

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)

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 19896-2:2023 sisaldab Euroopa standardi EN ISO/IEC 19896-2:2023 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 19896-2:2023 consists of the English text of the European standard EN ISO/IEC 19896-2:2023.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 25.01.2023.	Date of Availability of the European standard is 25.01.2023.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile [standardiosakond@evs.ee](mailto:standardiosakond@evs.ee).

ICS 35.030

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis-ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardimis-ja Akrediteerimiskeskusega: Koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation and Accreditation:

Homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

English version

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)

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)

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)

This European Standard was approved by CEN on 9 January 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



**CEN-CENELEC Management Centre:  
Rue de la Science 23, B-1040 Brussels**

## European foreword

The text of ISO/IEC 19896-2:2018 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 19896-2:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2023, and conflicting national standards shall be withdrawn at the latest by July 2023.

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

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

## Endorsement notice

The text of ISO/IEC 19896-2:2018 has been approved by CEN-CENELEC as EN ISO/IEC 19896-2:2023 without any modification.

# Contents

	Page
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Abbreviated terms</b> .....	<b>2</b>
<b>5 Structure of this document</b> .....	<b>2</b>
<b>6 Knowledge</b> .....	<b>2</b>
6.1 General.....	2
6.2 Tertiary education.....	2
6.2.1 General.....	2
6.2.2 Technical specialities.....	2
6.2.3 Speciality topics.....	3
6.3 Knowledge of standards.....	7
6.3.1 General.....	7
6.3.2 ISO/IEC 19790 concepts.....	7
6.3.3 ISO/IEC 24759.....	7
6.3.4 Additional ISO/IEC standards.....	8
6.4 Knowledge of the validation program.....	8
6.4.1 Validation program.....	8
6.5 Knowledge of the requirements of ISO/IEC 17025.....	10
<b>7 Skills</b> .....	<b>10</b>
7.1 General.....	10
7.2 Algorithm testing.....	10
7.3 Physical security testing.....	10
7.4 Side channel analysis.....	10
7.5 Technology types.....	10
<b>8 Experience</b> .....	<b>10</b>
8.1 General.....	10
8.2 Demonstration of technical competence to the validation program.....	11
8.2.1 Experience with performing testing.....	11
8.2.2 Experience with particular technology types.....	11
<b>9 Education</b> .....	<b>11</b>
<b>10 Effectiveness</b> .....	<b>11</b>
<b>Annex A (informative) Example of an ISO/IEC 24759 testers' log</b> .....	<b>12</b>
<b>Annex B (informative) Ontology of technology types and associated bodies of knowledge</b> .....	<b>13</b>
<b>Annex C (informative) Specific knowledge associated with the security of cryptographic modules</b> .....	<b>16</b>
<b>Annex D (informative) Competence requirements for ISO/IEC 19790 validators</b> .....	<b>33</b>
<b>Bibliography</b> .....	<b>34</b>

## 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](http://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](http://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](http://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](http://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.