INTERNATIONAL STANDARD

**ISO/IEC 18045**

First edition
2005-10-01

# Information technology — Security techniques — Methodology for IT security evaluation

*Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI*



Reference number
ISO/IEC 18045:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

 

# Contents

Page

# Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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

ISO/IEC 18045 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*. The identical text of ISO/IEC 18045 is published by the Common Criteria Project Sponsoring Organisations as *Common Methodology for Information Technology Security Evaluation*.



## Legal notice



The governmental organizations listed below contributed to the development of this version of the Common Methodology for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Methodology for Information Technology Security Evaluations, version 2.3 (called CEM 2.3), they hereby grant non-exclusive license to ISO/IEC to use CEM 2.3 in the continued development/maintenance of the ISO/IEC 18045 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CEM 2.3 as they see fit.

| | |
|---|---|
| Australia/New Zealand: | The Defence Signals Directorate and the Government Communications Security Bureau respectively; |
| Canada: | Communications Security Establishment; |
| France: | Direction Centrale de la Sécurité des Systèmes d'Information; |
| Germany: | Bundesamt für Sicherheit in der Informationstechnik; |
| Japan: | Information Technology Promotion Agency; |
| Netherlands: | Netherlands National Communications Security Agency; |
| Spain: | Ministerio de Administraciones Públicas and Centro Criptológico Nacional; |
| United Kingdom: | Communications-Electronic Security Group; |
| United States: | The National Security Agency and the National Institute of Standards and Technology. |

# Introduction

The methodology for IT security evaluation presented in this International Standard is limited to evaluations for EAL1 through EAL4,as defined in ISO/IEC 15408. It does not provide guidance for EALs 5 through 7, nor for evaluations using other assurance packages.

The target audience for this International Standard is primarily evaluators applying ISO/IEC 15408 and certifiers confirming evaluator actions; evaluation sponsors, developers, PP/ST authors and other parties interested in IT security may be a secondary audience.

This International Standard recognises that not all questions concerning IT security evaluation will be answered herein and that further interpretations will be needed. Individual schemes will determine how to handle such interpretations, although these may be subject to mutual recognition agreements. A list of methodology-related activities that may be handled by individual schemes can be found in Annex A.

# Information technology — Security techniques — Methodology for IT security evaluation

## 1 Scope

This International Standard is a companion document to ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security*. This International Standard describes the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.

## 2 Normative references

The following referenced documents are indispensable for the application 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 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*



## 3 Terms and definitions



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



NOTE Bold-faced type is used in the definitions to indicate terms which are themselves defined in this clause.

**3.1**
**action**
evaluator action element of ISO/IEC 15408-3. These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.

**3.2**
**activity**
the application of an assurance class of ISO/IEC 15408-3.

**3.3**
**check**
to generate a **verdict** by a simple comparison. Evaluator expertise is not required. The statement that uses this verb describes what is mapped.

**3.4**
**evaluation deliverable**
any resource required from the sponsor or developer by the evaluator or overseer to perform one or more evaluation or evaluation oversight activities.

**3.5**
**evaluation evidence**
a tangible **evaluation deliverable**.

**3.6**
**evaluation technical report**
a report that documents the **overall verdict** and its justification, produced by the evaluator and submitted to an overseer.

**3.7**
**examine**
to generate a **verdict** by analysis using evaluator expertise. The statement that uses this verb identifies what is analysed and the properties for which it is analysed.

**3.8**
**interpretation**
a clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045 or **scheme** requirement.

**3.9**
**methodology**
the system of principles, procedures and processes applied to IT security evaluations.

**3.10**
**observation report**
a report written by the evaluator requesting a clarification or identifying a problem during the evaluation.

**3.11**
**overall verdict**
a *pass or fail* statement issued by an evaluator with respect to the result of an evaluation.



**3.12**
**oversight verdict**
a statement issued by an overseer confirming or rejecting an *overall verdict* based on the results of evaluation oversight activities.



**3.13**
**record**
to retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time.

**3.14**
**report**
to include evaluation results and supporting material in the **evaluation technical report** or an **observation report**.

**3.15**
**scheme**
set of rules, established by an evaluation authority, defining the evaluation environment, including criteria and **methodology** required to conduct IT security evaluations.

**3.16**
**sub-activity**
the application of an assurance component of ISO/IEC 15408-3. Assurance families are not explicitly addressed in this International Standard because evaluations are conducted on a single assurance component from an assurance family.

**3.17**
**tracing**
a simple directional relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second.

**3.18**
**verdict**
a *pass, fail or inconclusive* statement issued by an evaluator with respect to an ISO/IEC 15408 evaluator action element, assurance component, or class. Also see **overall verdict**.

**3.19**
**work unit**
the most granular level of evaluation work. Each evaluation methodology action comprises one or more work units, which are grouped within the evaluation methodology action by ISO/IEC 15408 content and presentation of evidence or developer action element. The work units are presented in this International Standard in the same order as ISO/IEC 15408 elements from which they are derived. Work units are identified in the left margin by a symbol such as *4:ALC_TAT.1-2*. In this symbol, the first digit (*4*) indicates the EAL; the string *ALC_TAT.1* indicates ISO/IEC 15408 component (i.e. this International Standard sub-activity), and the final digit ( *2*) indicates that this is the second work unit in the ALC_TAT.1 sub-activity.

# 4 Symbols and abbreviated terms

**ETR** Evaluation Technical Report

**OR** Observation Report

# 5 Overview

## 5.1 Organisation of this International Standard



Clause 6 defines the conventions used in this International Standard.

Clause 7 describes general evaluation tasks with no verdicts associated with them as they do not map to ISO/IEC 15408 evaluator action elements.



Clause 8 defines the evaluation of a PP.

Clause 9 defines the evaluation of an ST.

Clauses 10 to 13 define the minimal evaluation effort for achieving EAL1 to EAL4 evaluations and to provide guidance on ways and means of accomplishing the evaluation.

Clause 14 defines the flaw remediation evaluation activities.

Annex A covers the basic evaluation techniques used to provide technical evidence of evaluation results.

# 6 Document Conventions

## 6.1 Terminology

Unlike ISO/IEC 15408, where each element maintains the last digit of its identifying symbol for all components within the family, this International Standard may introduce new work units when an ISO/IEC 15408 evaluator action element changes from sub-activity to sub-activity; as a result, the last digit of the work unit's identifying symbol may change although the work unit remains unchanged. For example, because an additional work unit labeled 4:ADV_FSP.2-7 was added at EAL4, the subsequent sequential numbering of FSP work units is offset by one. Thus work unit 3:ADV_FSP.1-8 is now mirrored by work unit 4:ADV_FSP.2-9; each express the same requirement though their numbering no longer directly correspond.

Any methodology-specific evaluation work required that is not derived directly from ISO/IEC 15408 requirements is termed *task* or *sub-task*.

## 6.2 Verb usage

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 ISO/IEC 15408 words in an evaluation. The described method is normative, meaning that the verb usage is in accordance with ISO definitions for these verbs; that is: the auxiliary verb *should* is used when the described method is strongly preferred and the auxiliary verb *may* is used where the described method(s) is allowed but no preference is indicated. (The auxiliary verb *shall* is used only for the text of work units.)

The verbs *check*, *examine*, *report* and *record* are used with a precise meaning within this International Standard and the clause 3 should be referenced for their definitions.

## 6.3 General evaluation guidance

Material that has applicability to more than one sub-activity is collected in one place. Guidance whose applicability is widespread (across activities and EALs) has been collected into Annex A. Guidance that pertains to multiple sub-activities within a single activity has been provided in the introduction to that activity. If guidance pertains to only a single sub-activity, it is presented within that sub-activity.

## 6.4 Relationship between ISO/IEC 15408 and ISO/IEC 18045 structures



There are direct relationships between ISO/IEC 15408 structure (i.e. class, family, component and element) and the structure of this International Standard. Figure 1 illustrates the correspondence between ISO/IEC 15408 constructs of class, family and evaluator action elements and evaluation methodology activities, sub-activities and actions. However, several evaluation methodology work units may result from the requirements noted in ISO/IEC 15408 developer action and content and presentation elements.



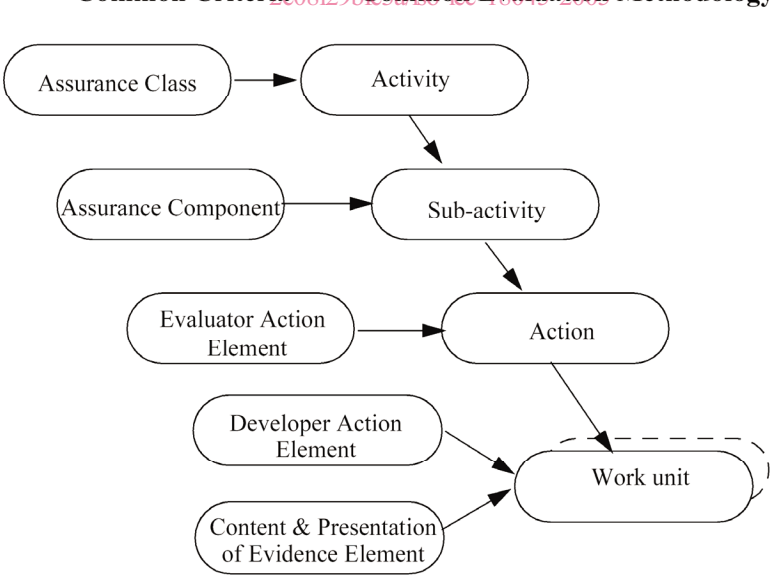


**Figure 1 - Mapping of ISO/IEC 15408 and ISO/IEC 18045 structures**

## 6.5 Evaluator verdicts

The evaluator assigns verdicts to the requirements of ISO/IEC 15408 and not to those of this International Standard. The most granular ISO/IEC 15408 structure to which a verdict is assigned is the evaluator action element (explicit or implied). A verdict is assigned to an applicable ISO/IEC 15408 evaluator action element as

a result of performing the corresponding evaluation methodology action and its constituent work units. Finally, an evaluation result is assigned, as described in ISO/IEC 15408-1, Subclause 6.3.

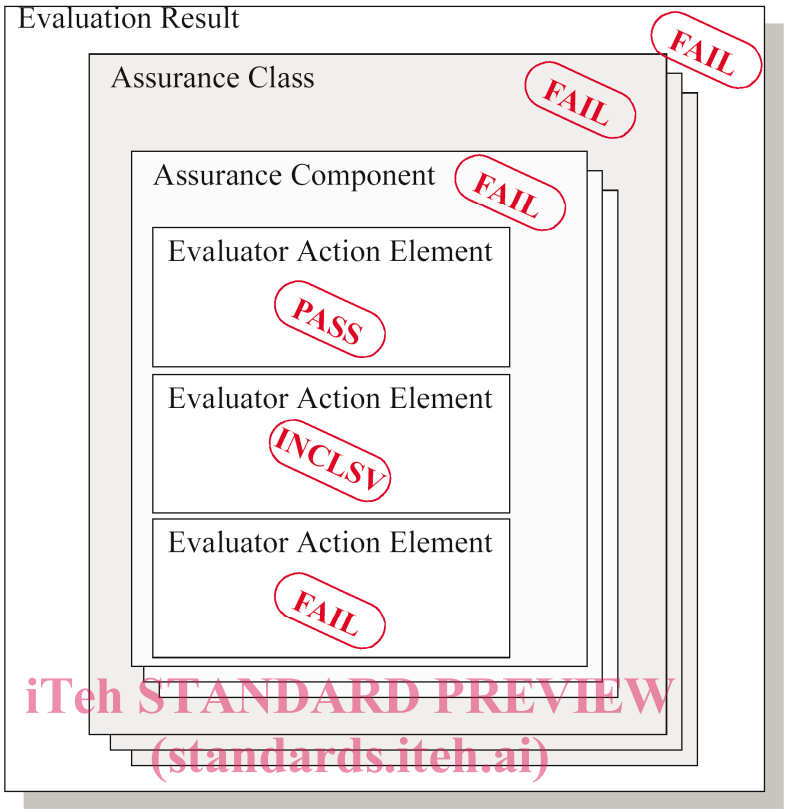




**Figure 2 - Example of the verdict assignment rule**

This International Standard recognises three mutually exclusive verdict states:

a) Conditions for a *pass* verdict are defined as an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, ST or TOE under evaluation are met. The conditions for passing the element are defined as the constituent work units of the related evaluation methodology action;

b) Conditions for an *inconclusive* verdict are defined as an evaluator incompletion of one or more work units of the evaluation methodology action related to ISO/IEC 15408 evaluator action element;

c) Conditions for a *fail* verdict are defined as an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, ST, or TOE under evaluation are not met.

All verdicts are initially *inconclusive* and remain so until either a *pass* or *fail* verdict is assigned.

The overall verdict is *pass* if and only if all the constituent verdicts are also *pass*. In the example illustrated in Figure 2, if the verdict for one evaluator action element is *fail* then the verdicts for the corresponding assurance component, assurance class, and overall verdict are also *fail*.

# 7 General evaluation tasks

## 7.1 Introduction

All evaluations, whether of a PP or TOE (including ST), have two evaluator tasks in common: the input task and the output task. These two tasks, which are related to management of evaluation evidence and to report

generation, are described in this clause. Each task has associated sub-tasks that apply to, and are normative for all ISO/IEC 15408 evaluations (evaluation of a PP or a TOE).

Although ISO/IEC 15408 does not mandate specific requirements on these evaluation tasks, this International Standard does so where it is necessary. In contrast to the activities described elsewhere in this International Standard, these tasks have no verdicts associated with them as they do not map to ISO/IEC 15408 evaluator action elements; they are performed in order to comply with this International Standard.

## 7.2 Evaluation input task

### 7.2.1 Objectives

The objective of this task is to ensure that the evaluator has available the correct version of the evaluation evidence necessary for the evaluation and that it is adequately protected. Otherwise, the technical accuracy of the evaluation cannot be assured, nor can it be assured that the evaluation is being conducted in a way to provide repeatable and reproducible results.

### 7.2.2 Application notes

The responsibility to provide all the required evaluation evidence lies with the sponsor. However, most of the evaluation evidence is likely to be produced and supplied by the developer, on behalf of the sponsor. Since the assurance requirements apply to the entire TOE, evaluation evidence pertaining to all products that are part of the TOE is made available to the evaluator. The scope and required content of such evaluation evidence is independent of the level of control that the developer has over each of the products that are part of the TOE. For example, if a high-level design is required, then the High-level design (ADV_HLD) requirements will apply to all subsystems that are part of the TSF. In addition, assurance requirements that call for procedures to be in place (for example, CM capabilities (ACM_CAP) and Delivery (ADO_DEL)) will also apply to the entire TOE (including any product from another developer).



It is recommended that the evaluator, in conjunction with the sponsor, produce an index to required evaluation evidence. This index may be a set of references to the documentation. This index should contain enough information (e.g. a brief summary of each document, or at least an explicit title, indication of the subclauses of interest) to help the evaluator to find easily the required evidence.



It is the information contained in the evaluation evidence that is required, not any particular document structure. Evaluation evidence for a sub-activity may be provided by separate documents, or a single document may satisfy several of the input requirements of a sub-activity.

The evaluator requires stable and formally-issued versions of evaluation evidence. However, draft evaluation evidence may be provided during an evaluation, for example, to help an evaluator make an early, informal assessment, but is not used as the basis for verdicts. It may be helpful for the evaluator to see draft versions of particular appropriate evaluation evidence, such as:

a) test documentation, to allow the evaluator to make an early assessment of tests and test procedures;

b) design documents, to provide the evaluator with background for understanding the TOE design;

c) source code or hardware drawings, to allow the evaluator to assess the application of the developer's standards.

Draft evaluation evidence is more likely to be encountered where the evaluation of a TOE is performed concurrently with its development. However, it may also be encountered during the evaluation of an already-developed TOE where the developer has had to perform additional work to address a problem identified by the evaluator (e.g. to correct an error in design or implementation) or to provide evaluation evidence of security that is not provided in the existing documentation (e.g. in the case of a TOE not originally developed to meet the requirements of ISO/IEC 15408).

#### 7.2.3 Management of evaluation evidence sub-task

##### 7.2.3.1 Configuration control

The evaluator shall perform configuration control of the evaluation evidence.

ISO/IEC 15408 implies that the evaluator is able to identify and locate each item of evaluation evidence after it has been received and is able to determine whether a specific version of a document is in the evaluator's possession.

The evaluator shall protect the evaluation evidence from alteration or loss while it is in the evaluator's possession.

##### 7.2.3.2 Disposal

Schemes may wish to control the disposal of evaluation evidence at the conclusion of an evaluation. The disposal of the evaluation evidence should be achieved by one or more of:

a) returning the evaluation evidence;

b) archiving the evaluation evidence;

c) destroying the evaluation evidence.

##### 7.2.3.3 Confidentiality



An evaluator may have access to sponsor and developer commercially-sensitive information (e.g. TOE design information, specialist tools), and may have access to nationally-sensitive information during the course of an evaluation. Schemes may wish to impose requirements for the evaluator to maintain the confidentiality of the evaluation evidence. The sponsor and evaluator may mutually agree to additional requirements as long as these are consistent with the scheme.



Confidentiality requirements affect many aspects of evaluation work, including the receipt, handling, storage and disposal of evaluation evidence.

### 7.3 Evaluation output task

#### 7.3.1 Objectives

The objective of this subclause is to describe the Observation Report (OR) and the Evaluation Technical Report (ETR). Schemes may require additional evaluator reports such as reports on individual units of work, or may require additional information to be contained in the OR and the ETR. This International Standard does not preclude the addition of information into these reports as this International Standard specifies only the minimum information content.

Consistent reporting of evaluation results facilitates the achievement of the universal principle of repeatability and reproducibility of results. The consistency covers the type and the amount of information reported in the ETR and OR. ETR and OR consistency among different evaluations is the responsibility of the overseer.

The evaluator performs the two following sub-tasks in order to achieve this International Standard requirements for the information content of reports:

a) write OR sub-task (if needed in the context of the evaluation);

b) write ETR sub-task.