COMMITTEE DRAFT **ISO/IEC 3rd CD 15408-4**	Reference document: **SC 27 N19508**
Date: **2019-07-12**	Supersedes document N18806

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection Secretariat: Germany	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: **2019-09-06** Please submit your comments via the online balloting application by the due date indicated.

ISO/IEC 3rd CD 15408-4

Title: IT Security techniques – Evaluation criteria for IT security -- Part 4: Framework for the specification of evaluation methods and activities

Project: 1.27.16.04 (ISO/IEC 15408-4)

Explanatory Report

Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
For details regarding previous development stages refer to 2nd page of this explanatory report.			

ISO/IEC 15408-4
1st WD
	54th WG 3 meeting, April 2017, Recommendations 5,10 11, 14 (N17041 = WG 3 N1413).	SoV (N17028).	Liaisons to:
			CCDB (WG 3 N1391);
			The Open Group (WG 3 N1394);
			ISO/TC 22/SC 32 (N17373);
			Text f. 1st WD (WG 3 N1438).

ISO/IEC 15408-4
2nd WD
	55th WG 3 meeting, , October / November 2017, Recommendations 8, 10 (N17666 = WG 3 N1494).	SoCom (WG 3 N1470);
		Draft DoC (WG 3 N1501).
			Editor's report (WG 3 N1465);
			Liaisons to:
			CCDB (WG 3 N1455);
			ISO/TC 22/SC 32 (N18103);
			DoC (WG 3 N1462);
			Text f. 2nd WD (WG 3 N1472).

ISO/IEC 15408-4
1st CD
	56th WG 3 meeting, April 2018, Recommendations 8, 10 (N18471 = WG 3 N1557) / 30th SC 27 Plenary, April 2018, Resolution 6 (N18710)	SoCom (WG 3 N1532);
		Late Com (WG 3 N1565).
			Liaison to:
			CCDB (WG 3 N1521);
			DoC (WG 3 N1527);
			Text f. 1st CD (N18703).

ISO/IEC 15408-4
2nd CD
	57th WG 3 meeting / CRM, Sep / Oct 2018, Recommendations 11, 14 (N18820 = WG 3 N11610).	SoV (N18854).	Liaison to:
			CCDB (WG 3 N1619);
			DoC (N18802);
			Text f. 2nd CD (N18806).

ISO/IEC 15408-4
3rd CD
	58th WG 3 meeting / CRM April 2019, Recommendations 12, 14, 17, 21 (N19523 = WG 3 N1676).	SoV (N19490).	Liaison to:
			CCDB (WG 3 N1680);
			DoC (N19504);
			Text f. 3rd CD (N19508).

3rd CD Consideration

In accordance with Recommendation 14 (see SC 27 N19523) of the 58th SC 27/WG 3 meeting / CRM held in Tel Aviv, Israel, 2019-04-01/05 the hereby attached document is circulated for a 8-week 3rd CD letter ballot closing by

2019-09-06

Medium: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

No. of pages: 2 + 24

Explanatory Report (2nd page)

Status	SC 27 Decision	Reference documents	
		Input	Output
Study Period **IT security testing, evaluation and assurance standards and techniques**	51st WG 3 meeting, Oct. 2015, Recommendations 5, 6 (N15594 = WG 3 N1251).		Terms of Reference (WG 5 N1258); 1st /2nd call f. contr. (WG 3 N1259 /1317)..

	52nd WG 3 meeting, April 2016, Recommendation 5, 7 (N16026 = WG 3 N1296).	Expert contr. (WG 3 N1299, 1301).	3rd call f. contr. (WG 3 N1377);
			Rapporteur's report (WG 3 N1320);
			Liaison to:
			CCDB (WG 3 = N1266).

ISO/IEC NP 15408-4
by subdivision
Evaluation criteria for IT security -- Part 4
NWIP
	53rd WG 3 meeting, Oct. 2016, Recommendations 6, 15 (N16800 = WG 5 N600).	Expert contr. (WG 3 N1368, N1371, N13743).	SP report (WG 3 N1363);
			Call f. editor (WG 3 N1387 = N16886);
			Liaisons to:
			CCDB (WG 3 N1330);
			The Open Group (WG 3 N1332);
			Text f. NWIP (N16966 [replaces N16883]).

ISO/IEC JTC 1/SC 27/WG 3 N19508

Date: 2019-07-12

ISO/IEC 15408-4:####(EN)

ISO/IEC JTC 1/SC 27 IT Security techniques

Secretariat: DIN

IT security techniques — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities

Techniques de sécurité des technologies de l'information — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 4: Cadre général pour la spécification des méthodes et activités d'évaluation

CD stage

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see http://www.iso.org/patents).

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

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

This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

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

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at http://www.iso.org/members.html.

This is the first edition of ISO/IEC 15408-4.

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations. The ISO/IEC 15408 series does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. ISO/IEC 18045 provides a companion methodology for some of the assurance requirements specified in the ISO/IEC 15408 series, ISO/IEC 15408-1 and ISO/IEC 18045 also allow that more specific Evaluation Activities (EAs) may be derived for use in particular evaluation contexts. Specification of such Evaluation Activities is already occurring amongst practitioners and this creates a need for a specification for defining such Evaluation Activities.

This document provides a standardised framework for specifying objective, repeatable and reproducible Evaluation Methods (EMs), and Evaluation Activities.

IT Security techniques — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities

1 Scope

The model of security evaluation in ISO/IEC 15408-1:20XX provides high-level generic Evaluation Activities which are defined in ISO/IEC 18045. More specific Evaluation Activities may be derived from these generic work units for particular situations such as for SFRs or SARs applied to specific technologies or TOE types. This document describes a framework that can be used for deriving Evaluation Activities from work units of ISO/IEC 18045 and grouping them into 'Evaluation Methods'. Evaluation Activities or Evaluation Methods may be included in PPs and any documents supporting them.

This document also allows for Evaluation Activities to be defined for extended SARs, in which case derivation of the Evaluation Activities relates to equivalent action elements and work units defined for that extended SAR. Where reference is made in this document to the use of ISO/IEC 18045 or ISO/IEC 15408-3 for SARs (such as when defining rationales for Evaluation Activities) then in the case of an extended SAR the reference applies instead to the equivalent action elements and work units defined for that extended SAR.

For clarity, this document specifies how to define Evaluation Activities and methods but does NOT itself specify instances of Evaluation Activities or methods.

This document does not specify how to evaluate, adopt, or maintain Evaluation Activities and methods. These aspects are a matter for those originating the Evaluation Activities and methods in their particular area of interest.

2 Normative references

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

ISO/IEC 15408-1:20XX, *IT Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model,*

ISO/IEC 15408-2:20XX, *IT Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:20XX, *IT Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045:20XX, *IT Security techniques — Methodology for IT security evaluation*

[**Editorial note: reference dates for 15408 (all parts) and 18045 to be updated here and throughout when known]

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1:20XX and the following apply.

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

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Overview

The model of security evaluation in ISO/IEC 15408-1 identifies that high-level generic Evaluation Activities are defined in ISO/IEC 18045, but that more specific Evaluation Activities may be defined as technology-specific adaptations of these generic activities for particular situations (e.g. for SFRs or SARs applied to specific technologies or TOE types). This document, ISO/IEC 15408-4, describes a framework that can be used for defining these more specific Evaluation Activities, and which is integrated with ISO/IEC 15408-3 and ISO/IEC 18045.

Clause 5 introduces the model and basic terms used in defining Evaluation Activities and methods in relation to the terminology given by ISO/IEC 18045. It also provides guidance on how to derive such activities and methods from functional and assurance requirements.

Clause 6 describes how to construct an Evaluation Method as a set of Evaluation Activities. By starting with the general structure for documenting an Evaluation Method, the chapter continues with minimal requirements for their identification, scope, and dependencies on other Evaluation Methods, activities or actions, noting that some content requirements may be met at either or both of Evaluation Method level and Evaluation Activity level. An Evaluation Method may specify further requirements for evaluation inputs, tool types, evaluator competencies, and reporting requirements which are also subject of this clause. Details for specifying rationales for an Evaluation Method are provided.

Clause 7 provides details on the minimum content of an Evaluation Activity. In general, Evaluation Activities are based on evaluation objectives for specific technologies, derived from generic work units and the derivation relationship is then described in a rationale. Clause 7 describes how to specify objectives and rationales when deriving specific Evaluation Activities. Such activities may consider specific inputs, tool types, assessment strategies, and pass/fail criteria which are also subject of this clause.

5 General model of Evaluation Methods and Evaluation Activities

5.1 Concepts and model

ISO/IEC 18045 defines a generic set of work units that an evaluator carries out in order to reach a verdict for many of the assurance classes, families and components defined in ISO/IEC 15408-3. The relationship between the structure of a Security Assurance Requirement (SAR) in ISO/IEC 15408-3 and the work units in ISO/IEC 18045 is described in subclause 6.4 of ISO/IEC 18045:20XX ***[**check correct final reference location]***, and summarised in Figure 1 below.

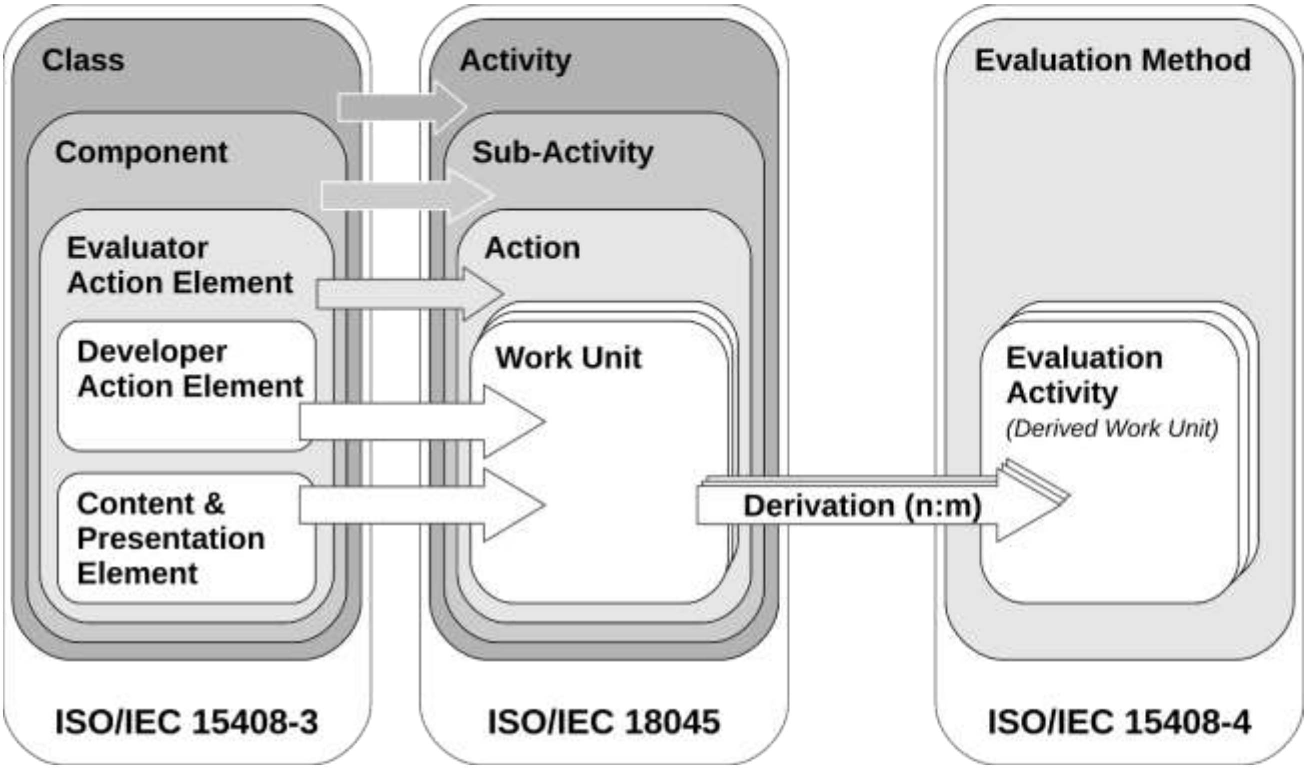

Figure 1 - Mapping of ISO/IEC 15408-3 and ISO/IEC 18045 structures

For the purposes of defining new Evaluation Activities and methods, the main point to note is that each Action (representing an Evaluator Action Element in ISO/IEC 15408-3 or an *implied* evaluator action element) is represented in ISO/IEC 18045 as a set of Work Units that are carried out by an evaluator.

This document specifies the ways in which new Evaluation Activities may be derived from the generic Work Units in ISO/IEC 18045, and combined into an Evaluation Method that is intended for use in some particular evaluation context. A typical example of such an evaluation context would be a particular TOE type or particular technology type.

EXAMPLE

TOE type: A network device

Technology type: Specific cryptographic functions

If Evaluation Methods and Evaluation Activities are required to be used with a particular PP, PP-Module, PP-Configuration, then a PP or PP-Module or PP-Configuration shall identify this requirement in its Conformance Statement. If Evaluation Methods and Evaluation Activities are required to be used with a particular package, then the package shall identify this requirement in the security requirement section. No formal claim of conformance to ISO/IEC 15408-4 is made in any of these cases. (The contents of PPs, PP-Modules, PP-Configurations and packages are described in more detail in ISO/IEC 15408-1.)

A PP (or PP-Module) may use more than one EM or separate set of EAs, such as where separate EMs have been defined for cryptographic operations and for secure channel protocols used in a PP.

NOTE Where exact conformance (as described in ISO/IEC 15408-1) is used, EMs/EAs are not allowed to be defined in a PP-Configuration (i.e. the EMs/EAs to be used are identified only in the PPs and PP-Modules used in the PP-Configuration).

5.2 Deriving Evaluation Methods and Evaluation Activities

In general, defining Evaluation Activities and Evaluation Methods may start either from an SAR, aiming to make some or all parts of its work units more specific, or from an SFR, aiming to define specific aspects of work units related to that SFR.

When starting from an SAR a guideline for the process is as follows:

a) Identify the relevant ISO/IEC 18045 work units from which to derive at least one individual Evaluation Activity or groups of Evaluation Activities;

b) For each work unit from which an Evaluation Activity is derived:

   1) Define the new Evaluation Activities in terms of the specific work to be carried out and the method of judging pass/fail criteria as described in 7.2;

   2) Group Evaluation Activities into an Evaluation Method if necessary;

   3) State the rationale for the new Evaluation Activities and the Evaluation Method under which they are grouped as described in 6.2.10 and 7.2.10.

   EXAMPLE A rationale can include reference to the developer action, and content and presentation elements of the work units from which they are derived.

A guideline for starting from an SFR would be as follows:

a) Identify the relevant SFR;

b) Identify the SARs (from 15408-3 or a set of extended SARs, or both) to be addressed for that particular SFR, and the corresponding ISO/IEC 18045 work units;

c) Define the new Evaluation Activities in terms of the specific work to be carried out and evaluation criteria (including, if required, pass/fail criteria as described in 7.2.8);

   EXAMPLE Evaluation Activities can be defined to examine the presentation of a specific SFR in the TOE Summary Specification (derived from ASE), to examine the presentation of the SFR in the guidance documentation (derived from AGD), and to carry out specific tests of the SFR (derived from ATE).

d) Map the affected work units for the SARs to the new Evaluation Activities;

e) State the rationale for the new Evaluation Activities, and the Evaluation Method under which they are grouped, as described in 6.2.10 and 7.2.10.

Although an author may choose to start from SARs or SFRs, it is noted that SARs will ultimately cover all SFRs. Starting from SFRs as described above is a technique that can be useful when clarifying the detail of how an SAR applies to a particular SFR, and that can be useful for presenting SFRs alongside the description of their Evaluation Activities.

It is not required to have a 1:1 mapping between work units and new Evaluation Activities, and the actual correspondence is documented in a rationale (as described in 6.2.10). The derivation may begin at different abstraction levels in Figure 1, and this is depicted in Figure 2. In case (a) of Figure 2 the author maps each work unit from ISO/IEC 18045 to a corresponding Evaluation Activity, while in case (b) the author maps a different number of Evaluation Activities, whilst still addressing all aspects of an action (i.e. the collection of work units), and the level of detail in the mapping may then be at the level of the action. (Even when mapping at the level of the action, it may nonetheless be useful to refer to work units that are being replaced by the Evaluation Activities.)

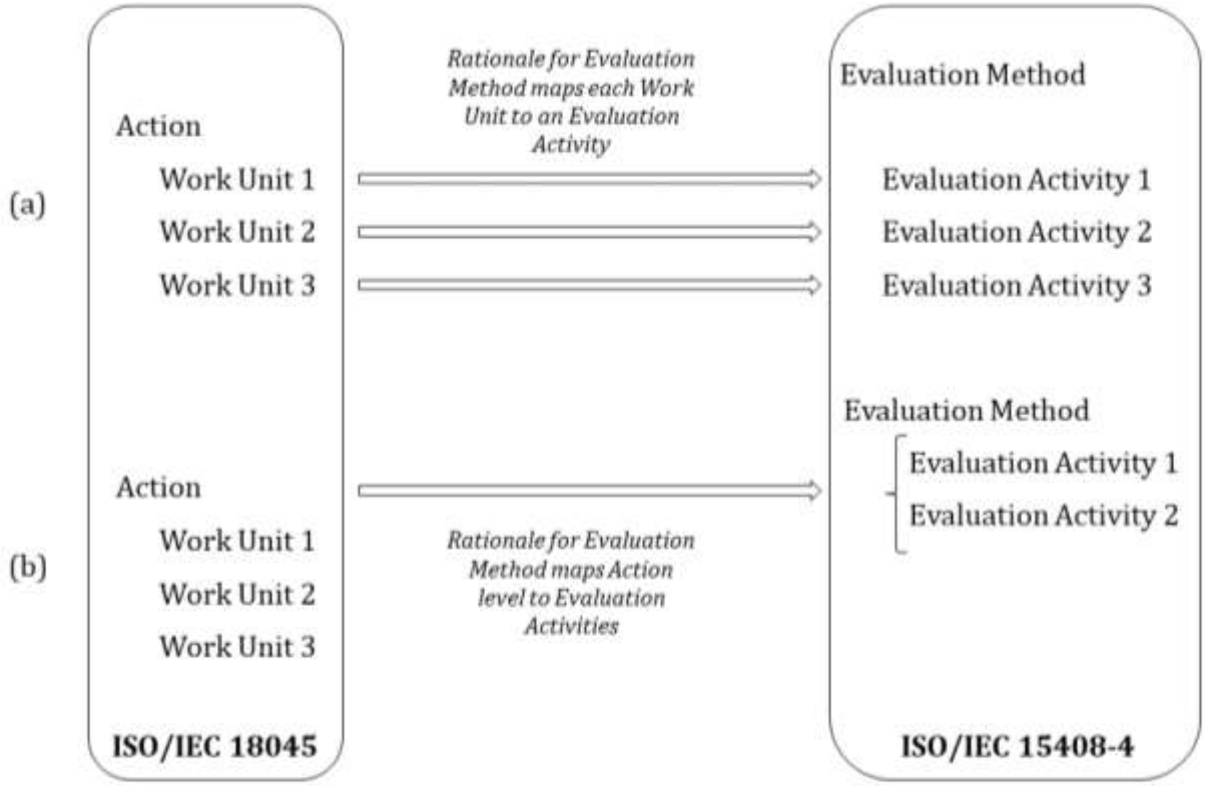

Figure 2 – Alternative approaches to mapping ISO/IEC 18045 to derived Evaluation Activities

Other approaches are possible depending on the content of the specific work units and evaluation activities: even where the same number of work units and evaluation activities exist, a simple 1:1 mapping may not be possible and therefore a mapping at the action level may be appropriate. Some more detailed mapping situations are described in the examples below[1].

EXAMPLE 1

If a TOE type includes both software and hardware then additional Evaluation Activities may be needed to deal with a manufacturing environment and its processes. Considering the ALC_DVS family, a possible approach would therefore be to adopt all the existing ALC_DVS work units for the software development environment and to define additional Evaluation Activities for each of the relevant hardware and manufacturing aspects. These aspects may include protection of hardware design in the development environment, secure transfer of software from the development environment to the manufacturing environment, security of the manufacturing site, and protection of the manufactured product while awaiting delivery. In this example the original ALC_DVS.1.1E action is mapped to include all the new Evaluation Activities, but an alternative approach would be to define additional Evaluation Activities for each individual work unit for ALC_DVS.1E, identifying the additional activities to cover the manufacturing environment for that work unit.

EXAMPLE 2

If AVA_VAN.1 vulnerability analysis is applied to a particular type of TOE, where there is a specific need to achieve consistency in the public domain vulnerability sources used then a possible approach would therefore be to define Evaluation Activities that replace the AVA_VAN work unit dealing with searching public domain sources with one that specifies the particular sources to be used, perhaps along with particular searches to be carried out and decision criteria for selecting a resulting list of potential vulnerabilities to be analysed and tested. In this example the original AVA_VAN.1-3 work unit is mapped to the new Evaluation Activity.

[1] These examples assume that the Evaluation Activities described are being defined by a community that can judge the suitability of the rationale for completeness of the Evaluation Activities. The examples are concerned only with the form and structure of the mappings: not with the nature or acceptance of the completeness rationale.

5.3 Verb usage

Where a verb is defined in ISO/IEC 15408-1 ***[**check correct final reference location]*** then the description of Evaluation Activities shall use those verbs only in accordance with the definitions. Alternative verbs may be used in an Evaluation Method for use in its Evaluation Activities provided that the alternative verbs are defined in the Evaluation Method. Any such verb definition shall make clear the extent to which evaluator judgement (as opposed to simple checking) is involved.

EXAMPLE An Evaluation Method that includes automated test generation for a protocol can define a verb “cover”, applied to enumerated types in a protocol parameter, to mean trying all defined and undefined values of the parameter within the available parameter length. Then Evaluation Activities can be written in forms such as “The evaluator shall cover the PaymentMode field”.

The paragraphs below describe conventions used in ISO/IEC 15408-3 and ISO/IEC 18045 that support consistency in the description of Evaluation Methods and Evaluation Activities.

All work unit and sub-task verbs are preceded by the auxiliary verb *shall* and by presenting both the verb and the *shall* in ***bold italic*** type face. The auxiliary verb *shall* is used only when the provided text is mandatory and therefore only within the work units and sub-tasks. The work units and sub-tasks contain mandatory activities that the evaluator must perform in order to assign verdicts.

Guidance text accompanying work units and sub-tasks gives further explanation on how to apply the work units and sub-tasks in an evaluation.

Evaluator action verbs such as *check*, *examine*, *report* and *record* are used in this document with the meanings defined in ISO/IEC 15408-1 ***[**check correct final reference location]***.

6 Structure of an Evaluation Method

6.1 Overview

An Evaluation Method and its constituent Evaluation Activities are defined for use in a particular evaluation context. For example, separate Evaluation Methods may be defined for specific technology areas which can range from specific functions up to specific product types or even - in the extreme case - for a specific product when the product is evaluated for unique features but where there is a requirement to have the product evaluated using a separately defined method that supports visibility, repeatability and reproducibility of the evaluation.

EXAMPLE Evaluation contexts for which separate Evaluation Methods can be defined are:

- specific product types like network devices, smart cards, biometric devices, mobile devices
- specific security functions reused for multiple product types, such as cryptographic functions, cryptographic protocols, digital certificate validation, identification and authentication schemes.

An Evaluation Method comprises a collection of individual Evaluation Activities, with additional information about the way in which the Evaluation Activities collectively meet a goal related to an identified evaluation context.

The description of an Evaluation Method includes:

a) Identification of the entity that is responsible for definition and maintenance of the Evaluation Method
b) The intended scope of the Evaluation Method, identifying the objective for deriving the Evaluation Activities in the Evaluation Method, the evaluation context in which it is intended to be applied, and any known limitation of, or aspects not intended to be covered by, the Evaluation Method
c) Any tool types and/or evaluator competences required to carry out the Evaluation Activities contained in the Evaluation Method

d) Any requirements for reporting on the results of applying the Evaluation Method.

e) Identification of each work unit in ISO/IEC 18045 (or equivalent for an extended SAR) that is addressed by the Evaluation Activities in the Evaluation Method

f) Identification of any extended SARs from which an Evaluation Method is derived (if applicable)

g) Any additional verbs used in the description of Evaluation Activities in place of verbs defined in ISO/IEC 15408-1 ***[**check reference in mature part 1]***.

Further description of the content, including identification of which content elements are mandatory, and how content elements may be distributed between Evaluation Method and its Evaluation Activities, is given in 6.2 and 7.2 below and is summarised in Table 1. Where a content element is optional (e.g. identification of specific evaluator competences, or required tool types), then that part may simply be omitted from the relevant definition: it is not necessary to include a blank section.

6.2 Specification of an Evaluation Method

6.2.1 Overview

An Evaluation Method is specified in terms of the information identified in 6.2 below. No specific format is required for providing or presenting this information, except where stated for individual elements in 6.2 below. The purpose of specifying the description of an Evaluation Method in these subclauses is to ensure that the assurance techniques used in an evaluation can be unambiguously identified, and that the Evaluation Method will be used appropriately (in the context for which it was intended) and in a way that supports consistent evaluation results.

In general, the description of an Evaluation Method may be taken to include the descriptions of the individual Evaluation Activities that it contains. This means that aspects of the Evaluation Method description may be deduced from the Evaluation Activity descriptions.

Figure 3 illustrates the content described in this document for an Evaluation Method: it does not define a mandatory structure for describing an Evaluation Method.

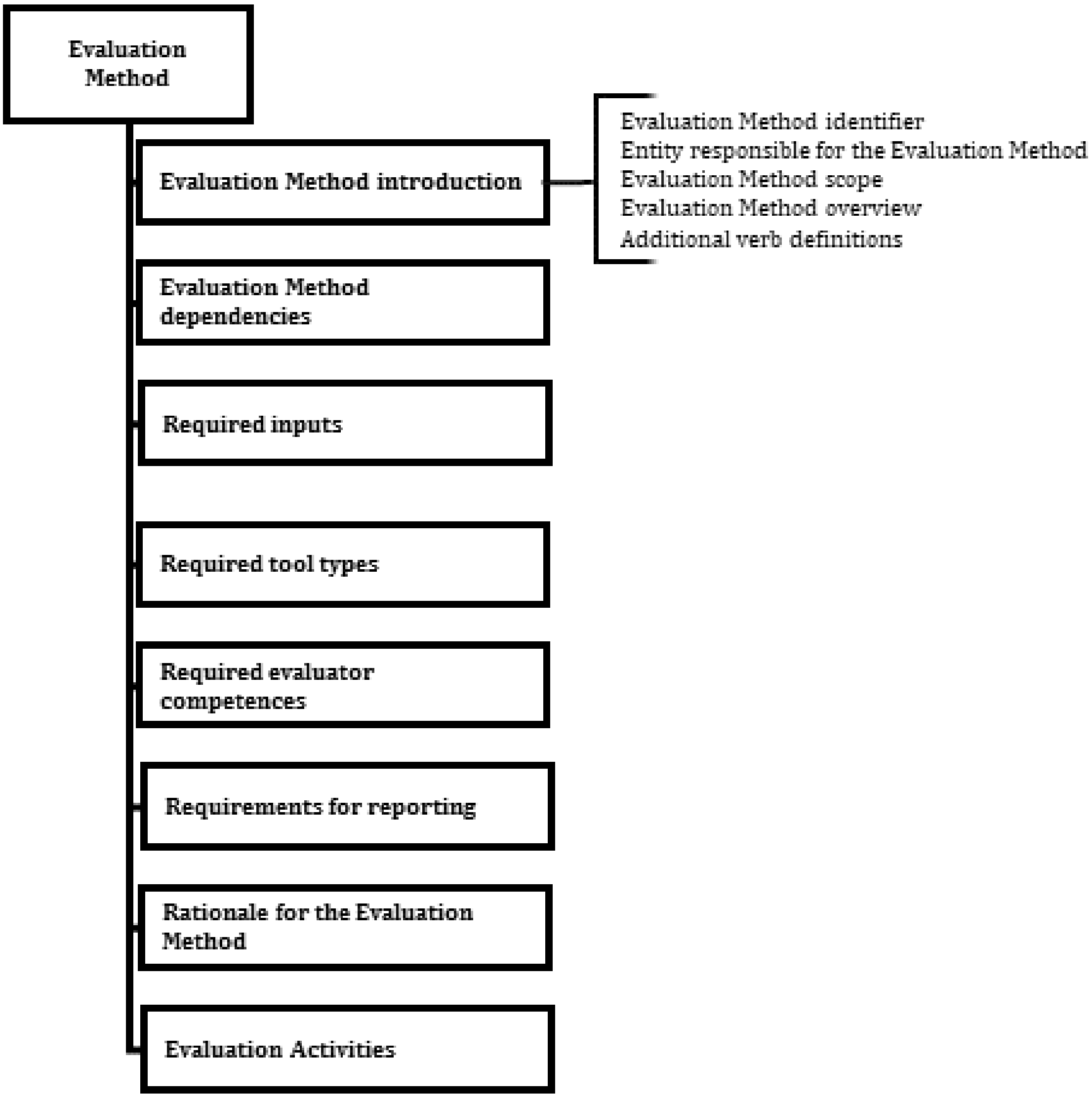
Evaluation Method
Evaluation Method introduction
Evaluation Method identifier
Entity responsible for the Evaluation Method
Evaluation Method scope
Evaluation Method overview
Additional verb definitions
Evaluation Method dependencies
Required inputs
Required tool types
Required evaluator competences
Requirements for reporting
Rationale for the Evaluation Method
Evaluation Activities

Figure 3 – Contents of an Evaluation Method

The contents shown in Figure 3 are described in more detail in 6.2 and 7.2, and a summary of the mandatory and optional requirements for specifying Evaluation Methods and Evaluation Activities is given in Table 1.

Table 1 – Distribution of content between Evaluation Method (EM) and Evaluation Activities (EA)

Content Element	Evaluation Method	Evaluation Activity
Identifier	Mandatory	Mandatory
Entity Responsible	Mandatory	
Scope	Mandatory	
Dependencies	Optional at EM or EA level	
Required inputs	Mandatory at EM or EA level	
Required tool types	Optional at EM or EA level	
Required evaluator competences	Optional at EM or EA level	
Requirements for reporting	Optional at EM or EA level	
Rationale	Mandatory at EM or EA level	
Evaluation Activities	Mandatory	
Additional verb definitions	Optional	
Objective		Mandatory
Evaluation Activity links to SFRs, SARs and other Evaluation Activities		Optional
Assessment strategy		Mandatory
Pass/fail criteria		Optional

A shaded cell in Table 1 indicates that the content in that row is not applicable to the Evaluation Method or Evaluation Activity.

6.2.2 Identification of Evaluation Methods

The definition of an Evaluation Method shall include a unique identifier in order to unambiguously identify the set of Evaluation Activities to be applied in any given evaluation. An identifier should be assigned at the Evaluation Method level (rather than just at the level of the Evaluation Activities it contains), reflecting the fact that an Evaluation Method is intended to be applied as a whole, and is subject to rationale and defined purpose and objectives at this level. If a set of Evaluation Activities has been grouped into an Evaluation Method then it shall only be identified as the same Evaluation Method when the complete set of Evaluation Activities in the Evaluation Method is used, with the same rationale as contained in the original Evaluation Method. If there is a need to divide the Evaluation Method into smaller subsets of Evaluation Activities then a separate Evaluation Method, with its own rationale, shall be defined for each subset.

EXAMPLE A unique identifier may be expressed by the title and version number of a supporting document or protection profile containing the Evaluation Method. Alternatively an identifier may also be obtained from a registration authority.

As described in 6.2.10 an Evaluation Method may be overlain by another Evaluation Method (e.g. for use in other PPs or PP-Modules). In such a case, if the original Evaluation Method rationale still holds (as described in 6.2.10) then the identifier of the original Evaluation Method shall be used; but if the rationale is changed as part of the overlay then a separate identifier defined in the relevant PP-Module or PP shall be used. The intention here is to ensure that a significant change to the rationale results in a different identifier being used.

6.2.3 Entity responsible for the Evaluation Method

The definition of an Evaluation Method shall state the entity that is responsible for definition and maintenance of the Evaluation Method.

6.2.4 Scope of the Evaluation Method

The definition of an Evaluation Method shall describe its scope, including:

a) The objective of the Evaluation Method in terms of assurance goals and a high-level description of how these are implemented by the Evaluation Activities performed within the Evaluation Method

b) The evaluation context in which the Evaluation Method is intended to be applied. For example, this can describe a TOE type such as a smart card or network device, or a type of function such as cryptographic functions using certain algorithms and modes applied to certain types of data transmission and data storage

c) Any known limitation of the Evaluation Method, or aspects not intended to be covered by the Evaluation Method.

Evaluation activities may be defined to apply specifically to one or more SFRs, and when an Evaluation Method includes such SFR-specific Evaluation Activities then a subsection of the scope shall identify the individual SFRs that the Evaluation Method is defined to address and the location where the SFRs are defined (e.g. ISO/IEC 15408-2 or extended SFRs defined in a Protection Profile). For extended SFRs that are not defined in ISO/IEC 15408-2, the identification of the location is particularly important since the same SFR name may have been used in different sources to refer to SFRs with different content. (If the Evaluation Method is not specific to any SFRs then this subsection is not required.)

Similarly, Evaluation Activities may be defined to apply specifically to one or more extended SARs (i.e. SARs that are not defined in ISO/IEC 15408-3), and when an Evaluation Method includes such Evaluation Activities then a subsection of the scope shall identify the relevant extended SARs and the location where they are defined (e.g. in a Protection Profile). As with extended SFRs, the identification of the location is particularly important since the same SAR name may have been used in different sources to refer to SARs with different content. (If the Evaluation Method does not apply to any extended SARs then this subsection is not required.)

NOTE The rationale for completeness of the Evaluation Method (6.2.10) may give further information relevant to the scope of the Evaluation Method.

6.2.5 Dependencies

The definition of an Evaluation Method shall describe any dependencies on other Evaluation Methods, Evaluation Activities, or on some of the generic actions in ISO/IEC 18045.

EXAMPLE The Evaluation Method may rely on information obtained from some other developer action element in ISO/IEC 15408-3 or some action in ISO/IEC 18045.

Dependencies may be identified either at the level of the Evaluation Method, or at the level of an individual Evaluation Activity contained within the Evaluation Method.

6.2.6 Required input from the developer or other entities

The definition of an Evaluation Method shall identify any developer input required to perform the Evaluation Activity. This may be done either at the level of the Evaluation Method, or at the level of an individual Evaluation Activity included in the Evaluation Method. The description of the inputs may also be made by reference to those defined for the generic SAR from which the Evaluation Activities are derived, as defined in ISO/IEC 15408-3 (or the equivalent generic definition if dealing with an extended SAR).

EXAMPLE The inputs for an Evaluation Method dealing with media encryption TOEs can define a requirement for description of particular details of a key hierarchy.

6.2.7 Required tool types

If the Evaluation Activities require any tool types then those shall be listed as part of the definition of the Evaluation Method. The tool types may be identified either at the level of the Evaluation Method, or at the level of an individual Evaluation Activity contained within the Evaluation Method.

6.2.8 Required evaluator competences

An Evaluation Method may identify specific evaluator competences required for its Evaluation Activities (see [2]). If specific evaluator competences are identified then this may be done either at the level of the Evaluation Method, or at the level of individual Evaluation Activities contained within the Evaluation Method (or a combination of both).

6.2.9 Requirements for reporting

The description of the Evaluation Method may include a description of reporting requirements. This description may be given at the level of the Evaluation Method, or the level of individual Evaluation Activities, or at both levels.

EXAMPLE 1 The Evaluation Method level can give general reporting requirements, but with some Evaluation Activities also requiring particular observations, justifications, or answers to specific questions to be included.

Any stated requirements for reporting shall be consistent with the requirements for the Evaluation Technical Report in ISO/IEC 18045, and any other standards required for the conduct of the evaluation.

EXAMPLE 2 An example of another standard that may be required for the conduct of an evaluation is ISO/IEC 17025.

The reporting requirements may specify the reporting to be included in the Evaluation Technical Report (ETR – as described in ISO/IEC 18045) but may also define content for other output reports to be produced.

EXAMPLE 3 There can be separate reports defined for public distribution and for more limited distribution (e.g. the developer, evaluator, and evaluation authority).

Where more than one report is defined in this way the reporting requirements for the Evaluation Method (including those for individual Evaluation Activities) may then specify the aspects to be reported in each of the output reports.

If an Evaluation Method does not require reports or report details other than those given in the work units from which it is derived (or if all the additional reporting requirements are stated in the Evaluation Activities), then this section is not required.

6.2.10 Rationale for the Evaluation Method

A rationale must be given to show that the derivation of the Evaluation Activities in an Evaluation Method, from the original work units in ISO/IEC 18045, is appropriate. (In the case of an extended SAR then references to work units in ISO/IEC 18045 apply instead to work units in the relevant methodology definition for the extended SAR). This may be given either at the level of the Evaluation Method, or at the level of individual Evaluation Activities. If the Evaluation Activities contained in the Evaluation Method do not have individual rationales according to 7.2.10, then the Evaluation Method shall include a rationale for the derivation of Evaluation Activities from work units in ISO/IEC 18045. That rationale may contain an explanation of why work units were reworked for the scope and depth of an evaluation of a specific technology or TOE type. The rationale shall further state how the Evaluation Activities it contains address all aspects of the ISO/IEC 15408-3 action elements to which they apply and shall justify that the manner in which the action elements or work units are addressed is complete with respect to the evaluation context in which the Evaluation Method is intended to be applied.

If an Evaluation Activity has been derived from an extended SAR, the rationale shall justify that the Evaluation Activity corresponds either to the description of the work units for that extended SAR or, if no such work units are defined, to the description of the extended SAR itself.

The rationale may, if appropriate, identify specific assumptions that are made for the evaluation context.

In cases when different sources of requirements are combined, such as where PP-Modules are used with a base PP in a PP-Configuration, the Evaluation Activities from each source (e.g. EAs for the base PP and EAs for each PP-Module) are combined and applied to the whole of the resulting TOE[2]. As part of the combination an Evaluation Method may be 'overlain' by another Evaluation Method, subject to a justification for any changes made by the overlay such that a rationale for the resulting Evaluation Method is still given. An overlay exists where the scope of more than one Evaluation Activity is the same, and the reason for the overlay is to make the resulting Evaluation Method more specific to the TOE when the two parts are used together (in this example the parts are a base PP and a PP-Module, but other cases can arise such as when a package is used in a PP and a more specific Evaluation Method defined for the PP overlays a more generic Evaluation Method defined for the package).

EXAMPLE An Evaluation Method can be defined in a base PP for a network device TOE, including Evaluation Activities for generic secure channels supported by the TOE. A PP-Module can be defined for certain remote management operations on network devices, using a specific secure channel type (e.g. this might consider particular operations or particular protocols). The Evaluation Activities for the PP-Module then overlay the Evaluation Method for the base PP, meaning that the PP-Module Evaluation Activities replace the base PP Evaluation Activities for the particular remote management activities covered in the PP-Module (other secure channel capabilities would still be subject to the Evaluation Activities in the Evaluation Method for the base PP).

The rationale for the resulting Evaluation Method may be based on allowances already made for the overlay in the original Evaluation Method rationale (i.e. where the rationale for the overlay is already included in the original Evaluation Method definition), or else the more specific Evaluation Method (e.g. in the PP-Module) may include a separate rationale dealing with its effect on the original Evaluation Method (e.g. in the base PP). Where the overlaying Evaluation Method (e.g. the PP-Module) includes a separate rationale, this must show that the resulting Evaluation Method preserves the relevant aspects of the overlain Evaluation Method, taking into account the context in which the combined parts are to be used. For the case of PPs used in combination, the same principle applies: either the original Evaluation Method describes the permitted variations according to the context in which it is applied, or else the resulting overlain Evaluation Method deals with the effect on the original Evaluation Method.

6.2.11 Additional verb definitions

As described in 5.3 above, alternative verbs to those defined in ISO/IEC 15408-1 ***[**check reference in mature part 1]*** may be used in the specification of an Evaluation Activity but any such alternative verbs shall be defined as part of the Evaluation Method that contains the Evaluation Activity, and shall make clear the extent to which evaluator judgement (as opposed to simple checking) is involved.

6.2.12 Set of Evaluation Activities

The Evaluation Activities contained in the Evaluation Method shall be defined using the structure defined in Clause 7.

[2] Although by default the Evaluation Activities apply to the whole of the resulting TOE, the definition of the Evaluation Methods or Evaluation Activities may define limits for their application. For example, Evaluation Activities can be defined specifically for cryptographic operations that are used in the context of certain secure channel protocols: these Evaluation Activities would not then apply to the same cryptographic operations when used in the context of protecting stored data.

7 Structure of Evaluation Activities

7.1 Overview

At the level of an individual Evaluation Activity, the emphasis of the specification is on ensuring that the Evaluation Activity has a clear objective, clear pass/fail criteria (if required), and that any dependencies on other Evaluation Activities are identified. This is intended to support understanding of the evaluation and hence consistent application of the activity in each evaluation.

As stated in the subclauses of 6.2 and summarised in Table 1, some of the details to be specified for Evaluation Activities may be included at either the Evaluation Method level or at the level of individual Evaluation Activities.

It is intended that the contents of Evaluation Activities may be given in various formats, including a format that consists of, for example, nothing more than a short narrative description of a test or an analysis activity (e.g. to confirm that user documentation describes the secure generation of credentials for use with a protocol). Furthermore some Evaluation Activities may be grouped together, and content elements described for the group as a whole rather than repeated for each individual Evaluation Activity. Each content element of an Evaluation Activity is described in more detail in the clauses below, and a summary of the mandatory and optional status of each element is summarised in Table 1.

7.2 Specification of an Evaluation Activity

7.2.1 Unique Identification of the Evaluation Activity

Evaluation activities shall be uniquely identified within their source document, and the source document shall itself be uniquely identified. Where Evaluation Activities have been grouped into an Evaluation Method then the individual Evaluation Activity identifiers are defined in addition to an identifier for the Evaluation Method as a whole (see section 6.2.2).

7.2.2 Objective of the Evaluation Activity

The objective of performing the Evaluation Activity shall be stated. This may be stated with reference to SFRs and SARs as discussed in 7.2.3 and to the pass/fail criteria in 7.2.8, However, it is also important that the statement of the objective supports an evaluator in understanding the flexibility and limitations on varying the Evaluation Activity to fit a specific TOE.

7.2.3 Evaluation Activity links to SFRs, SARs, and other Evaluation Activities

Where an Evaluation Activity is related to specific SFRs (possibly to specific instances of SFRs in another document such as a package, PP or PP-module) then this shall be identified as part of the Evaluation Activity definition.

EXAMPLE An Evaluation Activity can be related to an SFR stated in a particular PP with partial completion of an assignment to limit the acceptable values that can be used in a conformant ST.

Similarly, the relationship to specific SARs shall be identified (this may be achieved via the rationale for derivation from the work units of the original SAR (see 6.2.10 and 7.2.10) unless there is additional information to be given about the relationship).

Where an Evaluation Activity depends on completion of another Evaluation Activity then the dependency and the other Evaluation Activity shall be identified as part of the definition of the dependent Evaluation Activity. (Dependencies may be identified either at the level of the Evaluation Method, or at the level of an individual Evaluation Activity.)

7.2.4 Required input from the developer or other entities

As stated in 6.2.6, additional detail may be specified regarding the required format and content of the inputs to an Evaluation Activity. This additional detail would generally be used to support precise specification of the Evaluation Activity and its pass/fail criteria. (This may be done either at the level of the Evaluation Method, or at the level of an individual Evaluation Activity.)

If an Evaluation Activity does not require other input other than those defined in the work unit from which it is derived, then this section is not required.

7.2.5 Required tool types

If performing the Evaluation Activity requires any tool types in order to complete the activities then these tool types shall be defined as part of the definition of the Evaluation Activity. The definition of the tool type shall include sufficient detail to enable a tool of that type to be obtained or recreated in order that the Evaluation Activity can be consistently carried out with respect to the Evaluation Activity description and its pass/fail criteria. (This may be done either at the level of the Evaluation Method, or at the level of an individual Evaluation Activity.)

If an Evaluation Activity does not require specific tool types other than those given or implied in the work unit from which it is derived, then this section is not required.

7.2.6 Required evaluator competences

As stated in 6.2.8, an Evaluation Method may identify specific evaluator competences required for its Evaluation Activities (see [2]). If specific evaluator competences are identified then this may be done either at the level of the Evaluation Method, or at the level of individual Evaluation Activities contained within the Evaluation Method (or a combination of both).

7.2.7 Assessment strategy

This section of an Evaluation Activity shall provide guidance and details on how to perform the activity. It includes, as appropriate to the content of the Evaluation Activity:

a) How to assess the input from the developer or other entities for completeness with respect to the Evaluation Activity

b) How to make use of any tool types required (potentially including guidance for the calibration or setup of the tools)

c) Guidance on the steps for performing the activity.

Allowing some room for technology-specific adaptation is important for most Evaluation Activities. Finding the right balance between a precise specification of the assessment strategy and the allowed room for such adaptation is important to ensure objective and reproducible results on the one hand and meaningful results on the other hand. When the developer has more flexibility regarding how to implement the functional requirement(s) then the Evaluation Activity definition will need to allow more room for adapting the evaluation to different potential implementations. In those cases, the assessment strategy should provide general guidance on how to perform a TOE-specific refinement and adaptation rather than specifying every detail of the actions the evaluator has to perform. In general, deviations/refinements (that is, doing something other than what the EA states) from an EA are not allowed.

An assessment strategy may consist of several stages that the evaluator has to perform, in which case those stages shall be specified with the expected outcome of each stage. Some stages may depend on the result of previous stages and in this case the assessment strategy shall also define what the evaluator needs to do if one of the stages does not produce the expected result. Examples for those cases are to return to a previous stage with some modified input, terminate the Evaluation Activity indicating what to document as the result of the activity, or continue with another stage.

Depending on the needs of the evaluation context and the nature of the Evaluation Activity itself, an assessment strategy may be brief and may form part of the general description of the Evaluation Activity (e.g. the description of how to conduct a particular test or analysis action).

7.2.8 Pass/fail criteria

This section of an Evaluation Activity allows definition of criteria that the evaluator uses to determine whether the Evaluation Activity has demonstrated that the TOE has met the relevant requirement or that it has failed to meet the relevant requirement. In some cases, it may be suitable to rely on the description of the original work unit from which the Evaluation Activity is derived, but in other cases the author of the Evaluation Activity may decide that it is necessary or beneficial to state more specific criteria. Ultimately the pass/fail criteria will be concerned with determining whether the objective stated for the Evaluation Activity (7.2.2) has been met. If an Evaluation Activity mandates separate pass/fail criteria, then these criteria shall maximise the consistency of results from carrying out the Evaluation Activity in different evaluations. Making an explicit statement of specific criteria in this way minimises the chance that a different evaluator will reach a different conclusion for the Evaluation Activity, given the same evidence. In general, therefore the pass/fail criteria should be made as specific as possible.

Ways of achieving specific pass/fail criteria for analysing documents include expressing criteria in terms of the presence or absence of specific features, for example the presence of the detailed configuration of a communication stack or the set of failure triggers of an execution environment, and in terms of 'yes/no' answers to specific 'closed' questions (perhaps supported by answers obtained to other 'open' questions).

Ways of achieving specific pass/fail criteria for tests would be to express the criteria in terms of a particular visible result, such as observing successful communication on a channel, or receiving an error message indicating that the channel setup has failed or observing a memory access/setting. A phrase such as "the TOE deletes the data" would generally be a poor choice as a pass/fail criterion, because it is not clear how this deletion is to be determined by the evaluator: a better choice would be "the TOE returns a 'file not found' error" or "the evaluator uses <a named interface call> and confirms that the file is not present on the file-list returned". Another method of expressing specific pass/fail criteria for Evaluation Activities would be in terms of determining compliance with specific clauses of an identified standard, or in terms of comparison with a reference model or set of examples such as the ISO/IEC 18045 attack potential model or a specific attack potential model as defined for some IT product types.

However, it is also recognised that criteria will generally need to allow for differences in implementation details between different TOEs. Therefore, the pass/fail criteria may also be described in terms of the objective defined for the Evaluation Activity (7.2.2).

If an Evaluation Activity does not require pass/fail other than those given in the work unit from which it is derived, then this section is not required.

7.2.9 Requirements for reporting

As stated in 6.2.9, specific requirements for reporting (in the ETR and possibly in other outputs) may be specified for an Evaluation Activity – the requirements may be stated at the level of the Evaluation Method, or the level of individual Evaluation Activities. At this level the defined requirements for reporting would generally be intended to support visibility and reproducibility of the pass/fail judgement by documenting answers to particular questions, rationale for conclusions, or giving a clear description of the result of a particular test. In particular, where pass/fail criteria are expected to require evaluator judgements then the requirements for reporting shall include recording of specific factors defined to be involved in making the judgment and reaching the pass/fail conclusion.

If an Evaluation Activity does not require reports or report details other than those given in the work unit from which it is derived, then this section is not required.

7.2.10 Rationale for the Evaluation Activity

The Evaluation Activity shall include a justification for its derivation from one or more work units in ISO/IEC 18045 (or equivalent work unit definition for an extended SAR). That justification may contain an explanation why work units had to be reworked for the scope and depth of an evaluation of a specific technology or TOE type. The combination of rationale at the levels of Evaluation Method (see 6.2.10) and Evaluation Activity shall justify that the Evaluation Method addresses all aspects of the ISO/IEC 15408-3 action elements to which it applies. Additionally, the combined rationale shall describe how the derivation from the original action elements or work units ensures that the Evaluation Activity is complete with respect to the evaluation context in which the Evaluation Activity is intended to be applied.

NOTE The rationale may identify and justify that some aspects are not applicable for its particular evaluation context.

If the Evaluation Activity defines pass/fail criteria that are different from the work units it is derived from, then the justification shall provide reasons for the new criteria's feasibility and effectiveness.

The rationale may, if appropriate, identify specific assumptions that are made for the evaluation context.

The rationale may be given either at the level of the Evaluation Method, or at the level of an individual Evaluation Activity.

Bibliography

[1] ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

[2] *ISO/IEC 19896-3, Information technology — Security techniques — Competence requirements for information security testers and evaluators – Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators*

[3] *ISO/IEC 15408-5:20XX, IT Security techniques — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*