SLOVENSKI STANDARD
oSIST prEN ISO/IEC 19896-3:2025

01-marec-2025

Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Zahteve za usposobljenost osebja za ugotavljanje skladnosti z varnostjo IT - 3. del: Zahteve glede znanja in spretnosti ocenjevalcev in certifikacijskih organov v skladu s standardom ISO/IEC 15408 (ISO/IEC DIS 19896-3:2024)

Information security, cybersecurity and privacy protection - Requirements for the competence of IT security conformance assessment body personnel - Part 3: Knowledge and skills requirements for ISO/IEC 15408 evaluators and certifiers (ISO/IEC DIS 19896-3:2024)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Anforderungen an die Kompetenz des Personals von Konformitätsbewertungsstellen für IT-Sicherheit - Teil 3: Anforderungen an die Kenntnisse und Fähigkeiten von Evaluatoren und Zertifizierern nach ISO/IEC 15408 (ISO/IEC DIS 19896-3:2024)

Sécurité de l'information, cybersécurité et protection de la vie privée - Exigences relatives aux compétences du personnel des organismes d'évaluation de la conformité de la sécurité TI - Partie 3: Exigences en matière de connaissances et de compétences pour les évaluateurs et certificateurs de l'ISO/IEC 15408 (ISO/IEC DIS 19896-3:2024)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 19896-3**

ICS:

03.100.30	Vodenje ljudi	Management of human resources
35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 19896-3:2025 **en,fr,de**

DRAFT International Standard

ISO/IEC DIS 19896-3

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel —

Part 3: Knowledge and skills requirements for ISO/IEC 15408 evaluators and certifiers

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2024-12-16

Voting terminates on:
2025-03-10

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/IEC DIS 19896-3:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

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 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 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 www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 19896 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 www.iso.org/members.html.

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations. It 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. Many certification and evaluation schemes as well as certification bodies have been developed using the ISO/IEC 15408 series and ISO/IEC 18045 as a basis, which permits comparability between the results of evaluation projects.

The evaluation process usually relies on both pre-defined tests/methods for a type of TOE, and TOE-specific tests/methods that are defined for a given implementation of the TOE. Hence, the competence of the individual evaluators, which are expected not only to apply pre-defined tests/methods but to define and run TOE-specific tests/methods, is key to ensure the comparability and repeatability of evaluation results which is the foundation for mutual recognition.

[Editor's Note: This standard uses the phrase "organizations implementing an evaluation scheme". Experts and national bodies are kindly requested to review if this wording can be improved, i.e. if this concept can be expressed more clearly.]

This document establishes a baseline for the minimum competence of ISO/IEC 15408 evaluators and certifiers with the goal of establishing conformity in the requirements for the training of ISO/IEC 15408 evaluators and certifiers associated with IT organizations implementing evaluation schemes and certification bodies. It provides the specialized requirements to demonstrate the competence of individuals in performing IT product security evaluations and certifications in accordance with the ISO/IEC 15408 series and ISO/IEC 18045. ISO/IEC 15408-1 describes the general framework for competences including the various elements of competence: knowledge, skills, experience and education. This document includes knowledge and skills especially in the following areas.

— Information security

  Knowledge: Information security principles, information security properties, information security threats and vulnerabilities

  Skills: Understand information security requirements, understand the context

— Information security evaluation

  Knowledge: Knowledge of the ISO/IEC 15408 series and ISO/IEC 18045, laboratory management system

  Skills: Basic evaluation skills, core evaluation skills, skills required when evaluating specific security assurance classes, skills required when evaluating specific security functional requirements classes

— Information systems architecture

  Knowledge: Technology being evaluated

  Skills: Understand the interaction of security components and information

— Information security testing

  Knowledge: Information security testing techniques, information security testing tools, product development lifecycle, test types

  Skills: Create and manage an information security test plan, design information security tests, prepare and conduct information security tests

The audience for this document includes certification authorities, testing laboratory accreditation bodies, organizations implementing evaluation schemes, laboratories, evaluators and organizations offering professional credentialing

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel —

Part 3: Knowledge and skills requirements for ISO/IEC 15408 evaluators and certifiers

1 Scope

This document provides the specialized requirements to demonstrate competence of individuals in performing IT product security evaluations and certifications in accordance with the ISO/IEC 15408 series and ISO/IEC 18045.

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 19896-1, *Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel — Part 1: Introduction and concepts*

ISO/IEC 15408 (all parts), *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security*

ISO/IEC 18045:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19896-1, ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 18045 and the following apply.

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

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

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

3.1
supporting document
document that specifies the use of the Common Criteria (CC) or Common Methodology for Information Technology Security Evaluation (CEM) in a particular field or domain of technology

Note 1 to entry: Such document may be either mandatory or guidance and generally specifies harmonised interpretations of the CC and CEM where deemed necessary and/or useful.

3.2
technical domain
family of IT products that require specific technical competencies, especially with regard to the vulnerability analysis, requiring a common understanding of the attack potential for performing the evaluation

4 Knowledge

4.1 Knowledge required for evaluators

4.1.1 General

Subclauses 4.1.2 to 4.1.6 address the knowledge that is needed for evaluation to the ISO/IEC 15408 series and ISO/IEC 18045.

Some knowledge is required for every evaluator independent of their specific task, while other knowledge is required only depending on the specific evaluation task and TOE the evaluator is assigned to.

NOTE Previous experience in tasks related to the use of ISO/IEC 15408 and its related documents including, but not limited to, performing related work such as consultancy, product development, research and specification of requirements can contribute to the elements of knowledge that are required for competence.

4.1.2 Knowledge of ISO/IEC 15408 and ISO/IEC 18045

4.1.2.1 ISO/IEC 15408-1

Every evaluator shall be able to demonstrate knowledge about the topics required to fulfil their role according to their competence level and on which they are authorized to work.

Every evaluator's knowledge shall include:

a) the terms and definitions defined in ISO/IEC 15408 (all parts);

b) the terms and definitions defined in ISO/IEC 18045;

c) the context for ISO/IEC 15408 evaluations; and

d) the general model for the ISO/IEC 15408 series given in ISO/IEC 15408-1.

When the evaluator's role and competency level demand it, their knowledge shall include the relevant items of the following list:

e) tailoring security requirements: operations, dependencies between components and extended components;

f) specification of protection profiles, modules, configurations and packages;

g) handling of evaluation results;

h) specification of security targets;

i) composition models;

j) multi-assurance approach; and

k) modularization concepts.

4.1.2.2 ISO/IEC 15408-2

Every evaluator shall be able to demonstrate knowledge about the security functional requirements (SFRs) of ISO/IEC 15408-2 required to fulfil their role according to their competence level and the technology types

on which the evaluator is authorized to work, as well as any dependent SFRs. Examples for the knowledge required by ISO/IEC 15408-2 are given in Annex C.

If the evaluator needs to demonstrate competence in ISO/IEC 15408-2, then the knowledge in the respective security functional requirements shall be demonstrated.

4.1.2.3 ISO/IEC 15408-3

Every evaluator shall be able to demonstrate knowledge about the security assurance requirements (SARs) given in ISO/IEC 15408-3 required to fulfil their role according to their competence level and that are specified by Security Targets (ST) on which the evaluator is authorized to work on. The knowledge of particular SAR components shall include those on which the evaluator is authorized to work. Examples for the knowledge required by ISO/IEC 15408-3 are given in Annex B.

If the evaluator needs to demonstrate competence in ISO/IEC 15408-3, then the knowledge in the respective security assurance requirements shall be demonstrated.

4.1.2.4 ISO/IEC 15408-4

If the evaluator needs to demonstrate competence in ISO/IEC 15408-4, then the following shall be demonstrated:

a) the framework used for deriving evaluation activities from work units in ISO/IEC 18045;

b) the general model of evaluation methods and evaluation activities; and

c) defining evaluation activities for extended SARs.

4.1.2.5 ISO/IEC 15408-5

If the evaluator needs to demonstrate competence in ISO/IEC 15408-5, then those specified in ISO/IEC 15408-5 shall be demonstrated.

4.1.2.6 ISO/IEC 18045

Every evaluator shall demonstrate:

a) the evaluation process: this process is described in ISO/IEC 18045:2022, Clause 9; and

b) security evaluation method and activities: this information is given in ISO/IEC 18045.

Additionally, every evaluator shall have the necessary knowledge required by the evaluation methods and activities specified for the assurance classes on which they are authorized to work. Examples for the knowledge required by ISO/IEC 18045 are given in Annex B.

Every evaluator working in the ALC class shall additionally have the following knowledge:

c) site security (including physical, technical, organisational and personnel security requirements and measures, IT logical security / network security);

d) site audits;

e) secure development processes;

f) Software/Hardware Bill of Materials;

g) configuration management and development practices;

h) information security standards; and

i) methods for product development and its life cycle.

4.1.3 Knowledge of the assurance paradigm

4.1.3.1 Knowledge of the evaluation scheme and overall evaluation framework

Evaluation schemes usually specify an overall evaluation framework with scheme-specific scope, regulations and application rules. Organizations implementing such an evaluation scheme as well as certification bodies working within such an evaluation scheme typically define specifications based on the scheme. Within the predefined limits they also define their operational framework such as policies and procedures that are specific to the evaluation scheme.

Every evaluator shall be able to demonstrate knowledge of the evaluation schemes as required to fulfil their role according to their competence level and that is applicable to the evaluation schemes in which they are authorized to work.

Every evaluator shall have the necessary knowledge of the following items that are of relevance to the evaluation-related work on which the evaluator is authorized to work:

a) scope of the evaluation scheme;

b) any (sector-specific) regulations, legislation, policies, and further specifics;

c) different types of evaluation / certification procedures (e.g. initial certification, assurance continuity as re-certification, re-assessment, maintenance);

d) guidance to organizations implementing evaluation schemes and to their evaluators;

e) recognition arrangements; and

f) vulnerability disclosure and handling.

g) scope of the implementing organization;

h) policies regarding evaluation projects including entry criteria, time limits, site visit requirements;

i) specific supporting documents;

j) specific interpretations;

k) specific guidance for evaluators;

l) approved protection profiles and their supporting documents;

m) specific assurance methods;

n) reporting requirements;

o) vulnerability disclosure and handling;

p) quality; and

q) laboratory approval requirements.

NOTE See ISO/IEC 18045:2022, A.5 for guidance to evaluation schemes on this topic.

4.1.3.2 Knowledge of the certification body

Every evaluator shall be able to demonstrate knowledge of the certification bodies as required to fulfil their role according to their competence level and that is applicable to the certification bodies for which they are authorized to work.

NOTE Certification bodies are called “evaluation authority” in ISO/IEC 15408-1.

EXAMPLE The "Common Criteria Recognition Arrangement (CCRA)" and the "Senior Officials Group Information Systems Security (SOG-IS)" are mutual recognition arrangements under which several evaluation schemes with their certification bodies for Common Criteria certification work. The “EU Common Criteria Scheme (EUCC)” is an evaluation scheme itself with several assigned certification bodies.

Every evaluator shall have the necessary knowledge of the following items that are of relevance to the evaluation-related work on which the evaluator is authorized to work:

a) scope of the certification body;

b) different types of evaluation/certification procedures (e.g. initial certification, assurance continuity as re-certification, re-assessment, maintenance);

c) certification body policies;

d) policies regarding to evaluation projects including entry criteria, time limits, site visit requirements;

e) specific interpretations;

f) specific supporting documents;

g) specific guidance;

h) specific assurance methods;

i) reporting requirements;

j) vulnerability disclosure and handling; and

k) quality.

4.1.3.3 Knowledge of the laboratory and its management system

Every evaluator shall have knowledge of:

a) the laboratory’s management system, including policies, processes and procedures that are applicable to evaluators;

b) laboratory approved methods; and

c) laboratory competence requirements.

NOTE Management systems vary greatly in their implementations. However, items such as document control, record control, control of nonconforming testing and/or calibration work, handling of technical records, and conflict of interest are often the direct responsibility of every evaluator. Most laboratory management systems are based on ISO/IEC 17025.

4.1.4 Knowledge of information security

Every evaluator shall have the necessary knowledge of the following concepts in order to fulfil their role and in accordance with the requirements of the evaluation scheme:

a) security principles;

b) security properties;

c) mechanisms of attack;

d) attack potential;

e) cryptography;

f) secure development life cycles;

g) security testing; and

h) vulnerabilities and weaknesses.

Specific additional deeper / broader knowledge on information security topics outlined in the preceding bullet list that is expected from evaluators is addressed in Clause 4.1.5.

4.1.5 Knowledge of the technology

4.1.5.1 Knowledge of technology types

The ISO/IEC 15408 series and ISO/IEC 18045 can be used in the evaluation of a wide variety of information technologies. These technologies are often classified into various technology types by organizations implementing evaluation schemes, certification bodies or others.

Every evaluator shall have the necessary knowledge of the information technology types on which the evaluators are authorized to work, including the common security architectures deployed for that technology type.

NOTE Annex A provides an informative list of knowledge topics presented by commonly identified technology types.

EXAMPLE Commonly identified technology types include:

— access control devices and systems;

— encryption, key management and PKI systems, products for digital signatures;

— databases;

— operating systems;

— network and network-related devices and systems;

— mobile devices and systems;

— multi-function devices;

— ICs, smart cards and smart-card related devices and systems;

— hardware devices;

— detection devices and systems; and

— data protection, biometric systems and devices, trusted computing.

4.1.5.2 Knowledge of Protection Profiles, packages and supporting documents

Every evaluator shall have the necessary knowledge of the following, where they are applicable for the information technology the evaluators on which they are authorized to work :

a) protection profiles, functional packages, assurance packages, PP-Modules, PP-Configurations and any related supporting documents specified in connection with the evaluator's work;

b) any additional evaluation methods and assurance activities specified as applicable to an evaluation; and

c) how to determine if any interpretations or guidance in regard to protection profiles, packages and related supporting documents have been issued and whether they are applicable to a particular evaluation project.

Additionally, they may have knowledge of

d) specific supporting documents, e.g. from JIL or CCRA cPP; and

EXAMPLE

— technical domain Smart Cards