SLOVENSKI STANDARD
oSIST prEN ISO/IEC 18045:2020

01-januar-2020

Informacijska tehnologija - Varnostne tehnike - Metodologija za varnostno vrednotenje IT (ISO/IEC 18045:2008)

Information technology - Security techniques - Methodology for IT security evaluation (ISO/IEC 18045:2008)

Informationstechnik - Sicherheitstechniken - Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2008)

Technologies de l'information - Techniques de sécurité - Méthodologie pour l'évaluation de sécurité TI (ISO/IEC 18045:2008)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 18045**

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 18045:2020 **en**

INTERNATIONAL STANDARD

ISO/IEC 18045

Second edition
2008-08-15

Corrected version
2014-01-15

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 18045:2008(E)

COPYRIGHT PROTECTED DOCUMENT

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*. The common XML source for both publications can be found at http://www.commoncriteriaportal.org/cc/ .

This second edition cancels and replaces the first edition (ISO/IEC 18045:2005), which has been technically revised.

This second corrected version of ISO/IEC 18045:2008 incorporates miscellaneous editorial corrections related to the following:

— consistency with the corrected versions of ISO/IEC 15408-3:2008 and ISO/IEC 15408-1:2009;

— APE_CCL and ASE_CCL, APE_SPD and ASE_SPD, AGD_PRE, ALC_CMC, ALC_DVS, ADV_TDS, ASE_TSS, AVA_VAN, and ADV_FSP.

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 3.1 (called CEM 3.1), they hereby grant non-exclusive license to ISO/IEC to use CEM 3.1 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 3.1 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 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 the “Evaluation criteria for IT security”, ISO/IEC 15408. This International Standard defines 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.

This International Standard does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

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 Terms which are presented in bold-faced type are themselves defined in this Subclause.

3.1
action
evaluator action element of ISO/IEC 15408-3

NOTE 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
application of an assurance class of ISO/IEC 15408-3

3.3
check
generate a **verdict** by a simple comparison

NOTE 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 evaluation authority to perform one or more evaluation or evaluation oversight activities

3.5
evaluation evidence
tangible **evaluation deliverable**

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

3.7
examine
generate a **verdict** by analysis using evaluator expertise

NOTE The statement that uses this verb identifies what is analysed and the properties for which it is analysed.

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

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

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

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

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

3.13
record
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
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
application of an assurance component of ISO/IEC 15408-3

NOTE 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
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
pass, fail or inconclusive statement issued by an evaluator with respect to an ISO/IEC 15408 evaluator action element, assurance component, or class

NOTE Also see **overall verdict**.

3.19
work unit
most granular level of evaluation work

NOTE 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 ALC_TAT.1-2. In this symbol, 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 addresses the work necessary for reaching an evaluation result on a PP.

Clauses 9 to 15 define the evaluation activities, organised by Assurance Classes.

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

Annex B provides an explanation of the Vulnerability Analysis criteria and examples of their application

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.

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