

<b>COMMITTEE DRAFT</b> <b>ISO/IEC CD 15408-4</b>		Reference document: <b>SC 27 N18703</b>	
Date: <b>2018-06-25</b>		Supersedes document WG 3 N1472	
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 technology - Security techniques  Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: <b>2018-08-20</b>  Please submit your comments via the online balloting application by the due date indicated.		
<b>ISO/IEC CD 15408-4, revision</b> <b>Title: IT Security techniques – Evaluation criteria for IT security -- Part 4: Framework for the specification of evaluation methods and activities</b> <b>Project: ISO/IEC 15408-4 (revision)</b>			
<b>Explanatory Report</b>			
<b>Status</b>	<b>SC 27 Decision</b>	<b>Reference documents</b>	
		<b>Input</b>	<b>Output</b>
<i>For details regarding previous development stages refer to 2<sup>nd</sup> page of this explanatory report.</i>			
<b>ISO/IEC NP 15408-4</b> <b>by subdivision</b> <b>Evaluation criteria for IT security -- Part 4</b> <b>NWIP</b>	53 <sup>rd</sup> 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]).
<b>ISO/IEC 15408-4</b> <b>1<sup>st</sup> WD</b>	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).
<b>ISO/IEC 15408-4</b> <b>2<sup>nd</sup> WD</b>	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).
<b>ISO/IEC 15408-4</b> <b>1<sup>st</sup> CD</b>	56 <sup>th</sup> WG 3 meeting, April 2018, Recommendations 8, 10 (N18471 = WG 3 N1557) / 30 <sup>th</sup> 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. 1 <sup>st</sup> CD (N18703).
<b>CD Registration and Consideration</b> In accordance with resolution 6 (see SC 27 N18710) of the 30th SC 27 Plenary meeting held in Wuhan, China, 2018-04-23/24 the hereby attached document has been registered with the ISO Central Secretariat (ITTF) as 1st Committee Draft (CD) and is being circulated for a 1st CD 8 weeks letter ballot closing by  <b>2018-08-20</b>  Medium: <a href="http://isotc.iso.org/livelink/livelink/open/jtc1sc27">http://isotc.iso.org/livelink/livelink/open/jtc1sc27</a> No. of pages: 2 + 19			

Secretariat, ISO/IEC JTC 1/SC27 –

DIN Deutsches Institut für Normung e.V., Am DIN-Platz, Burggrafenstr. 6, D-10787 [D-10772 postal] Berlin, Germany

Telephone: + 49 2601-2652; Facsimile: + 49 2601-4-2652; E-mail: [krystyna.passia@din.de](mailto:krystyna.passia@din.de), <http://www.din.de/go/jtc1sc27>

Explanatory Report (2 <sup>nd</sup> page)			
Status	SC 27 Decision	Reference documents	
		Input	Output
Study Period IT security testing, evaluation and assurance standards and techniques	51 <sup>st</sup> WG 3 meeting, Oct. 2015, Recommendations 5, 6 (N15594 = WG 3 N1251).		Terms of Reference (WG 5 N1258); 1 <sup>st</sup> /2 <sup>nd</sup> call f. contr. (WG 3 N1259 /1317)..
	52 <sup>nd</sup> WG 3 meeting, April 2016, Recommendation 5, 7 (N16026 = WG 3 N1296).	Expert contr. (WG 3 N1299, 1301).	3 <sup>rd</sup> call f. contr. (WG 3 N1377); Rapporteur's report (WG 3 N1320); Liaison to: CCDB (WG 3 = N1266).

ISO/IEC JTC 1/SC 27/WG 3 N18703

Date: 2018-06-22

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

**Warning for WDs and CDs**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

21

© ISO 2018, Published in Switzerland

22

23

24

25

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

26

27

28

29

30

31

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

32

www.iso.org

## Contents

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Overview</b> .....	<b>2</b>
<b>5 General model of evaluation methods and evaluation activities.</b> .....	<b>2</b>
<b>5.1 Concepts and model</b> .....	<b>2</b>
<b>5.2 Verb usage</b> .....	<b>4</b>
<b>6 Structure of an evaluation method</b> .....	<b>4</b>
<b>6.1 Overview</b> .....	<b>4</b>
<b>6.2 Specification of an evaluation method</b> .....	<b>6</b>
6.2.1 Overview .....	6
6.2.2 Identification of evaluation methods .....	6
6.2.3 Scope of the evaluation method .....	6
6.2.4 Dependencies .....	7
6.2.5 Required input from the developer or other entities .....	7
6.2.6 Set of evaluation activities.....	7
6.2.7 Required tool types .....	7
6.2.8 Required evaluator competences .....	7
6.2.9 Rationale for the evaluation method .....	8
6.2.10 Additional verb definitions .....	8
6.2.11 Requirements for reporting.....	8
<b>7 Structure of evaluation activities</b> .....	<b>9</b>
<b>7.1 Overview</b> .....	<b>9</b>
<b>7.2 Specification of an evaluation activity</b> .....	<b>9</b>
7.2.1 Unique Identification of the evaluation activity.....	9
7.2.2 Objective of the evaluation activity.....	9
7.2.3 Relationship of the evaluation activity to SFRs, SARs, and other evaluation activities.....	9
7.2.4 Rationale for the evaluation activity .....	9
7.2.5 Tool types required to perform the activity .....	10
7.2.6 Required evaluator competences .....	10
7.2.7 Required input from the developer or other entities .....	10
7.2.8 Assessment Strategy.....	10
7.2.9 Pass/fail criteria .....	11
7.2.10 Requirements for reporting.....	12
<b>Bibliography</b> .....	<b>13</b>

## 73 Foreword

74 ISO (the International Organization for Standardization) is a worldwide federation of national  
75 standards bodies (ISO member bodies). The work of preparing International Standards is normally  
76 carried out through ISO technical committees. Each member body interested in a subject for which a  
77 technical committee has been established has the right to be represented on that committee.  
78 International organizations, governmental and non-governmental, in liaison with ISO, also take part in  
79 the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all  
80 matters of electrotechnical standardization.

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

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

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

91 For an explanation on the meaning of ISO specific terms and expressions related to conformity  
92 assessment, as well as information about ISO's adherence to the World Trade Organization (WTO)  
93 principles in the Technical Barriers to Trade (TBT) see the following URL:  
94 [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

95 The committee responsible for this document is Joint Technical Committee ISO/IEC JTC 1, Information  
96 technology, Subcommittee SC 27, IT Security techniques.

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

## 98 Introduction

99 ISO/IEC 15408 is a multi-part standard, with five parts:

100 IT Security techniques – Evaluation criteria for IT security –

- 101                      • Part 1: Introduction and general model
- 102                      • Part 2: Security functional components
- 103                      • Part 3: Security assurance components
- 104                      • Part 4: Framework for the specification of evaluation methods and activities
- 105                      • Part 5: Pre-defined packages of security requirements

106 While the associated standard ISO/IEC 18045 provides a companion methodology for some of the  
107 assurance requirements specified in ISO/IEC 15408, ISO/IEC 15408 also allows that refined evaluation  
108 activities can be specified for use with ISO/IEC 15408. Specification of such evaluation activities is  
109 already occurring amongst practitioners and this creates a need for a specification for defining such  
110 evaluation activities.

111 This document provides a standardised framework for specifying objective, repeatable and  
112 reproducible evaluation methods 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 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 (e.g. for SFRs or SARs applied to specific technologies or TOE types). This document, ISO/IEC 15408-4, describes a framework that shall 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, STs and any documents supporting them.

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, *IT Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*,

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

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

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

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

## 3 Terms and definitions

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

## 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 shall be used for defining these more specific evaluation activities.

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

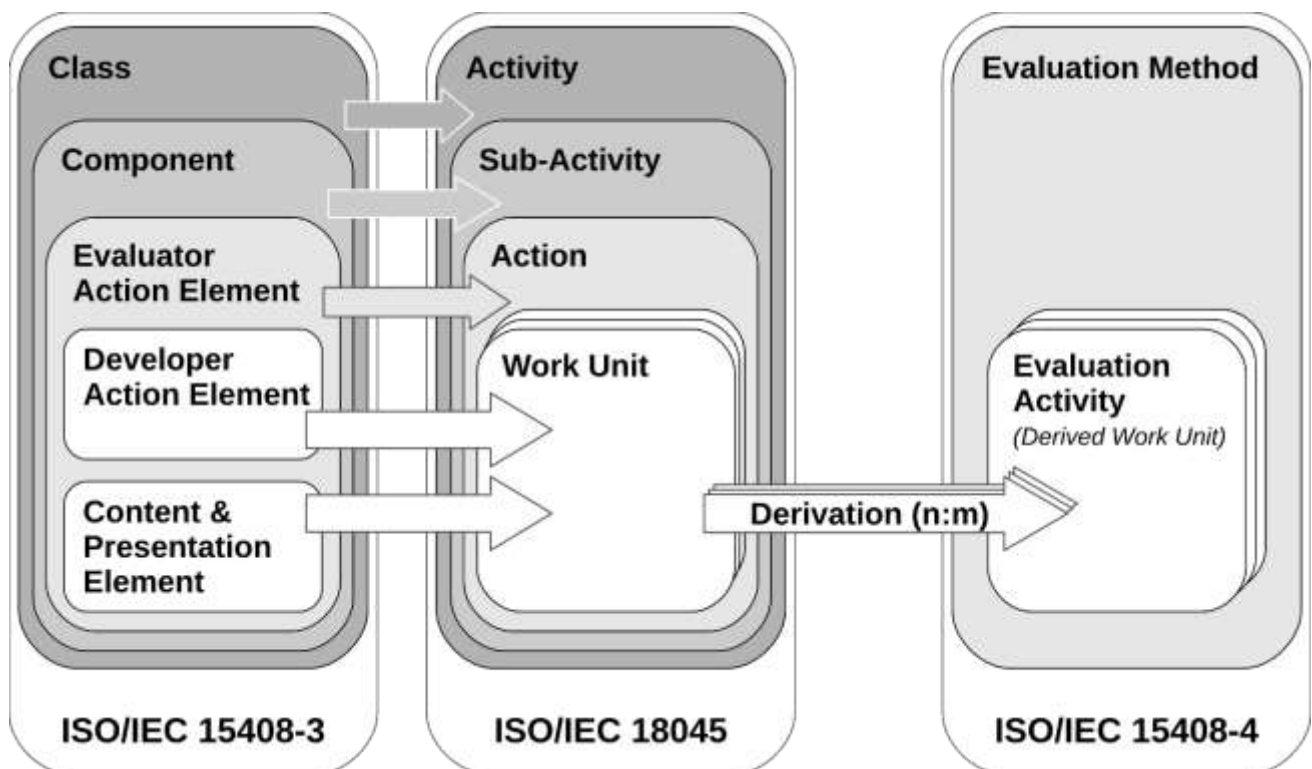
Clause 6 describes how to construct an evaluation method as a set of evaluation activities. By starting with the general structure for documenting an evaluation method, the chapter continues with minimal requirements to their identification, scope, and dependencies to other evaluation methods, activities or actions. 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, pass/fail criteria, and assessment strategies which are also subject of this chapter.

## 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, and summarised in Figure 1 below.



**Figure 1 - Mapping of ISO/IEC 15408 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 (e.g. a network device) or particular technology type (e.g. specific cryptographic functions).

In general, defining evaluation activities and evaluation methods can 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:

1. Identify the relevant ISO/IEC 18045 work units from which to derive at least one individual evaluation activity or groups of evaluation activities
2. For each work unit from which an evaluation activity is derived:
  - a. 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
  - b. Group evaluation activities into an evaluation method if necessary
  - c. State the rationale for the new evaluation activities (e.g. by referring to the developer action and content and presentation elements of the work units from which they are derived) and the evaluation method under which they are grouped as described in 6.2.9 and 7.2.4.

When starting from an SFR an alternative guideline would be as follows:

1. Identify the relevant SFR
2. Identify the SARs to be addressed for that particular SFR, and the corresponding ISO/IEC 18045 work units
3. 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
4. Map the new evaluation activities to the affected work units for the SARs
5. State the rationale for the new evaluation activities (e.g. by referring to the developer action and content and presentation elements of the work units from which they are derived), and the evaluation method under which they are grouped, as described in 6.2.9 and 7.2.4.

Subject to a suitable rationale (as described in clause 6.2.9), it is not required to have a 1:1 mapping between work units and new evaluation activities. The derivation may begin at different abstraction levels in Figure 1: for example, an author may map a different number of evaluation activities, whilst still addressing all aspects of an action (i.e. the collection of work units), where the level of detail in the mapping is related to the selected work units.. At other times the author may want to derive evaluation activities only from individual work units and would therefore provide the mappings at work unit level.

## 5.2 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 might 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 might be written in forms such as “The evaluator shall cover the PaymentMode field”.

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 CC words 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

242 requirement to have the product evaluated using a separately defined method that supports  
 243 transparency, repeatability and reproducibility of the evaluation.

244 EXAMPLE Evaluation contexts for which separate evaluation methods might be defined are:

- 245 • specific product types like network devices, smart cards, biometric devices, mobile devices
- 246 • specific security functions used in different product types like cryptographic algorithms,  
 247 cryptographic protocols, digital certificate validation, identification and authentication schemes.

248 An evaluation method comprises a collection of individual evaluation activities, with additional  
 249 information about the way in which the evaluation activities collectively meet some goal related to an  
 250 identified evaluation context.

251 The description of an evaluation method shall include:

- 252 a. the entity that is responsible for definition and maintenance of the evaluation method
- 253 b. the intended scope of the evaluation method, identifying the evaluation context in which it is  
 254 intended to be applied
- 255 c. the objective for deriving the relevant generic actions and work units in ISO/IEC 18045 (this  
 256 may be defined at the level of the evaluation method, or at the level of the evaluation activities  
 257 that it collects, or at both levels)
- 258 d. identification of each work unit in ISO/IEC 18045 that is addressed by the evaluation activities  
 259 in the evaluation method
- 260 e. identification of any extended SARs from which an evaluation method is derived
- 261 f. any known limitation of the evaluation method, or aspects not intended to be covered by the  
 262 evaluation method
- 263 g. any tool types and/or evaluator competences required to carry out the evaluation activities  
 264 contained in the evaluation method
- 265 h. any additional verbs used in the description of evaluation activities in place of verbs defined in  
 266 ISO/IEC 15408-1 [**\*\*check reference in mature part 1**]
- 267 i. requirements for reporting on the results of applying the evaluation method. This may be done  
 268 at the level of the evaluation method or at the level of each individual evaluation activity or as a  
 269 combination of both levels (for example: a general reporting requirement might be defined for  
 270 the evaluation method but with some evaluation activities requiring particular observations,  
 271 justifications or answers to specific questions to be included). The reporting requirements may  
 272 also identify some aspects to be reported as public information and other aspects to be  
 273 reported only to a specific limited audience (e.g. the developer, evaluator and evaluation  
 274 authority)

275 Where subclauses defining parts of a specification indicate that the part is optional (e.g. identification of  
 276 specific evaluator competences, or required tool types), then that part may simply be omitted from the  
 277 definition of the evaluation method or evaluation activity. It is not necessary to include a blank section  
 278 to represent the part in the definition.

## 6.2 Specification of an evaluation method

### 6.2.1 Overview

An evaluation method is specified in terms of the information identified in the subclauses below. No specific format is required for providing or presenting this information, except where specific for individual elements in the subclauses below. The purpose of stating requirements for the description of an evaluation method 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.

### 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. The identifier should be assigned at the evaluation method level (rather than 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 separate grouping.

EXAMPLE A unique identifier can 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.

For the cases defined in clause 6.2.9 where an evaluation method is 'overlain' by another evaluation method (for use in other PPs or PP-Modules) then if the original evaluation method rationale still holds (either because the original evaluation method rationale allows for the overlay, or because a justification is provided that the overlay preserves the original rationale) 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 Scope of the evaluation method

The definition of an evaluation method shall describe:

- 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 might 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. SFRs 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 that the rationale for completeness of the evaluation method (6.2.9) may give further information relevant to the scope of the evaluation method.

#### **6.2.4 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. For 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.

#### **6.2.5 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). For example, the inputs for an evaluation method dealing with media encryption TOEs might define a requirement for description of particular details of a key hierarchy.

#### **6.2.6 Set of evaluation activities**

The evaluation activities contained in the evaluation method shall be defined using the structure defined in clause 7.

#### **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 optionally identify specific evaluator competences required for its evaluation activities (e.g. using [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).

## 364 6.2.9 Rationale for the evaluation method

365 A rationale needs to be given to show that the derivation of the evaluation activities in an evaluation  
 366 method, from the original work units in ISO/IEC 18045, is appropriate. This may be given either at the  
 367 level of the evaluation method, or at the level of individual evaluation activities. If the evaluation  
 368 activities contained in the evaluation method do not have individual rationales according to 7.2.4, then  
 369 the evaluation method shall include a rationale for the derivation of evaluation activities from work  
 370 units in ISO/IEC 18045. That rationale may contain an explanation of why work units were reworked  
 371 for the scope and depth of an evaluation of a specific technology or TOE type. The rationale shall further  
 372 state how the evaluation activities it contains address all aspects of the ISO/IEC 18045 action elements  
 373 to which they apply, and shall justify that the manner in which the action elements or work units are  
 374 addressed is complete with respect to the evaluation context in which the evaluation method is  
 375 intended to be applied.

376 If an evaluation activity has been derived from an extended SAR, the rationale shall justify the  
 377 correspondence of the evaluation activity to the description of the work units for that extended SAR or,  
 378 if no such work units are defined, to the description of the extended SAR itself.

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

381 Note that an evaluation method may be 'overlain' by another evaluation method in cases where PP-  
 382 Modules are used with a Base-PP, subject to a justification for any changes made by the overlay such  
 383 that a rationale for the resulting evaluation method is still given. The rationale for the resulting  
 384 evaluation method may exist because the original evaluation method rationale allows for the overlay  
 385 (i.e. the rationale is already included in the original evaluation method definition), or else because the  
 386 PP-Module includes a separate rationale dealing with its effect on the original evaluation method. For  
 387 the case of PPs used in combination, the same principle applies: either the original evaluation method  
 388 describes the permitted variations according to the context in which it is applied, or else the resulting  
 389 overlain evaluation method deals with the effect on the original evaluation method.

390 ***[\*\*Editors' Note: it has been suggested that the presence of overlays should be discussed in the***  
 391 ***review of CD1 (note that this also affects 6.2.2). Since we allow conformance to multiple PPs to be***  
 392 ***claimed, and since PP-Modules can make modifications to the elements of their Base-PP(s) – e.g.***  
 393 ***subclause 10.3.2.1 in 15408-1 CD1 says “A PP-Module may introduce new SPD-elements to the***  
 394 ***Base-PPs and may also refine or interpret some of the SPD-elements of the Base-PPs” – it seems***  
 395 ***inevitable that we have to allow and deal with this situation when defining evaluation activities***  
 396 ***and methods. However, comments are invited on this.]***

## 397 6.2.10 Additional verb definitions

398 As described in 5.2 above, alternative verbs to those defined in ISO/IEC 15408-1 ***[\*\*check reference in***  
 399 ***mature part 1]*** may be used in the specification of an evaluation activity but any such alternative verbs  
 400 shall be defined as part of the evaluation method that contains the evaluation activity, and shall make  
 401 clear the extent to which evaluator judgement (as opposed to simple checking) is involved.

## 402 6.2.11 Requirements for reporting

403 The description of the evaluation method may include a description of reporting requirements. This  
 404 description may be given at the level of the evaluation method, or the level of individual evaluation  
 405 activities, or at both levels (e.g. giving general reporting requirements for the evaluation method, but  
 406 with some evaluation activities also requiring particular observations, justifications or answers to  
 407 specific questions to be included). Any stated requirements for reporting shall be consistent with the  
 408 requirements for the Evaluation Technical Report in ISO/IEC 18045, and any other standards required  
 409 for the conduct of the evaluation (e.g. ISO/IEC 17025 may apply).



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. For example, there may 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.

## **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 (where defined), 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 noted in the subclauses of 6.2, some of the details to be specified for evaluation activities can be included at either the evaluation method level or at the level of individual evaluation activities.

### **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.

#### **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 subclause below and to the pass/fail criteria in subclause 7.2.9. 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 Relationship of the evaluation activity 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 (e.g. an evaluation activity might 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 mapping to work units for the original SAR from ISO/IEC 18045 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 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. 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 clause 6.2.9) and evaluation activity shall justify that the evaluation method addresses all aspects of the ISO/IEC 18045 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 that the rationale may identify and justify that some aspects are not applicable for its particular evaluation context.)

If the evaluation activity mandates pass/fail criteria different from the work units it is derived from, 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.

## **7.2.5 Tool types required to perform the activity**

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 the tool 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 noted in 6.2.8, an evaluation method may optionally identify specific evaluator competences required for its evaluation activities (e.g. using [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 Required input from the developer or other entities**

As noted in 6.2.5, 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.

## **7.2.8 Assessment Strategy**

This section of an evaluation activity shall provide guidance and details 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. It is obvious that the room for technology-specific adaptation needs to increase with the flexibility a developer has to implement the functional requirement(s) to be assessed by the evaluation activity. In those cases the assessment strategy should provide general guidance how to perform a TOE-specific refinement and adaptation rather than specifying every detail of the actions the evaluator has to perform. The specification of an assessment strategy shall require the evaluator to justify any refinement and adaptation made by showing how they contribute to the objective of the evaluation activity.

An assessment strategy may consist of several stages that the evaluator has to perform. 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.

### 7.2.9 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 and consistently justifies its necessity, 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 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 (subclause 7.2.2).

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

540 **7.2.10 Requirements for reporting**

541 As noted in subclause 6.2.11, specific requirements for reporting (in the ETR and possibly in other  
542 outputs) may be specified for an evaluation activity – the requirements may be stated at the level of the  
543 evaluation method, or the level of individual evaluation activities. At this level the defined requirements  
544 for reporting would generally be intended to support transparency and reproducibility of the pass/fail  
545 judgement by documenting answers to particular questions, rationale for conclusions, or giving a clear  
546 description of the result of a particular test. In particular, where pass/fail criteria are expected to  
547 require evaluator judgements then the requirements for reporting shall include recording of specific  
548 factors defined to be involved in making the judgment and reaching the pass/fail conclusion. Similarly,  
549 where an evaluator has needed to adapt an evaluation activity for a particular TOE then the  
550 requirements for reporting shall include a justification of why the result obtained nevertheless satisfies  
551 the objective defined for the evaluation activity (as in subclause 7.2.2).

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

554

555

## Bibliography

- 556 [1] *ISO/IEC 18045, Information technology — Security techniques — Methodology for IT security*  
557 *evaluation*
- 558 [2] *ISO/IEC 19896-3 Information technology — Security techniques — Competence requirements for*  
559 *information security testers and evaluators – Part 3: Knowledge, skills and effectiveness*  
560 *requirements for ISO/IEC 15408 evaluators*
- 561 ***[(\*\*At this time, ISO/IEC 19896-3 is at DIS. The editor expects that ISO/IEC 19896-3 standard***  
562 ***will be published before this standard)]***

563