SLOVENSKI STANDARD
oSIST prEN ISO/IEC 19896-2:2022

01-november-2022

IT varnostne tehnike - Zahteve za usposobljenost za preskuševalce in ocenjevalce informacijske varnosti - 2. del: Zahteve glede znanja, veščin in učinkovitosti za preskuševalce ISO/IEC 19790 (ISO/IEC 19896-2:2018)

IT security techniques - Competence requirements for information security testers and evaluators - Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers (ISO/IEC 19896-2:2018)

IT-Sicherheitstechniken - Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit - Teil 2: Anforderungen an Wissen, Fähigkeiten und Effektivität für ISO/IEC 19790 Tester (ISO/IEC 19896 2:2018)

Techniques de sécurité IT - Exigences de compétence pour l'information testeurs d'assurance et les évaluateurs - Partie 2: Exigences en matière de connaissances, de compétences et d'efficacité pour ISO/IEC 19790 testeurs (ISO/IEC 19896-2:2018)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 19896-2**

ICS:

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

oSIST prEN ISO/IEC 19896-2:2022 **en,fr,de**

INTERNATIONAL STANDARD

ISO/IEC 19896-2

First edition
2018-08

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

Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

Techniques de sécurité IT — Exigences de compétence pour l'information testeurs d'assurance et les évaluateurs —

Partie 2: Exigences en matière de connaissances, de compétences et d'efficacité pour ISO / IEC 19790 testeurs

Reference number
ISO/IEC 19896-2:2018(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*.

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.

A list of all parts in the ISO/IEC 19896 series can be found on the ISO website.

Introduction

This document provides the specialized requirements to demonstrate knowledge, skills and effectiveness requirements of individuals in performing security testing projects in accordance with ISO/IEC 19790 and ISO/IEC 24759. ISO/IEC 19790 provides the specification of security requirements for cryptographic modules. Many certification, validation schemes and recognition arrangements have been developed using it as a basis. ISO/IEC 19790 permits comparability between the results of independent security testing projects. ISO/IEC 24759 supports this by providing a common set of testing requirements for testing a cryptographic module for conformance with ISO/IEC 19790.

One important factor in assuring comparability of the results of such validations or certifications is the knowledge, skills and effectiveness requirements of the individual testers responsible for performing testing projects.

ISO/IEC 17025, which is often specified as a standard to which testing facilities conform, states in 5.2.1 that “Personnel performing specific tasks shall be qualified on the basis of appropriate education, training, experience and/or demonstrated skills”.

The audience for this document includes validation and certification authorities, laboratory testing accreditation bodies, testing projects schemes, testing facilities, testers and organizations offering professional credentials and recognitions.

This document establishes a baseline for the knowledge, skills and effectiveness requirements of ISO/IEC 19790 testers with the goal of establishing conformity in the requirements for the training of ISO/IEC 19790 testing professionals associated with cryptographic module conformance testing programs.

Annex D illustrates the usefulness of this document by validators within a validation program.

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

Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

1 Scope

This document provides the minimum requirements for the knowledge, skills and effectiveness requirements of individuals performing testing activities for a conformance scheme using ISO/IEC 19790 and ISO/IEC 24759.

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

ISO/IEC 17825, *Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*

ISO/IEC 18367, *Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 19896-1, *IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*

ISO/IEC 20085-1, *Information technology — Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques*

ISO/IEC 20085-2, *Information technology — Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part: 2 Test calibration methods and apparatus*

ISO/IEC 20543, *Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*

ISO/IEC 24759, *Information technology — Security techniques — Test requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19896-1 and ISO/IEC 19790 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/

4 Abbreviated terms

AES advanced encryption standard

HDD hard disk drive

RSA rivest-shamir-adleman

SHA secure hash algorithm

SSD solid state drive

5 Structure of this document

This document is divided into the following clauses: Knowledge (Clause 5), Skills (Clause 6), Experience (Clause 7), Education (Clause 8) and Effectiveness (Clause 9). Each clause corresponds to an aspect of the knowledge, skills, experience, education and effectiveness requirements of individuals performing testing activities as introduced in ISO/IEC 19896-1 for a conformance scheme using ISO/IEC 19790 and ISO/IEC 24759.

6 Knowledge

6.1 General

Knowledge is what a tester knows and can describe. Clauses 6 to 9 address education requirements and knowledge areas that are specifically needed for conformance testing to ISO/IEC 19790 and ISO/IEC 24759.

6.2 Tertiary education

6.2.1 General

Testers shall have educational qualifications such as an associate, bachelor, or higher degree that is relevant to the security requirements addressed in ISO/IEC 19790 and the test requirements in ISO/IEC 24759. The testers shall at a minimum demonstrate they have either:

a) successfully completed appropriate tertiary education with at least 3 years of study in disciplines related to IT or IT security; or

b) experience equivalent to the tertiary education in disciplines related to IT, IT security or IT system administration.

6.2.2 Technical specialities

In addition to the minimum level of educational requirements in 6.2.1, testers shall have educational qualifications such as an associate, bachelor, or higher degree that addresses the specific technical specialities. Examples of specific technical specialities include:

— cryptographic concepts;

— engineering technology;

— electrical engineering;

— mechanical engineering;

— material engineering;

— chemical engineering;

— computer information technology;

— computer engineering;

— computer science;

— computer networks;

— cybersecurity;

— information systems;

— laboratory management;

— software development and security; or

— software engineering.

6.2.3 Speciality topics

ISO/IEC 19790:2012 and the test requirements in ISO/IEC 24759 address the following specific speciality knowledge topics. A tester shall, at a minimum, demonstrate knowledge in at least one specific speciality topic.

A testing laboratory shall have knowledge in all the speciality areas as an aggregate of its technical staff.

ISO/IEC 19790:2012 and ISO/IEC 24759 specify speciality topics:

a) software and firmware development:

   1) programming languages (e.g. assembler and high-level);

   2) compilers;

   3) debugging tools;

   4) product testing performed by vendor:

      i) unit testing;

      ii) integration testing;

      iii) regression testing;

b) operating systems:

   1) installation;

   2) configuration;

   3) operation;

   4) architecture;

   5) system hardening;

   6) virtual machines;

7) java runtime environment;

c) hardware development:

1) hardware embodiments:

i) single-chip;

ii) multi-chip embedded;

iii) multi-chip standalone;

2) technology:

i) single-chip fabrication;

ii) electrical components and design, schematics and concepts including logic design and HDL representations;

iii) mechanical design and packaging;

3) manufacturing:

i) supply chain integrity;

ii) fabrication methods;

iii) initialization of parameters;

iv) packing and shipping;

v) testing and characterization;

4) hardware security features;

d) operational environments:

1) boot loader;

2) loading;

3) linking;

4) memory management and protection;

5) inter-process communication;

6) discretionary access control;

7) role-based access control;

8) executable forms;

9) audit mechanisms;

e) cryptographic algorithms, mechanisms and techniques:

1) cryptographic algorithms and security functions:

i) symmetric key;

ii) asymmetric key;

iii) hashing;

iv) random bit generators;

v) message authentication;

vi) entropy;

vii) modes of operation;

2) sensitive security parameter management:

i) sensitive security parameter generation;

ii) sensitive security parameter establishment;

I) automated SSP transport or SSP agreement;

II) manual SSP entry or output via direct or electronic;

iii) sensitive security parameter entry and output;

iv) sensitive security parameter storage;

v) sensitive security parameter zeroization;

f) identification and authentication mechanisms:

1) identity-based authentication;

2) role-based authentication;

3) multi-factor–based authentication;

g) best practices in design and development:

1) design assurance such as configuration management, delivery, operation and development;

2) design by contract;

h) informal modelling;

1) finite state model;

i) non-invasive security;

1) non-invasive attacks:

i) DPA/DEMA;

ii) SPA/SEMA;

iii) timing attacks;

2) countermeasures:

i) physical countermeasures;

EXAMPLE 1 Precharge logic, dual-rail logic, current flattening, probe detection, adding noise, random interrupts, jittered clock.

ii) Logical countermeasures;

EXAMPLE 2 Masking, hiding, dummy operation, balanced timing, shuffling, automatic re-keying.

j) self-test mechanisms:

1) pre-operational tests;