SLOVENSKI STANDARD
oSIST prEN ISO/IEC 19896-3:2022

01-november-2022

IT varnostne tehnike - Zahteve za usposobljenost za preskuševalce in ocenjevalce informacijske varnosti - 3. del: Zahteve glede znanja, veščin in učinkovitosti za ocenjevalce ISO/IEC 15408 (ISO/IEC 19896-3:2018)

IT security techniques - Competence requirements for information security testers and evaluators - Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators (ISO/IEC 19896-3:2018)

IT-Sicherheitstechniken - Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit - Teil 3: Anforderungen an die Kenntnisse, Fähigkeiten und Effektivität von Evaluatoren nach ISO/IEC 15408 (ISO/IEC 19896□3:2018)

Techniques de sécurité IT - Exigences en matière de compétences des spécialistes en tests et évaluations de la sécurité de l'information - Partie 3: Exigences en matière de connaissances, compétences et efficacité des spécialistes en évaluations ISO/IEC 15408 (ISO/IEC 19896-3:2018)

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 19896-3:2022 **en,fr,de**

INTERNATIONAL STANDARD

ISO/IEC 19896-3

First edition
2018-08

IT security techniques — Competence requirements for information security testers and evaluators —

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

Techniques de sécurité IT — Exigences en matière de compétences des spécialistes en tests et évaluations de la sécurité de l'information —

Partie 3: Exigences en matière de connaissances, compétences et efficacité des spécialistes en évaluations ISO/IEC 15408

Reference number
ISO/IEC 19896-3:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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, *IT Security techniques*.

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 evaluation authorities 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.

One important factor in assuring comparability of the results of such evaluations is to understand that the evaluation process includes the specification of both objective and subjective assurance measures. Hence, the competence of the individual evaluators is important when the comparability and repeatability of evaluation results are the foundation for mutual recognition.

ISO/IEC 17025, provides general requirements for the competence of testing and calibration laboratories. In ISO/IEC 17025:2017, 5.2.1, it is stated that "*Personnel performing specific tasks shall be qualified on the basis of appropriate education, training, experience and/or demonstrated skills*".

This document establishes a baseline for the minimum competence of ISO/IEC 15408 evaluators with the goal of establishing conformity in the requirements for the training of ISO/IEC 15408 evaluator professionals associated with IT product evaluation schemes and authorities. It provides the specialized requirements to demonstrate the competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045. ISO/IEC 15408-1 describes the general framework for competences including the various elements of competence; knowledge, skills, experience, education and effectiveness. 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 ISO/IEC 15408 (all parts) 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 validation and certification authorities, testing laboratory accreditation bodies, evaluation schemes, laboratories, evaluators and organizations offering professional credentialing.

IT security techniques — Competence requirements for information security testers and evaluators —

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

1 Scope

This document provides the specialized requirements to demonstrate competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) 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, *IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

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

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

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 17025, 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 http://www.electropedia.org/

3.1
evaluation scheme
organization implementing policies and a set of rules established by an evaluation authority, defining the evaluation environment, including criteria and methodology required to conduct IT security evaluations

3.2
subjective method
method based on a given person's experience, and understanding

4 Knowledge

4.1 General

Knowledge is what an evaluator knows and can describe. Subclauses 4.2 to 4.8 address the knowledge that is needed for evaluation to ISO/IEC 15408 (all parts) and ISO/IEC 18045.

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

4.2.1 ISO/IEC 15408-1

All evaluators shall have knowledge of:

a) the terms and definitions defined in ISO/IEC 15408-1;

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

c) the context for ISO/IEC 15408 evaluations;

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

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

f) protection profiles and packages;

g) evaluation results; and

h) the specification of security targets.

4.2.2 ISO/IEC 15408-2

All evaluators shall have knowledge of those security functional requirements (SFRs) of ISO/IEC 15408-2 which are used for the technology types the evaluator is authorized to work with, as well as any dependent SFRs. The classes of SFRs given in ISO/IEC 15408-2 are:

a) security audit (FAU);

b) communication (FCO);

c) cryptographic support (FCS);

d) user data protection (FDP);

e) identification and authentication (FIA);

f) security management (FMT);

g) privacy (FPR);

h) protection of the target of evaluation security functions (FPT);

i) resource utilisation (FRU);

j) target of evaluation access (FTA); and

k) trusted path/channels (FTP).

4.2.3 ISO/IEC 15408-3

All evaluators shall have knowledge of the security assurance requirements (SARs) given in ISO/IEC 15408-3 which are specified by Security Targets (ST) that the evaluator is authorized to work with.

The knowledge of particular SAR components shall include those to which the evaluator is authorized to work at. The classes of SARs given in ISO/IEC 15408-3 are:

a) development (ADV);

b) guidance documentation (AGD);

c) life-cycle support (ALC);

d) security target structure (ASE);

e) protection profile structure (APE);

f) tests (ATE);

g) vulnerability assessment (AVA); and

h) composition (ACO).

4.2.4 ISO/IEC 18045

All evaluators shall have knowledge of:

a) the evaluation process: this process is described in ISO/IEC 18045:2008, Clause 8; and

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

4.3 Knowledge of the assurance paradigm

4.3.1 Knowledge of the evaluation authority

All evaluators shall have knowledge of the requirements of the evaluation authority or evaluation authorities that are applicable to the evaluation schemes for which they are authorized to work.

NOTE Examples of such evaluation authorities include "Common Criteria Recognition Agreement (CCRA)" and the "Senior Officials Group Information Systems Security (SOG-IS)".

Requirements from evaluation authorities can include topics such as:

a) the scope of the evaluation authority;

b) recognition arrangements;

c) evaluation authority policies;

d) guidance to evaluation schemes, validators and evaluators;

e) interpretations;

f) supporting documents;

g) knowledge of related standards; and

h) quality requirements.

4.3.2 Knowledge of the evaluation scheme

Evaluation schemes typically define operational aspects such as policies, and procedures that are specific to the evaluation scheme. Such items are often based on the scope of the evaluation scheme.

All evaluators shall have knowledge of:

a) The requirements of the evaluation scheme or schemes for which they are authorized to work;

EXAMPLE

— any sector specific policies, regulations and legislation;

— laboratory approval requirements for the evaluation scheme;

— evaluation scheme policies in regard to evaluation projects including entry criteria, time limits, report requirements, site visit requirements;

— guidance to validators and evaluators;

— evaluation scheme specific interpretations;

— evaluation scheme specific guidance;

— approved protection profiles and their supporting documents;

— evaluation scheme specific assurance methods and activities; and

— reporting requirements.

b) the competence requirements of the evaluation scheme for evaluators.

NOTE See ISO/IEC 18045:2008, A.5 for guidance to evaluation schemes on this topic.

4.3.3 Knowledge of the laboratory and it's management system

All evaluators 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 evaluators. Most laboratory management systems are based on ISO/IEC 17025.

4.4 Knowledge of information security

All evaluators shall have knowledge of:

a) security principles;

b) security properties;

c) mechanisms of attack;

d) concepts of attack potential;

e) secure development life cycles;

f) security testing; and

g) vulnerabilities and weaknesses.

4.5 Knowledge of the technology being evaluated

4.5.1 Knowledge of the technology being evaluated

ISO/IEC 15408 (all parts) 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 evaluation schemes, evaluation authorities or others.

All evaluators shall have knowledge of the information technology types being evaluated by them, 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.

4.5.2 Protection Profiles, packages and supporting documents

All evaluators shall have knowledge of the following, where they are applicable for the information technology evaluated by them:

a) protection profiles, packages and any related supporting documents specified in connection with the evaluator's work;

b) the knowledge required to meet any additional evaluation methods and assurance activities specified as applicable to an evaluation;

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.

4.6 Knowledge required for specific assurance classes

Evaluators need the knowledge required by the evaluation methods and activities specified for the assurance classes for which they are authorized to work. Examples for the knowledge required by ISO/IEC 18045 are given in Annex B.