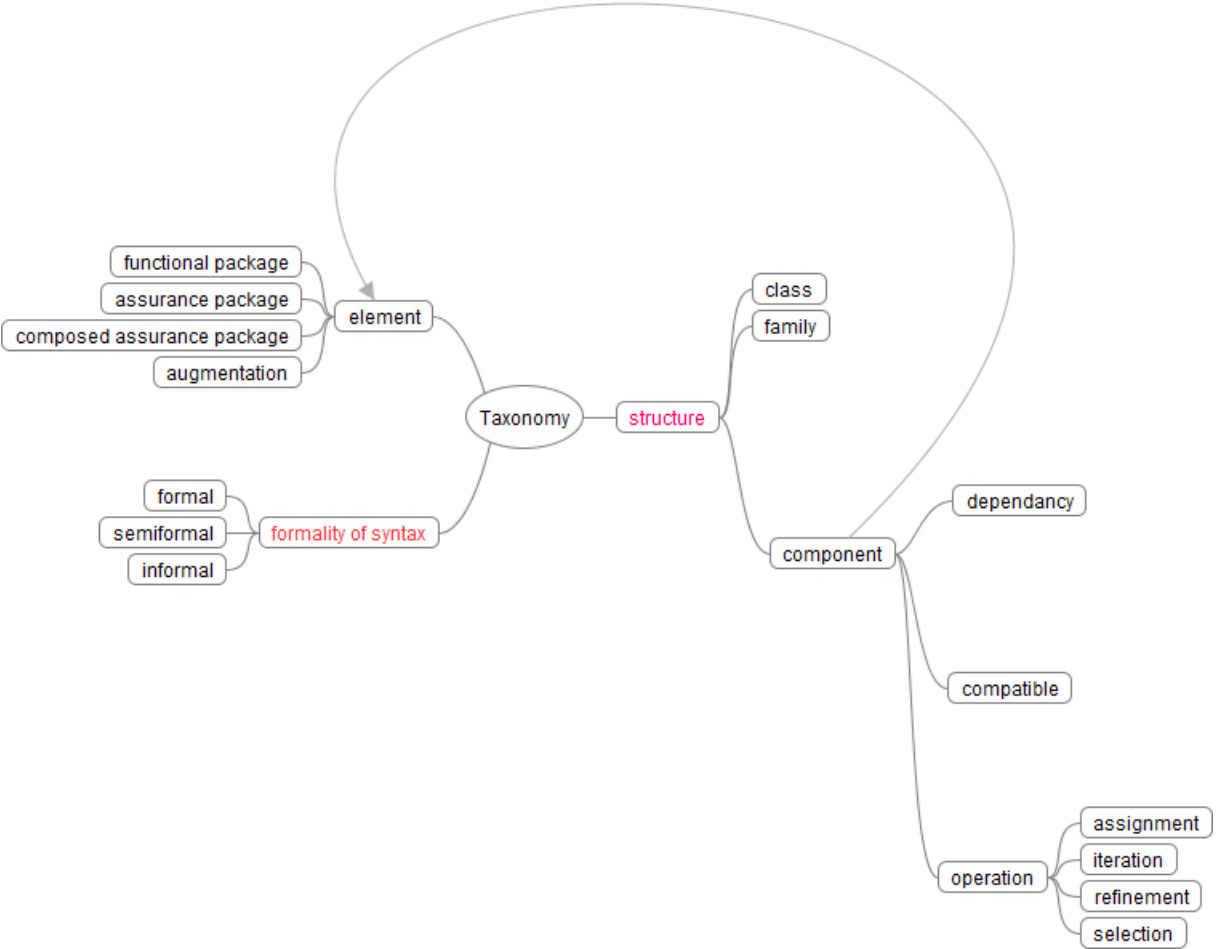
Fig. 10 Concept map for 'taxonomy'

Terms and Definitions per concept map

1. Security model

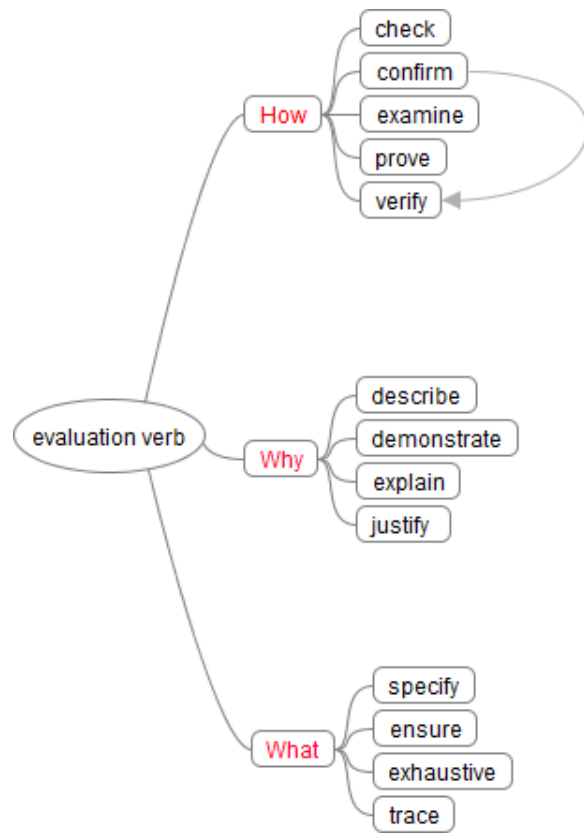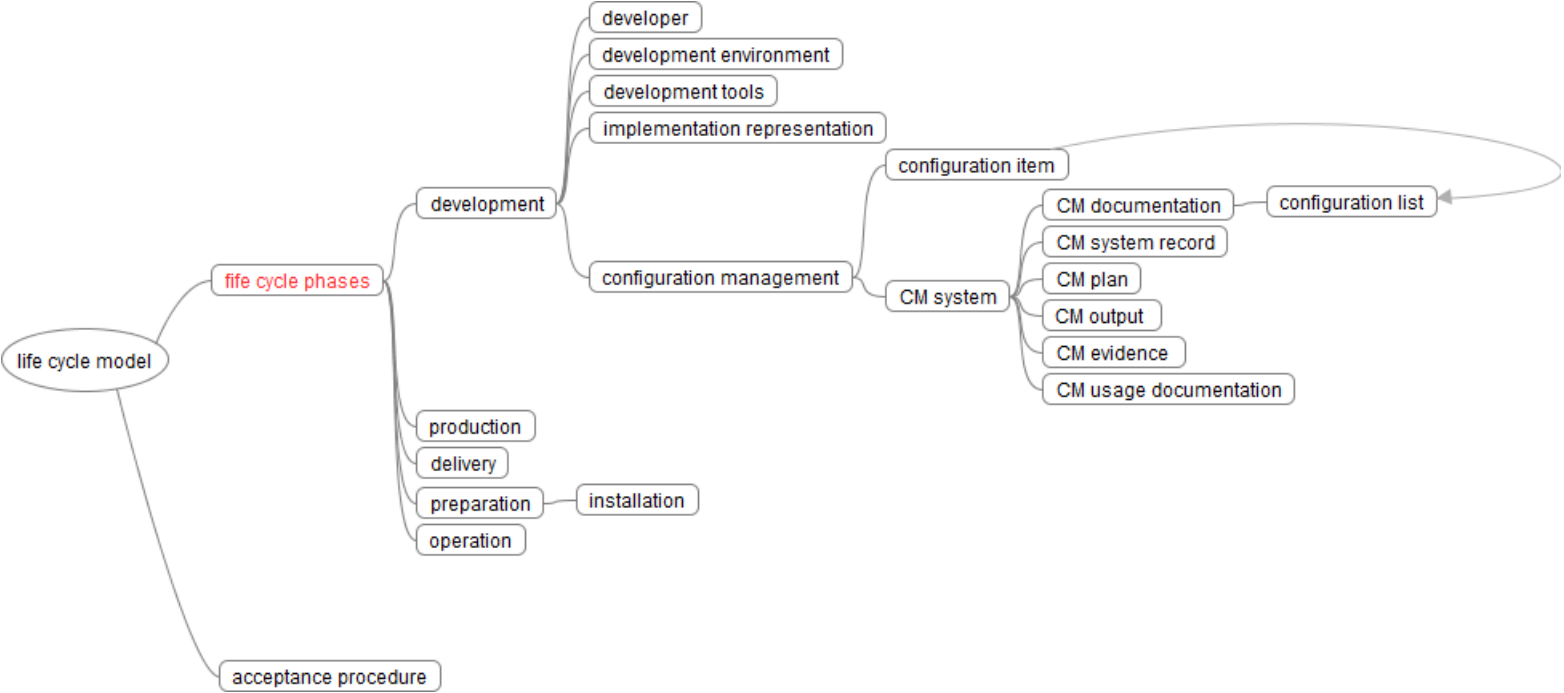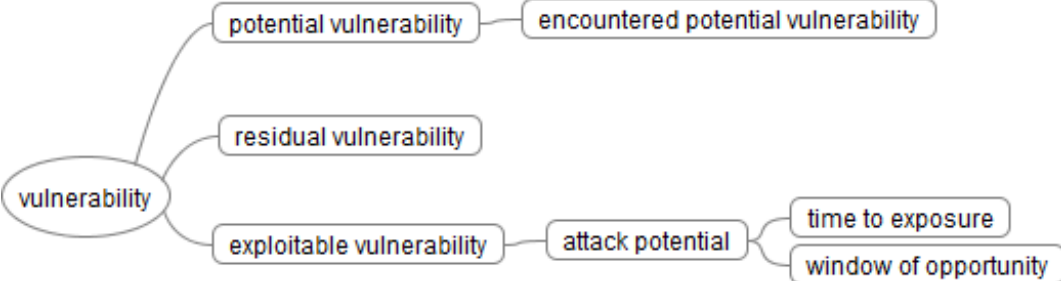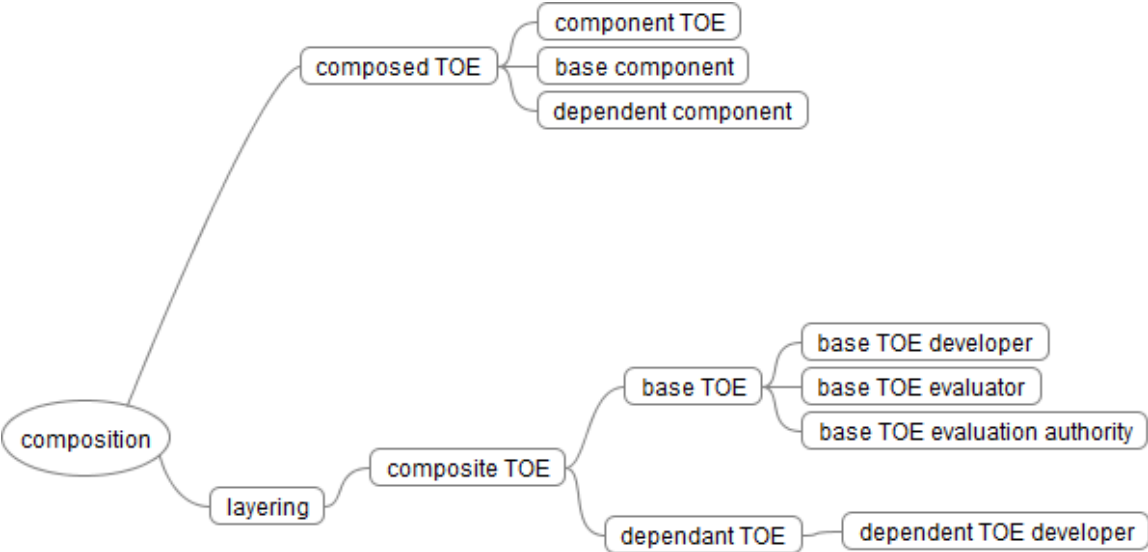| ID_conc	Term	Current definition	Concept
1.	general model	type of Protection Profile or Security Target in which the SPD-elements of the SPD are mapped to the Security Objectives for the TOE and to the Security Objectives for the operational environment. Note 1 to entry: SFRs in the general model have to cover all security objectives for the TOE.	security model
2.	direct rationale	type of Protection Profile or Security Target in which the threats and organisational security policies in the SPD are mapped directly to the SFRs and possibly security objectives for the operational environment Note 1 to entry: Direct rationale does not include security objectives for the TOE. Note 2 to entry: Direct rationale is simpler solution than mapping via a set of TOE security objectives.	security model
3.	security problem security problem definition SPD	statement which in a formal manner defines the nature and scope of the security that the TOE 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, the OSPs enforced by the TOE and its operational environment, and the assumptions that are upheld for the operational environment of the TOE.	security model
4.	Asset	entity that the owner of the TOE presumably places value upon	security model
5.	threat agent	entity that can exercise adverse actions on assets protected by the TOE	security model
6.	adverse action	action performed by a threat agent on an asset	security model
7.	organizational security policy OSP	set of security rules, procedures, or guidelines for an organization Note 1 to entry: A policy may pertain to a specific operational environment.	security model

ID_conc	Term	Current definition	Concept
8.	security objective	statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions	security model
9.	counter, verb	act on or respond to a particular threat so that the threat is eradicated or mitigated	security model
10.	security requirement	requirement, stated in a 15408a standardized language, which is part of a TOE security specification as defined in a specific ST or in a PP.	security model
11.	security functional requirement, SFR	security requirement, which contributes to fulfil the TOE's Security Problem Definition (SPD) as defined in a specific ST or in a PP	security model
12.	security assurance requirement, SAR	security requirement, which refers to the conditions and processes such as specification, design, development, and delivery under which the TOE is developed and configured before being accepted by its final user	security model
13.	extended security requirement	security requirement developed according to the rules given in ISO/IEC 15408 but that is not specified in any part of ISO/IEC 15408 Note 1 to entry: An extended security requirement may be either an SAR or an SFR. Note 2 to entry: Extended security requirements are defined within extended component definitions.	security model
14.	operational environment	environment in which the TOE is operated	security model
15.	TOE type	set of TOEs that have common characteristics Note 1 to entry: The TOE type may be more explicitly defined in a PP.	security model
16.	Protection Profile PP	implementation-independent statement of security needs for a TOE type	security model
17.	base Protection Profile base PP	Protection Profile specified in a PP-Module used as a basis to build a Protection Profile Configuration	security model
18.	Protection Profile module PP-Module	implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles	security model

ID_conc	Term	Current definition	Concept
19.	Protection Profile configuration PP-Configuration	Protection Profile composed of Base Protection Profile(s) and Protection Profile module(s)	security model
20.	security target, ST	implementation-dependent statement of security requirements for a TOE based on a security problem definition	security model
21.	selection-based Security Functional Requirement selection-based SFR	SFR in a Protection Profile that contributes to a stated aspect of the PP's security problem definition that shall is to be included in a conformant ST if a selection choice identified in the PP indicates that it has an associated selection-based SFR	security model
22.	strict conformance	hierarchical relationship between a PP and an ST where all the requirements in the PP also exist in the ST Note 1 to entry: This relation can be paraphrased as "the ST shall contain all statements that are in the PP, but may contain more". Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner.	security model
23.	demonstrable conformance	relation between a ST and a PP, where the ST provides an equivalent or more restrictive solution which solves the generic security problem in the PP	security model
24.	exact conformance	hierarchical relationship between a PP and an ST where all the requirements in the ST are drawn only from the PP Note 1 to entry: an ST is allowed to claim exact conformance to one or more PPs and/or PP configurations.	security model

2. Target ofevaluation, TOE

ID_conc	Term	Current definition	Concept
1.	target of evaluation TOE	set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation	TOE
2.	TSF interface TSFI	means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF,	TOE
3.	TOE security functionality TSF	combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs	TOE
4.	sub-TSF (TSF part)	notion applied in multi-assurance evaluation to denote a portion of the TSF that provides a well-defined subset of security functionality, which corresponds to a set of SFRs that is closed by dependencies, objectives, and SPD elements. Note 1 to entry: a sub-TSF has the characteristics of a TSF . Note 2 to entry: a sub-TSF is associated with its own assurance package	TOE
5.	security function policy	set of rules describing specific security behaviour enforced by the **TSF** and expressible as a set of **SFRs**	TOE
6.	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	TOE
7.	security attribute	property of subjects, users, objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs Note 1 to entry: Users can include external IT products.	TOE
8.	Identity	representation uniquely identifying an entity within the context of the TOE EXAMPLE An example of such a representation is a string. Note 1 to entry: entities can be diverse such as a user, process, or disk. For a human user, the representation could be the full or abbreviated name or a unique pseudonym. Note 2 to entry: An entity can have more than one identity.	TOE

ID_conc	Term	Current definition	Concept
9.	Subject	entity in the TOE that performs operations on objects	TOE
10.	Object	entity in the TOE, that contains or receives information, and upon which subjects perform operations	TOE
11.	Operation	⟨on an object⟩ specific type of action performed by a subject on an object	TOE
12.	Role	predefined set of rules establishing the allowed interactions between a user and the TOE	TOE
13.	external entity user	human, technical system or one of its components interacting with the TOE from outside of the TOE boundary	TOE
14.	authorized user	TOE user who may, in accordance with the SFRs, perform an operation	TOE
15.	Administrator	entity that has a level of trust with respect to all policies implemented by the TSF Note 1 to entry: Not all PPs or STs assume the same level of trust for administrators. Typically, administrators are assumed to adhere at all times to the policies in the ST of the TOE. Some of these policies may be related to the functionality of the TOE, others may be related to the operational environment.	TOE
16.	TOE resource	anything useable or consumable in the TOE	TOE
17.	TSF data	data for the operation of the TOE upon which the enforcement of the SFR relies	TOE
18.	user data	data received or produced by the TOE, which is meaningful to some external entity but which do not affect the operation of the TSF Note 1 to entry: Depending of the concept, this definition assumes that the same data created by users that has an actual impact on the operation of the TSF can be regarded as the TSF data.	TOE
19.	Secret	information that shall be known only to authorised users and/or the TSF in order to enforce a specific SFP	TOE
20.	secure state	state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs	TOE
21.	security domain	environment provided by the TSF for the use by untrusted entities in such a way that the environment is isolated and protected from other environments	TOE

ID_conc	Term	Current definition	Concept
22.	domain separation	security architecture property whereby the TSF defines separate security domains for each user and for the TSF and ensures that no user process can affect the contents of a security domain of another user or of the TSF	TOE
23.	TSF-self protection	security architecture property whereby the TSF cannot be corrupted by non-TSF code or entities	TOE
24.	non-bypassability	⟨of the TSF⟩ security architecture property whereby all SFR-related actions are mediated by the TSF	TOE
25.	monitoring attacks	generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds to the guidance documents	TOE
26.	covert channel	enforced, illicit signalling channel that allows a user to surreptitiously contravene the multi-level separation policy and unobservability requirements of the TOE	TOE
27.	Connectivity	property of the TOE allowing interaction with IT entities external to the TOE Note 1 to entry: This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.	TOE
28.	internal TOE transfer	communicating data between separated parts of the TOE	TOE
29.	internal communication channel	communication channel between separated parts of the TOE	TOE
30.	transfer outside of the TOE	TSF mediated communication of data to entities not under the control of the TSF	TOE

ID_conc	Term	Current definition	Concept
31.	trusted path	means by which a user and a TSF can communicate with the necessary confidence Note 1 to entry: Communication typically implies the establishment of identification and authentication of both parties, as well as the concept of a user specific session which is integrity-protected. Note 2 to entry: When the external entity is a trusted IT product, the notion of trusted channel is used instead of trusted path. Note 3 to entry: Both physical and logical aspects of secure communication can be considered as mechanisms for gaining confidence.	TOE
32.	trusted channel	means by which a TSF and another trusted IT product can communicate with necessary confidence	TOE
33.	inter TSF transfer	communicating data between the TOE and the security functionality of other trusted IT products	TOE
34.	trusted IT product	IT product, other than the TOE, which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly EXAMPLE An IT product that has been separately evaluated.	TOE
35.	guidance documentation	documentation that describes the delivery, preparation, operation, management and/or use of the TOE	TOE
36.	Coherent	logically ordered and having discernible meaning Note 1 to entry: For documentation, this term addresses both the actual text and the structure of the document, in terms of whether it is understandable by its target audience.	TOE

ID_conc	Term	Current definition	Concept
37.	internally consistent	no apparent contradictions exist between any aspects of an entity 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.	TOE
38.	module TOE Module	small architectural unit that can be characterized in terms of the properties discussed in TSF internals (ADV_INT)	TOE

3. Assurance

ID_conc	Term	Current definition	Concept
1.	Assurance	grounds for confidence that a TOE meets the SFRs	assurance
2.	Evaluation	assessment of a PP, an ST or a TOE, against defined criteria	assurance
3.	evaluation method	set of one or more evaluation activities that are derived from ISO/IEC 18045 work units for application in a specific context	assurance
4.	Activity	application of an assurance class of ISO/IEC 15408-3	assurance
5.	sub-activity	application of an assurance component of ISO/IEC 15408-3 Note 1 to entry: Assurance families are not explicitly addressed in this International Standard because evaluations are conducted on a single assurance component from an assurance family	assurance
6.	Action	evaluator action element of ISO/IEC 15408-3 NOTE to entry: These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.	assurance
7.	work unit	most granular level of evaluation work	assurance
8.	evaluation activity EA	activities derived from work units defined in ISO/IEC 18045 Note 1 to entry: The concept of evaluation activities, and the combination of evaluation activities into "evaluation methods", is defined in ISO/IEC 15408-4.	assurance

ID_conc	Term	Current definition	Concept
9.	Record	<evaluation verb> retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time	assurance
10.	evaluation scheme	rules, procedures, and management to carrying evaluations of IT products security implementing all parts of ISO/IEC 15408 Note 1 to entry: Administrative and regulatory framework is usually a part of an evaluation scheme. Such framework is out of the scope of ISO/IEC 15408. Note 2 to entry: The objective of evaluation scheme is to ensure that high standards of competence and impartiality are maintained and a consistency of evaluations is achieved. Note 3 to entry: Evaluation scheme is usually established by an evaluation authority, which defines the evaluation environment, including criteria and methodology required to conduct IT security evaluations.	assurance
11.	Laboratory	organization with a management system providing evaluation and or testing work in accordance with a defined set of policies and procedures and utilizing a defined methodology for testing or evaluating the security functionality of IT products Note 1 to entry: These organizations are often given alternative names by various approval authorities. For example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF). [SOURCE ISO/IEC DIS 19896-1 ,3.7]	assurance
12.	evaluation evidence	item used as a basis for establishing the verdict of an evaluation activity	assurance

ID_conc	Term	Current definition	Concept
13.	Verdict	pass, fail or inconclusive statement issued by an evaluator with respect to an ISO/IEC 15408 evaluator action element, assurance component, or class Note 1 to entry: The statement can be presented as: pass, fail or inconclusive. Note 2 to entry: Also see overall verdict.	assurance
14.	overall verdict	pass or fail statement issued by an evaluator with respect to the result of an evaluation Note 1 to entry: The statement can be expressed as "pass" or "fail".	assurance
15.	evaluation deliverable	any resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities	assurance
16.	Report	<evaluation verb> include evaluation results and supporting material in the evaluation technical report or an observation report	assurance
17.	evaluation technical report	documentation of the overall verdict and its justification, produced by the evaluator and submitted to an evaluation authority	assurance
18.	observation report	report written by the evaluator requesting a clarification or identifying a problem during the evaluation	assurance
19.	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 ISO/IEC 15408 (all parts) with the associated evaluation methodology given in ISO/IEC 18045 SOURCE: ISO/IEC 19896-1:2018	assurance

ID_conc	Term	Current definition	Concept
20.	evaluation authority	body operating an evaluation scheme Note 1 to entry: By applying the evaluation scheme evaluation authority sets the standards and monitors the quality of evaluations conducted by bodies within a specific community.	assurance
21.	Interpretation	clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045 or scheme requirement	assurance
22.	oversight verdict	statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities	assurance
23.	single- assurance evaluation	evaluation using a single set of assurance requirements	assurance
24.	evaluation assurance level EAL	well formed package of assurance requirements defined in ISO/IEC 15408-3 and drawn from ISO/IEC 15408-3, representing a point on the ISO/IEC 15408 predefined assurance scale, that form an assurance package	assurance
25.	multi-assurance evaluation	evaluation where the TOE is organised in parts, each part being associated with its own assurance package	assurance
26.	sub-TSF	combined functionality of all hardware, software, and firmware of a TOE that are relied upon for the correct enforcement of the SFRs defined in one PP-Configuration component Note 1 to entry: This set of SFRs is closed by dependencies, objectives, and SPD 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 STs. It can be used in the single-assurance approach but it must be used in the multi-assurance approach: sub-TSFs must be defined in a multi-assurance PP-Configuration and in conformant STs. Note 3 to entry: each sub-TSF is associated with its own set of SARs in a multi-assurance PP-Configuration. In the rest of the document, a set of SARs may be an assurance package. Note 4 to entry: a sub-TSF has the characteristics of a TSF.	assurance
27.	global assurance level	set of assurance requirements drawn from CC Part 3 that are to be applied to the entire TSF in a multi-assurance evaluation.	assurance

4. Evaluation verb

ID_conc	Term	Current definition	Concept
1.	Check	<evaluation verb> generate a verdict by a simple comparison NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped.	evaluation verb
2.	Confirm	<evaluation verb> declare that something has been reviewed in detail with an independent determination of sufficiency Note 1 to entry: The level of rigour required depends on the nature of the subject matter	evaluation verb
3.	Examine	<evaluation verb> generate a verdict by analysis using evaluator expertise Note 1 to entry: The statement that uses this verb identifies what is analysed and the properties for which it is analysed.	evaluation verb
4.	Determine	<evaluation verb> affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion Note 1 to entry: The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms "confirm" or "verify" which imply that an analysis has already been performed which needs to be reviewed	evaluation verb
5.	Verify	<evaluation verb> rigorously review in detail with an independent determination of sufficiency Note 1 to entry: Also see "confirm". This term has more rigorous connotations. The term "verify" is used in the context of evaluator actions where an independent effort is required of the evaluator.	evaluation verb
6.	Prove	<evaluation verb> show correspondence by formal analysis in its mathematical sense Note 1 to entry: It is completely rigorous in all ways. Typically, the term prove is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.	evaluation verb
7.	Describe	<evaluation verb> provide specific details of an entity	evaluation

25

ID_conc	Term	Current definition	Concept
8.	Demonstrate	<evaluation verb> provide a conclusion gained by an analysis which is less rigorous than a "proof"	verb evaluation verb
9.	Explain	<evaluation verb> give argument accounting for the reason for taking a course of action Note 1 to entry: This term differs from both "describe" and "demonstrate". It is intended to answer the question "Why?" without actually attempting to argue that the course of action that was taken was necessarily optimal.	evaluation verb
10.	Justify	<evaluation verb> provide a rationale providing sufficient reason Note 1 to entry: The term 'justify' is more rigorous than a 'demonstrate'. This term requires significant rigour in terms of very carefully and thoroughly explaining every step of a logical analysis leading to a conclusion.	evaluation verb
11.	Specify	<evaluation verb> provide specific details about an entity in a rigorous and precise manner	evaluation verb
12.	Ensure	<evaluation verb> guarantee a strong causal relationship between an action and its consequences Note 1 to entry: When this term is preceded by the word "help" it indicates that the consequence is not fully certain, on the basis of that action alone.	evaluation verb
13.	Exhaustive	<evaluation verb> characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan Note 1 to entry: This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is related to "systematic" but is considerably stronger, in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to ensure that all possible avenues have been exercised.	evaluation verb

ID_conc	Term	Current definition	Concept
14.	Trace	<evaluation verb> simple directional relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second	evaluation verb

5. Lifecycle

No_conc	Term	Current definition	Concept
1.	life cycle model	framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a product, spanning the life of the system from the definition of its requirements to the termination of its use Note 1 to entry: See also Figure 1. [SOURCE: ISO/IEC/IEEE 24765:2010 3.1587 modified, note 1 to entry added]	life cycle
2.	Development	product life-cycle phase which is concerned with generating the implementation representation of the TOE Note 1 to entry: Throughout the ALC: Life-cycle support requirements, development and related terms (developer, develop) are meant in the more general sense to comprise development and production.	life cycle
3.	Developer	organisation responsible for the development of the TOE	life cycle
4.	development environment	environment in which the TOE is developed Note 1 to entry: The conditions include physical facilities, security controls, IT systems and development tools.	life cycle
5.	development tools	tools (including test software, if applicable) supporting the development and production of the TOE EXAMPLE For a software TOE, development tools are usually programming languages, compilers, linkers and generating tools.	life cycle

No_conc	Term	Current definition	Concept
6.	implementation representation	least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement 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.	life cycle
7.	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	life cycle
8.	configuration item	item or aggregation of hardware, software, or both that is designated for configuration management and treated as a single entity in the configuration management process [during the TOE development] Note 1 to entry: These may be either parts of the TOE or objects related to the development of the TOE like evaluation documents or development tools. configuration mnagement items may be stored in the configuration mnagement system directly (for example files) or by reference (for example hardware parts) together with their version [SOURCE: ISO/IEC/IEEE 24765:2010 3.563 modified, specification of TOE development requirement and note 1 to entry added].	life cycle

No_conc	Term	Current definition	Concept
9.	configuration management system	set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of his products during their life-cycles Note 1 to entry: Configuration management systems may have varying degrees of rigour and function. At higher levels, configuration management systems may be automated, with flaw remediation, change controls, and other tracking mechanisms.	life cycle
10.	configuration management documentation CM documentation	all configuration mnagement documentation including configuration mnagement output, configuration mnagement list (configuration list), configuration mnagement system records,configuration mnagement plan andconfiguration mnagement usage documentation	life cycle
11.	configuration list	configuration management output document listing all configuration items for a specific product together with the exact version of each configuration management item relevant for a specific version of the complete product Note 1 to entry: This list allows distinguishing the items belonging to the evaluated version of the product from other versions of these items belonging to other versions of the product. The final configuration management list is a specific document for a specific version of a specific product. (Of course, the list can be an electronic document inside of a configuration management tool. In that case, it can be seen as a specific view into the system or a part of the system rather than an output of the system. However, for the practical use in an evaluation the configuration list will probably be delivered as a part of the evaluation documentation.) The configuration list defines the items that are under the configuration management requirements of ALC_CMC.	life cycle

No_conc	Term	Current definition	Concept
12.	configuration management system record	output produced during the operation of the configuration management system documenting important configuration management activities Note 1 to entry: Examples of configuration management system records are configuration management item change control forms or configuration management item access approval forms.	life cycle
13.	configuration management plan	description of how the configuration management system is used for the TOE Note 1 to entry: The objective of issuing a configuration management plan is that staff members can see clearly what they have to do. From the point of view of the overall configuration management system this can be seen as an output document (because it may be produced as part of the application of the configuration management system). From the point of view of the concrete project it is a usage document because members of the project team use it in order to understand the steps that they have to perform during the project. The configuration management plan defines the usage of the system for the specific product; the same system may be used to a different extent for other products. That means the configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE development.	life cycle
14.	configuration management output	results, related to configuration management, produced or enforced by the configuration management system Note 1 to entry: These configuration management related results could occur as documents (for example filled paper forms, configuration management system records, logging data, hard-copies and electronic output data) as well as actions (for example manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are configuration lists, configuration management plans and/or behaviours during the product life-cycle.	life cycle

No_conc	Term	Current definition	Concept
15.	configuration management tool	manually operated or automated tool realising or supporting a configuration management system EXAMPLE Tools for the version management of the parts of the TOE.	life cycle
16.	configuration management evidence	everything that may be used to establish confidence in the correct operation of the CM system EXAMPLE configuration mnagement output, rationales provided by the developer, observations, experiments or interviews made by the evaluator during a site visit	life cycle
17.	configuration management usage documentation	part of the configuration management system, which describes, how the configuration management system is defined and applied by using for example handbooks, regulations and/or documentation of tools and procedures	life cycle
18.	Production	life-cycle phase which follows the development phase and consists of transforming the implementation representation into the implementation of the TOE, i.e. into a state acceptable for delivery to the customer Note 1 to entry: This phase may comprise manufacturing, integration, generation, internal transports, storage, and labelling of the TOE.	life cycle
19.	Delivery	transmission of the finished TOE from the production environment into the hands of the customer Note 1 to entry: This product life-cycle phase may include packaging and storage at the development site, but does not include transportations of the unfinished TOE or parts of the TOE between different developers or different development sites.	life cycle
20.	Preparation	activity in the life-cycle phase of a product, comprising the customer's acceptance of the delivered TOE and its installation which may include such things as booting, initialisation, start-up and progressing the TOE to a state ready for operation	life cycle

No_conc	Term	Current definition	Concept
21.	Installation	procedure performed by a human user embedding the TOE in its operational environment and putting it into an operational state Note 1 to entry: This operation is performed normally only once, after receipt and acceptance of the TOE. The TOE is expected to be progressed to a configuration allowed by the ST. If similar processes have to be performed by the developer they are denoted as "generation" throughout ALC: Life-cycle support. If the TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as installation.	life cycle
22.	Operation	usage phase of the TOE including "normal usage", administration and maintenance of the TOE after delivery and preparationusage phase of the TOE including "normal usage", administration and maintenance of the TOE after delivery and preparation	life cycle
23.	acceptance procedure	procedure followed in order to accept newly created or modified configuration items as part of the TOE, or to move them to the next step of the life-cycle Note 1 to entry: These procedures identify the roles or individuals responsible for the acceptance and the criteria to be applied in order to decide on the acceptance. There are several types of acceptance situations some of which may overlap: a) acceptance of an item into the configuration management system for the first time, in particular inclusion of software, firmware and hardware components from other manufacturers into the TOE ("integration"); b) progression of configuration items to the next life-cycle phase at each stage of the construction of the TOE (e.g. module, subsystem, quality control of the finished TOE); c) subsequent to transports of configuration items (for example parts of the TOE or preliminary products) between different development sites; d) subsequent to the delivery of the TOE to the consumer; e) subsequent to the integration of the TOE.	life cycle

6. Vulnerability

ID_conc	Term	Current definition	Concept
1.	Vulnerability	weakness in the TOE that can be used to violate the SFRs in some environment	vulnerability analysis
2.	potential vulnerability	suspected, but not confirmed, weakness Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the SFRs.	vulnerability analysis
3.	encountered potential vulnerability	potential weakness in the TOE identified by the evaluator while performing evaluation activities that could be used to violate the SFRs	vulnerability analysis
4.	residual vulnerability	weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE	vulnerability analysis
5.	exploitable vulnerability	weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE	vulnerability analysis
6.	attack potential	measure of the effort needed to exploit a vulnerability in a TOE Note 1 to entry: The effort is expressed as a function of properties related to the attacker (for example, expertise, resources, and motivation) and properties related to the vulnerability itself (for example, window of opportunity, time to exposure).	vulnerability analysis
7.	time period to exposure	time interval when an element is participating in an IT system and could be attacked	vulnerability analysis
8.	window of opportunity	period of time that an attacker has access to the TOE	vulnerability analysis

7. Composition

No_conc	Term	Current definition	Concept
1.	base component	entity in a composed TOE, which has itself been the subject of an evaluation, providing services and resources to a dependent component	composition
2.	base TOE	TOE comprising the independent component(s) of a layered composite TOE	composition
3.	base TOE developer	entity developing the base TOE or sponsoring a base TOE evaluation	composition

No_conc	Term	Current definition	Concept
4.	base TOE evaluation authority	evaluation authority performing its tasks to evaluated the platform base TOE	composition
5.	base TOE evaluator	entity performing the base TOE evaluation	composition
6.	component TOE	successfully evaluated TOE that is part of another composed TOE	composition
7.	composed TOE	TOE comprised solely of two or more components that have been successfully evaluated	composition
8.	composite evaluation	evaluation of a composite TOE	composition
9.	composite product	product comprised of two or more components which can be be organized in two layers: a layer of independent base component(s) and a layer of dependent components Note 1 to entry: The composite evaluation can be applied as many times as necessary to a multi-component/multi-layered product, in an incremental approach. Note 2 to entry: Usually, the layer consisted of base components has already been successfully evaluated.	composition
10.	composite TOE	TOE composed of a superposition of two layers	composition
11.	dependent component	entity in a composed TOE, which is itself the subject of an evaluation, relying on the provision on services by a base component	composition
12.	dependent TOE	entity in a composed TOE which is itself the subject of an evaluation, relying on the provision on services by one or more base components Note 1 to entry: applies only to the "composed" evaluation approach (not to the composite approach).	composition

No_conc	Term	Current definition	Concept
13.	functional interface	external interface providing a user with access to functionality of the TOE which is not directly involved in enforcing security functional requirements Note 1 to entry: In a composed TOE these are the interfaces provided by the base component that are required by the dependent component to support the operation of the composed TOE.	composition
14.	Layering	design technique where separate groups of modules (the layers) are hierarchically organised to have separate responsibilities such that one layer depends only on layers below it in the hierarchy for services, and provides its services only to the layers above it Note 1 to entry: Strict layering adds the constraint that each layer receives services only from the layer immediately beneath it, and provides services only to the layer immediately above it.	composition

8. Taxonomy

ID_no	Term	Current definition	Concept
1.	Class	<taxonomy>set of ISO/IEC 15408 families that share a common focus	taxonomy
2.	Family	<taxonomy> set of components that share a similar goal but differ in emphasis or rigour	taxonomy
3.	Component	<taxonomy> smallest selectable set of elements on which requirements may be based	taxonomy
4.	Compatible	⟨component⟩ property of a component able to provide the services required by another component, through the corresponding interfaces of each component, in consistent operational environments	taxonomy
5.	Dependency	relationship between components such that a PP, ST or package including a component shall also include any other components that are identified as being depended upon or include a rationale as to why they are not	taxonomy
6.	Operation	⟨on an ISO/IEC 15408 component⟩ modification or repetition of a component by assignment, iteration, refinement, or selection	taxonomy
7.	Assignment	specification of an identified parameter in a functional element component of a given functional or assurance component Note 1 to entry: Such functional element is also called a requirement.	taxonomy
8.	Iteration	use of the same component to express two or more distinct requirements	taxonomy

35

ID_no	Term	Current definition	Concept
9.	Refinement	addition of details to a component	taxonomy
10.	Selection	specification of one or more items from a list in a component	taxonomy
11.	Element	<taxonomy> most detailed level of definition of a security need as defined in SFRs and SARs	taxonomy
12.	functional package	named set of security functional requirements that may be accompanied by an SPD and security objectives derived from that SPD	taxonomy
13.	assurance package	named set of security assurance requirements EXAMPLE "EAL 3".	taxonomy
14.	composed assurance package, CAP	assurance package consisting of components drawn predominately from the ACO class, representing a point on the pre-defined scale for composition assurance	taxonomy
15.	Augmentation	addition of one or more requirements to a package Note 1 to entry: in case of a functional package such augmentation is considered only in the context of one package, and is not considered in the context with other packages or PPs. Note 2 to entry: in case of an assurance package augmentation refers to one or more SAR.	taxonomy
16.	Tailoring	addition of one or more functional requirements to a functional package, and/or the addition of one or more selections to an SFR 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, PPs, or PP-Modules. Note 2 to entry: the selections in the SFR may 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.	taxonomy
17.	Formal	expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts	taxonomy
18.	Semiformal	expressed in a restricted syntax language with defined semantics	taxonomy
19.	Informal	expressed in natural language	taxonomy

ID_no	Term	Current definition	Concept
20.	Translation	describes the 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 SFR expressed in standardized language can also be translated back to the Security Objectives.	taxonomy

Terms in alphabetical order

Terms in order given in Clause 3 of ISO/IEC 3rdCD 15408-1 are presentd below.

ID_no	Term	Current definition	Concept
3.1	acceptance procedure	procedure followed in order to accept newly created or modified configuration items as part of the TOE, or to move them to the next step of the life-cycle Note 1 to entry: These procedures identify the roles or individuals responsible for the acceptance and the criteria to be applied in order to decide on the acceptance. There are several types of acceptance situations some of which may overlap: a) acceptance of an item into the configuration management system for the first time, in particular inclusion of software, firmware and hardware components from other manufacturers into the TOE ("integration"); b) progression of configuration items to the next life-cycle phase at each stage of the construction of the TOE (e.g. module, subsystem, quality control of the finished TOE); c) subsequent to transports of configuration items (for example parts of the TOE or preliminary products) between different development sites; d) subsequent to the delivery of the TOE to the consumer; e) subsequent to the integration of the TOE.	life cycle
3.2	action	evaluator action element of ISO/IEC 15408-3 NOTE to entry: These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.	assurance
3.3	activity	application of an assurance class of ISO/IEC 15408-3	assurance
3.4	administrator	entity that has a level of trust with respect to all policies implemented by the TSF Note 1 to entry: Not all PPs or STs assume the same level of trust for administrators. Typically, administrators are assumed to adhere at all times to the policies in the ST of the TOE. Some of these policies may be related to the functionality of the TOE, others may be related to the operational environment.	TOE
3.5	adverse action	action performed by a threat agent on an asset	security model
3.6	asset	entity that the owner of the TOE presumably places value upon	security model

ID_no	Term	Current definition	Concept
3.7	assignment	specification of an identified parameter in a functional element component of a given functional or assurance component Note 1 to entry: Such functional element is also called a requirement.	taxonomy
3.8	assurance	grounds for confidence that a TOE meets the SFRs	assurance
3.9	assurance package	named set of security assurance requirements EXAMPLE "EAL 3".	taxonomy
3.10	attack potential	measure of the effort needed to exploit a vulnerability in a TOE Note 1 to entry: The effort is expressed as a function of properties related to the attacker (for example, expertise, resources, and motivation) and properties related to the vulnerability itself (for example, window of opportunity, time to exposure).	vulnerability analysis
3.11	augmentation	addition of one or more requirements to a package Note 1 to entry: in case of a functional package such augmentation is considered only in the context of one package, and is not considered in the context with other packages or PPs. Note 2 to entry: in case of an assurance package augmentation refers to one or more SAR.	taxonomy
3.12	authorized user	TOE user who may, in accordance with the SFRs, perform an operation	TOE
3.13	base component	entity in a multi-componentcomposed TOE, which provides services and resources to one or more dependent component(s)	composition
3.14	base Protection Profile base PP	Protection Profile specified in a PP-Module used as a basis to build a Protection Profile Configuration	security model
3.15	base TOE	TOE comprising the independent component(s) of a layered composite TOE	composition
3.16	base TOE developer	entity developing the base TOE or sponsoring a base TOE evaluation	composition
3.17	base TOE evaluation authority	evaluation authority performing its tasks to evaluated the platform base TOE	composition
3.18	base TOE evaluator	entity performing the base TOE evaluation	composition
3.19	check	<evaluation verb> generate a **verdict b**y a simple comparison NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped.	evaluation verb
3.20	class	<taxonomy>set of ISO/IEC 15408 families that share a common focus	taxonomy

ID_no	Term	Current definition	Concept
3.21	coherent	logically ordered and having discernible meaning Note 1 to entry: For documentation, this term addresses both the actual text and the structure of the document, in terms of whether it is understandable by its target audience.	TOE
3.22	compatible	⟨component⟩ property of a component able to provide the services required by another component, through the corresponding interfaces of each component, in consistent operational environments	taxonomy
3.23	component	<taxonomy> smallest selectable set of elements on which requirements may be based	taxonomy
3.24	component TOE	successfully evaluated TOE that is part of another composed TOE	composition
3.25	composed assurance package, CAP	assurance package consisting of components drawn predominately from the ACO class, representing a point on the pre-defined scale for composition assurance	taxonomy
3.26	composed TOE	TOE comprised solely of two or more components that have been successfully evaluated	composition
3.27	composite evaluation	evaluation of a composite TOE	composition
3.28	composite product	product comprised of two or more components which can be be organized in two layers: a layer of independent base component(s) and a layer of dependent components Note 1 to entry: The composite evaluation can be applied as many times as necessary to a multi-component/multi-layered product, in an incremental approach. Note 2 to entry: Usually, the layer consisted of base components has already been successfully evaluated.	composition
3.29	composite TOE	TOE composed of a superposition of two layers	composition
3.30	configuration item	item or aggregation of hardware, software, or both that is designated for configuration management and treated as a single entity in the configuration management process [during the TOE development] Note 1 to entry: These may be either parts of the TOE or objects related to the development of the TOE like evaluation documents or development tools. configuration mnagement items may be stored in the configuration mnagement system directly (for example files) or by reference (for example hardware parts) together with their version [SOURCE: ISO/IEC/IEEE 24765:2010 3.563 modified, specification of TOE development requirement and note 1 to entry added].	life cycle

ID_no	Term	Current definition	Concept
3.31	configuration list	configuration management output document listing all configuration items for a specific product together with the exact version of each configuration management item relevant for a specific version of the complete product Note 1 to entry: This list allows distinguishing the items belonging to the evaluated version of the product from other versions of these items belonging to other versions of the product. The final configuration management list is a specific document for a specific version of a specific product. (Of course, the list can be an electronic document inside of a configuration management tool. In that case, it can be seen as a specific view into the system or a part of the system rather than an output of the system. However, for the practical use in an evaluation the configuration list will probably be delivered as a part of the evaluation documentation.) The configuration list defines the items that are under the configuration management requirements of ALC_CMC.	life cycle
3.32	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	life cycle
3.33	configuration management documentation CM documentation	all configuration mnagement documentation including configuration mnagement output, configuration mnagement list (configuration list), configuration mnagement system records,configuration mnagement plan andconfiguration mnagement usage documentation	life cycle
3.34	configuration management evidence	everything that may be used to establish confidence in the correct operation of the CM system EXAMPLE configuration mnagement output, rationales provided by the developer, observations, experiments or interviews made by the evaluator during a site visit	life cycle

ID_no	Term	Current definition	Concept
3.35	configuration management output	results, related to configuration management, produced or enforced by the configuration management system Note 1 to entry: These configuration management related results could occur as documents (for example filled paper forms, configuration management system records, logging data, hard-copies and electronic output data) as well as actions (for example manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are configuration lists, configuration management plans and/or behaviours during the product life-cycle.	life cycle
3.36	configuration management plan	description of how the configuration management system is used for the TOE Note 1 to entry: The objective of issuing a configuration management plan is that staff members can see clearly what they have to do. From the point of view of the overall configuration management system this can be seen as an output document (because it may be produced as part of the application of the configuration management system). From the point of view of the concrete project it is a usage document because members of the project team use it in order to understand the steps that they have to perform during the project. The configuration management plan defines the usage of the system for the specific product; the same system may be used to a different extent for other products. That means the configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE development.	life cycle
3.37	configuration management system	set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of his products during their life-cycles Note 1 to entry: Configuration management systems may have varying degrees of rigour and function. At higher levels, configuration management systems may be automated, with flaw remediation, change controls, and other tracking mechanisms.	life cycle
3.38	configuration management system record	output produced during the operation of the configuration management system documenting important configuration management activities Note 1 to entry: Examples of configuration management system records are configuration management item change control forms or configuration management item access approval forms.	life cycle

ID_no	Term	Current definition	Concept
3.39	configuration management tool	manually operated or automated tool realising or supporting a configuration management system EXAMPLE Tools for the version management of the parts of the TOE.	life cycle
3.40	configuration management usage documentation	part of the configuration management system, which describes, how the configuration management system is defined and applied by using for example handbooks, regulations and/or documentation of tools and procedures	life cycle
3.41	confirm	<evaluation verb> declare that something has been reviewed in detail with an independent determination of sufficiency Note 1 to entry: The level of rigour required depends on the nature of the subject matter	evaluation verb
3.42	connectivity	property of the TOE allowing interaction with IT entities external to the TOE Note 1 to entry: This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.	TOE
3.43	counter, verb	act on or respond to a particular threat so that the threat is eradicated or mitigated	security model
3.44	covert channel	enforced, illicit signalling channel that allows a user to surreptitiously contravene the multi-level separation policy and unobservability requirements of the TOE	TOE
3.45	delivery	transmission of the finished TOE from the production environment into the hands of the customer Note 1 to entry: This product life-cycle phase may include packaging and storage at the development site, but does not include transportations of the unfinished TOE or parts of the TOE between different developers or different development sites.	life cycle
3.46	demonstrable conformance	relation between a ST and a PP, where the ST provides an equivalent or more restrictive solution which solves the generic security problem in the PP	security model
3.47	demonstrate	<evaluation verb> provide a conclusion gained by an analysis which is less rigorous than a "proof"	evaluation verb
3.48	dependancy	relationship between components such that a PP, ST, functional package or assurance package including a component shall also include any other components that are identified as being depended upon or include a rationale as to why they are not	taxonomy
3.49	dependent component	entity in a multi-component TOE, which is itself the subject of an evaluation, relying on the provision on services by a base component	composition
3.50	dependent TOE	entity in a composed TOE which is itself the subject of an evaluation, relying on the provision on services by one or more base components Note 1 to entry: applies only to the "composed" evaluation approach (not to the composite	composition

ID_no	Term	Current definition	Concept
		approach).	
3.51	describe	<evaluation verb> provide specific details of an entity	evaluation verb
3.52	determine	<evaluation verb> affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion Note 1 to entry: The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms "confirm" or "verify" which imply that an analysis has already been performed which needs to be reviewed	evaluation verb
3.53	developer	organisation responsible for the development of the TOE	life cycle
3.54	development	product life-cycle phase which is concerned with generating the implementation representation of the TOE Note 1 to entry: Throughout the ALC: Life-cycle support requirements, development and related terms (developer, develop) are meant in the more general sense to comprise development and production.	life cycle
3.55	development environment	environment in which the TOE is developed Note 1 to entry: The conditions include physical facilities, security controls, IT systems and development tools.	life cycle
3.56	development tools	tools (including test software, if applicable) supporting the development and production of the TOE EXAMPLE For a software TOE, development tools are usually programming languages, compilers, linkers and generating tools.	life cycle
3.57	direct rationale	type of Protection Profile or Security Target in which the threats and organisational security policies in the SPD are mapped directly to the SFRs and possibly to the Security Objectives for the operational environment Note 1 to entry: Direct rationale does not include security objectives for the TOE.	security model

ID_no	Term	Current definition	Concept
3.58	domain separation security domain separation	security architecture property whereby the TSF defines separate security domains for each user and for the TSF and ensures that no user process can affect the contents of a security domain of another user or of the TSF	TOE
3.59	element	<taxonomy> most detailed level of definition of a security need as defined in SFRs and SARs	taxonomy
3.60	encountered potential vulnerability	potential weakness in the TOE identified by the evaluator while performing evaluation activities that could be used to violate the SFRs	vulnerability analysis
3.61	ensure	<evaluation verb> guarantee a strong causal relationship between an action and its consequences Note 1 to entry: When this term is preceded by the word "help" it indicates that the consequence is not fully certain, on the basis of that action alone.	evaluation verb
3.62	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	TOE
3.63	evaluate	assessment of a PP, an ST or a TOE, against defined criteria	assurance
3.64	evaluation activity EA	activities derived from work units described in ISO/IEC 18045 Note 1 to entry: The concept of evaluation activities, and the combination of evaluation activities into "evaluation methods", is defined in ISO/IEC 15408-4.	assurance
3.65	evaluation assurance level EAL	well formed package of assurance requirements defined in ISO/IEC 15408-3 and drawn from ISO/IEC 15408-3, representing a point on the ISO/IEC 15408 predefined assurance scale	assurance
3.66	evaluation authority	body operating an evaluation scheme Note 1 to entry: By applying the evaluation scheme evaluation authority sets the standards and monitors the quality of evaluations conducted by bodies within a specific community.	assurance
3.67	evaluation deliverable	any resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities	assurance
3.68	evaluation evidence	item used as a basis for establishing the verdict of an evaluation activity	assurance
3.69	evaluation method	set of one or more evaluation activities that are derived from ISO/IEC 18045 work units for application in a specific context	assurance

ID_no	Term	Current definition	Concept
3.70	evaluation scheme	rules, procedures, and management to carrying evaluations of IT products security implementing all parts of ISO/IEC 15408 Note 1 to entry: Administrative and regulatory framework is usually a part of an evaluation scheme. Such framework is out of the scope of ISO/IEC 15408. Note 2 to entry: The objective of an evaluation scheme is to ensure that high standards of competence and impartiality are maintained and a consistency of evaluations is achieved. Note 3 to entry: An evaluation scheme is usually established by an evaluation authority, which defines the evaluation environment, including criteria and methodology required to conduct IT security evaluations.	assurance
3.71	evaluation technical report	documentation of the overall verdict and its justification, produced by the evaluator and submitted to an evaluation authority	assurance
3.72	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 ISO/IEC 15408 (all parts) with the associated evaluation methodology given in ISO/IEC 18045 SOURCE: ISO/IEC 19896-1:2018	assurance
3.73	exact conformance	hierarchical relationship between a PP or PP Configuration and an ST where all the requirements in the ST are drawn only from the PP/PP Configuration Note 1 to entry: Aan ST is allowed to claim exact conformance to one or more PPs but only to one PP configuration.	security model
3.74	examine	<evaluation verb> generate a **verdict** by analysis using evaluator expertise Note 1 to entry: The statement that uses this verb identifies what is analysed and the properties for which it is analysed.	evaluation verb

ID_no	Term	Current definition	Concept
3.75	exhaustive	<evaluation verb> characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan Note 1 to entry: This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is related to "systematic" but is considerably stronger, in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to ensure that all possible avenues have been exercised.	evaluation verb
3.76	explain	<evaluation verb> give argument accounting for the reason for taking a course of action Note 1 to entry: This term differs from both "describe" and "demonstrate". It is intended to answer the question "Why?" without actually attempting to argue that the course of action that was taken was necessarily optimal.	evaluation verb
3.77	exploitable vulnerability	weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE	vulnerability analysis
3.78	extended security requirement	security requirement developed according to the rules given in ISO/IEC 15408 but that is not specified in any part of ISO/IEC 15408 Note 1 to entry: An extended security requirement may be either a SAR or a SFR. Note 2 to entry: Extended security requirements are defined within extended component definitions.	security model
3.79	external entity user	human, technical system or one of its components interacting with the TOE from outside of the TOE boundary	TOE
3.80	family	<taxonomy> set of components that share a similar goal but differ in emphasis or rigour	taxonomy
3.81	formal	expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts	taxonomy
3.82	functional interface	external interface providing a user with access to functionality of the TOE which is not directly involved in enforcing security functional requirements Note 1 to entry: In a composed TOE these are the interfaces provided by the base component that are required by the dependent component to support the operation of the composed TOE.	composition
3.83	functional package	named set of security functional requirements that may be accompanied by an SPD and security objectives derived from that SPD	taxonomy

ID_no	Term	Current definition	Concept
3.84	general model	type of Protection Profile or Security Target in which the SPD-elements of the SPD are mapped to the Security Objectives for the TOE and to the Security Objectives for the operational environment. Note 1 to entry: SFRs in the general model have to cover all security objectives for the TOE.	TOE
3.85	global assurance level	assurance package, i.e. a well-formed set of assurance requirements drawn from ISO/IEC 15408-3 or defined as a set of extended assurance components, that applies to the entire TOE in a multi-assurance evaluation	assurance
3.86	guidance docummentation	documentation that describes the delivery, preparation, operation, management and/or use of the TOE	TOE
3.87	identity	representation uniquely identifying an entity within the context of the TOE EXAMPLE An example of such a representation is a string. Note 1 to entry: entities can be diverse such as a user, process, or disk. For a human user, the representation could be the full or abbreviated name or a unique pseudonym. Note 2 to entry: An entity can have more than one identity.	TOE
3.88	implementation representation	least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement 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.	life cycle
3.89	informal	expressed in natural language	taxonomy
3.90	installation	procedure performed by a human user embedding the TOE in its operational environment and putting it into an operational state Note 1 to entry: This operation is performed normally only once, after receipt and acceptance of the TOE. The TOE is expected to be progressed to a configuration allowed by the ST. If similar processes have to be performed by the developer they are denoted as "generation" throughout ALC: Life-cycle support. If the TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as installation.	life cycle
3.91	inter TSF transfer	communicating data between the TOE and the security functionality of other trusted IT products	TOE

ID_no	Term	Current definition	Concept
3.92	internal communication channel	communication channel between separated parts of the TOE	TOE
3.93	internal TOE transfer	communicating data between separated parts of the TOE	TOE
3.94	internally consistent	no apparent contradictions exist between any aspects of an entity 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.	TOE
3.95	interpretation	clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045 or scheme requirement	assurance
3.96	iteration	use of the same component to express two or more distinct requirements	taxonomy
3.97	justify	<evaluation verb> provide a rationale providing sufficient reason Note 1 to entry: The term 'justify' is more rigorous than a 'demonstrate'. This term requires significant rigour in terms of very carefully and thoroughly explaining every step of a logical analysis leading to a conclusion.	evaluation verb
3.98	laboratory	organization with a management system providing evaluation and or testing work in accordance with a defined set of policies and procedures and utilizing a defined methodology for testing or evaluating the security functionality of IT products Note 1 to entry: These organizations are often given alternative names by various approval authorities. For example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF). [SOURCE ISO/IEC DIS 19896-1 ,3.7]	assurance
3.99	layering	design technique where separate groups of modules are hierarchically organized to have separate responsibilities such that a group of modules depends on groups of modules below it in the hierarchy for services, and provides its services to the group of modules above it	composition
3.100	life cycle model	framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a product, spanning the life of the system from the definition of its requirements to the termination of its use Note 1 to entry: See also Figure 1. [SOURCE: ISO/IEC/IEEE 24765:2010 3.1587 modified, note 1 to entry added]	life cycle
3.101	module TOE Module	small architectural unit that can be characterized in terms of the properties discussed in TSF internals (ADV_INT)	TOE

ID_no	Term	Current definition	Concept
3.102	monitoring attacks	generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds to the guidance documents	TOE
3.103	multi-assurance evaluation	evaluation using a PP-Configuration where the TOE is organised in parts, each part being associated with its own assurance package	assurance
3.104	non-bypassability	⟨of the TSF⟩ security architecture property whereby all SFR-related actions are mediated by the TSF	TOE
3.105	object	entity in the TOE, that contains or receives information, and upon which subjects perform operations	TOE
3.106	observation report	report written by the evaluator requesting a clarification or identifying a problem during the evaluation	assurance
3.107	operation	⟨on an ISO/IEC 15408 component⟩ modification or repetition of a component by assignment, iteration, refinement, or selection	taxonomy
3.108	operation	⟨on an object⟩ specific type of action performed by a subject on an object	TOE
3.109	operation	usage phase of the TOE including "normal usage", administration and maintenance of the TOE after delivery and preparationusage phase of the TOE including "normal usage", administration and maintenance of the TOE after delivery and preparation	life cycle
3.110	operational environment	environment in which the TOE is operated	security model
3.111	optional Security Functional Requirement optional SFR	SFR in a Protection Profile or PP-Module that contributes to a stated aspect of the PP's security problem description but its inclusion in a conformant ST's list of SFRs is not mandatory. Note 1 to entry: An optional SFR can address appropriate SPD elements threat(s) and/or OSPs.	security model
3.112	organizational security policy OSP	set of security rules, procedures, or guidelines for an organization Note 1 to entry: A policy may pertain to a specific operational environment.	security model
3.113	overall verdict	pass or fail statement issued by an evaluator with respect to the result of an evaluation Note 1 to entry: The statement can be expressed as "pass" or "fail".	assurance
3.114	oversight verdict	statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities	assurance
3.115	potential vulnerability	suspected, but not confirmed, weakness Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the SFRs.	vulnerability analysis

ID_no	Term	Current definition	Concept
3.116	preparation	activity in the life-cycle phase of a product, comprising the customer's acceptance of the delivered TOE and its installation which may include such things as booting, initialisation, start-up and progressing the TOE to a state ready for operation	life cycle
3.117	production	life-cycle phase which follows the development phase and consists of transforming the implementation representation into the implementation of the TOE, i.e. into a state acceptable for delivery to the customer Note 1 to entry: This phase may comprise manufacturing, integration, generation, internal transports, storage, and labelling of the TOE.	life cycle
3.118	Protection Profile PP	implementation-independent statement of security needs for a TOE type	security model
3.119	Protection Profile configuration PP-Configuration	implementation-independent statement of security needs for a TOE type contained in base Protection Profile(s), Protection Profile Module(s), and Protection Profile(s) that are not base PPs for any PP-Module included	security model
3.120	Protection Profile module PP-Module	implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles	security model
3.121	prove	<evaluation verb> show correspondence by formal analysis in its mathematical sense Note 1 to entry: It is completely rigorous in all ways. Typically, the term prove is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.	evaluation verb
3.122	record	<evaluation verb> retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time	assurance
3.123	refinement	addition of details to a component	taxonomy
3.124	report	<evaluation verb> include evaluation results and supporting material in the evaluation technical report or an observation report	assurance

ID_no	Term	Current definition	Concept
3.125	residual vulnerability	weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE	vulnerability analysis
3.126	role	predefined set of rules establishing the allowed interactions between a user and the TOE	TOE
3.127	secret	information that shall be known only to authorised users and/or the TSF in order to enforce a specific SFP	TOE
3.128	secure state	state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs	TOE
3.129	security assurance requirement, SAR	security requirement, that refers to the conditions and processes for the development and delivery of the TOE, and the actions required of evaluators with respect to evidence produced from these conditions and processes	security model
3.130	security attribute	property of subjects, users, objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs Note 1 to entry: Users can include external IT products.	TOE
3.131	security domain	environment provided by the TSF for the use by untrusted entities in such a way that the environment is isolated and protected from other environments	TOE
3.132	security function policy	set of rules describing specific security behaviour enforced by the **TSF** and expressible as a set of SFRs Note 1 to entry: A security functional requirement can be addressed directly as in the direct rationale model, or indirectly, through the Security Objectives for the TOE, as in the general model.	TOE
3.133	security functional requirement, SFR	security requirement, which contributes to fulfil the TOE's Security Problem Definition (SPD) as defined in a specific ST or in a PP Note 1 to entry: A security functional requirement can be addressed directly as in the direct rationale model, or indirectly, through the Security Objectives for the TOE, as in the general model.	security model
3.134	security objective	statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions	security model

ID_no	Term	Current definition	Concept
3.135	security problem security problem definition SPD	statement which in a formal manner defines the nature and scope of the security that the TOE 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, the 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 assumption.	security model
3.136	security requirement	requirement, stated in a 15408a standardized language, which is part of a TOE security specification as defined in a specific ST or in a PP.	security model
3.137	security target, ST	implementation-dependent statement of security requirements for a TOE based on a security problem definition	security model
3.138	selection	specification of one or more items from a list in a component	taxonomy
3.139	selection-based Security Functional Requirement selection-based SFR	SFR in a Protection Profile/ PP-Module that contributes to a stated aspect of the PP's/ PP-Module's security problem definition that shall is to be included in a conformant ST if a selection choice identified in the PP/PP-Module indicates that it has an associated selection-based SFR	security model
3.140	semiformal	expressed in a restricted syntax language with defined semantics	taxonomy
3.141.	single-assurance evaluation	evaluation using a single set of assurance requirements	assurance
3.142	specify	<evaluation verb> provide specific details about an entity in a rigorous and precise manner	evaluation verb
3.143	strict conformance	hierarchical relationship between a PP and a ST/PP where all the requirements in the PP also exist in the ST/PP Note 1 to entry: This relation can be paraphrased as "the ST shall contain all statements that are in the PP, but may contain more". Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner.	security model
3.144	sub-activity	application of an assurance component of ISO/IEC 15408-3 Note 1 to entry: Assurance families are not explicitly addressed in ISO/IEC 15408 (all parts) because evaluations are conducted on a single assurance component from an assurance family	assurance

ID_no	Term	Current definition	Concept
3.145	sub-TSF	combined functionality of all hardware, software, and firmware of a TOE that are relied upon for the correct enforcement of the SFRs defined in one PP-Configuration component. Note 1 to entry: This set of SFRs is closed by dependencies, objectives, and SPD 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 STs. It can be used in the single-assurance approach but it must be used in the multi-assurance approach: sub-TSFs must be defined in a multi-assurance PP-Configuration and in conformant STs. Note 3 to entry: each sub-TSF is associated with its own set of SARs in a multi-assurance PP-Configuration. In the rest of the document, a set of SARs may be an assurance package. Note 4 to entry: a sub-TSF has the characteristics of a TSF.	assurance
3.146	subject	entity in the TOE that performs operations on objects	TOE
3.147	tailoring	addition of one or more functional requirements to a functional package, and/or the addition of one or more selections to an SFR 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, PPs, or PP-Modules. Note 2 to entry: the selections in the SFR may 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.	taxonomy
3.148	target of evaluation TOE	set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation	TOE
3.149	threat agent	entity that can exercise adverse actions on assets protected by the TOE	security model
3.150	time period to exposure	time interval when an element is participating in an IT system and could be attacked	vulnerability analysis
3.151	TOE resource	anything usable or consumable in the TOE	TOE
3.152	TOE security functionality TSF	combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs	TOE

ID_no	Term	Current definition	Concept
3.153	TOE type	set of TOEs that have common characteristics Note 1 to entry: The TOE type may be more explicitly defined in a PP. Note 1 to entry: The TOE type may be more explicitly defined in a PP.	security model
3.154	trace	<evaluation verb> identity relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second	evaluation verb
3.155	transfer outside of the TOE	TSF mediated communication of data to entities not under the control of the TSF	TOE
3.156	translation	describes the 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 SFR expressed in standardized language can also be translated back to the Security Objectives.	taxonomy
3.157	trusted channel	means by which a TSF and another trusted IT product can communicate with necessary confidence	TOE
3.158	trusted IT product	IT product, other than the TOE, which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly	TOE
3.159	trusted path	means by which a user and a TSF can communicate with the necessary confidence Note 1 to entry: Communication typically implies the establishment of identification and authentication of both parties, as well as the concept of a user specific session which is integrity-protected. Note 2 to entry: When the external entity is a trusted IT product, the notion of trusted channel is used instead of trusted path. Note 3 to entry: Both physical and logical aspects of secure communication can be considered as mechanisms for gaining confidence.	TOE
3.160	TSF data	data for the operation of the TOE upon which the enforcement of the SFR relies	TOE
3.161	TSF interface TSFI	means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF,	TOE
3.162	TSF self-protection	security architecture property whereby the TSF cannot be corrupted by non-TSF code or entities	TOE

ID_no	Term	Current definition	Concept
3.163	user data	data received or produced by the TOE, which is meaningful to some external entity but which do not affect the operation of the TSF Note 1 to entry: Depending of the concept, this definition assumes that the same data created by users that has an actual impact on the operation of the TSF can be regarded as the TSF data.	TOE
3.164	verdict	pass, fail or inconclusive statement issued by an evaluator with respect to an ISO/IEC 15408 evaluator action element, assurance component, or class Note 1 to entry: The statement can be presented as: pass, fail or inconclusive. Note 2 to entry: Also see overall verdict.	assurance
3.165	verify	<evaluation verb> rigorously review in detail with an independent determination of sufficiency Note 1 to entry: Also see "confirm". This term has more rigorous connotations. The term "verify" is used in the context of evaluator actions where an independent effort is required of the evaluator.	evaluation verb
3.166	vulnerability	weakness in the TOE that can be used to violate the SFRs in some environment	vulnerability analysis
3.167	window of opportunity	period of time that an attacker has access to the TOE	vulnerability analysis
3.168	work unit	most granular level of evaluation work	assurance