International Standard

ISO/IEC 19896-2

Second edition
2026-01

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

Part 2: Knowledge and skills requirements for testers and validators according to ISO/IEC 19790 and ISO/IEC 24759

Sécurité de l'information, cybersécurité et sécurité de la vie privée — Exigences relatives aux compétences du personnel des organismes d'évaluation de la conformité de la sécurité TI —

Partie 2: Exigences en matière de connaissances et de compétences pour les testeurs et les validateurs conformément à la série ISO/IEC 19790 et à l'ISO/IEC 24759

Reference number
ISO/IEC 19896-2:2026(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

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/IEC 19896-2:2018), which has been technically revised.

The main changes are as follows:

- the document has been restructured:
  - deleted subclauses related to experience, education and effectiveness;
- technical changes have been introduced:
  - deleted elements of competence, experience, education and effectiveness, except for knowledge and skill, according to comments from ISO/CASCO;
  - added competence requirements for the validators;
  - Annex C has been removed.

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

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 and www.iec.ch/national-committees.

Introduction

This document specifies the specialized knowledge and skills requirements for testers and validators, who perform security testing projects according to ISO/IEC 19790 and ISO/IEC 24759. ISO/IEC 19790 specifies security requirements for cryptographic modules. Many validation schemes and recognition arrangements have been developed using ISO/IEC 19790 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 of the important factors in assuring comparability of the results of such validations is the knowledge and skills requirements of the individual testers responsible for performing testing projects.

Another important factor in assuring comparability of the results of such validations is the knowledge and skills requirements of the individual validators responsible for validating the results of testing projects.

ISO/IEC TS 23532-2, which is often specified as a standard to which the testing laboratory conforms, states in ISO/IEC TS 23532-2:2021, 6.2 that the competence requirements for each function influencing the results of laboratory activities are documented, including requirements for education, qualification, training, technical knowledge, skills and experience. The document provides the requirement that the personnel have the competence to perform laboratory activities for which they are responsible and to evaluate the significance of deviations specified in ISO/IEC TS 23532-2:2021, 6.2.

The audience for this document includes validation authorities, testing laboratories, testers, validators and organizations offering professional credentials and recognitions.

This document establishes a baseline for the knowledge and skills requirements of:

- testers, to ensure harmonized requirements for cryptographic module conformance testing programmers, and
- validators, to ensure harmonized requirements for cryptographic module validation programmes.

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

Part 2:
Knowledge and skills requirements for testers and validators according to ISO/IEC 19790 and ISO/IEC 24759

1 Scope

This document provides the minimum requirements for the knowledge and skills of assessment body testers and validators performing testing activities and validating 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 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 19790:2025, *Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules*

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

ISO/IEC 20085-1, *IT 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, *IT 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 TS 23532-2:2021, *Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 2: Testing for ISO/IEC 19790*

ISO/IEC 24759:2025, *Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules*

Bibliography

[1] National Institute of Standards and Technology, Special Publication (SP) 132, *Recommendation for Password-Based Key Derivation,* December 2010

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

[3] ISO/IEC 17065, *Conformity assessment — Requirements for bodies certifying products, processes and services*