International Standard

ISO/IEC 19896-1

Second edition
2025-11

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

Part 1: Overview and concepts

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 1: Vue d'ensemble et concepts

Reference number
ISO/IEC 19896-1:2025(en)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Concepts ... **3**
5 Elements of competence ... **4**
5.1 Competences ... 4
5.2 Knowledge ... 4
5.3 Skills ... 5
5.3.1 General ... 5
5.3.2 Testers and evaluators ... 5
5.3.3 Validators and reviewers ... 6
6 Competency levels ... **6**
6.1 General ... 6
6.2 Testers and evaluators ... 7
6.2.1 Competency level 1 ... 7
6.2.2 Competency level 2 ... 7
6.2.3 Competency level 3 ... 7
6.3 Validators and reviewers ... 7
6.3.1 Competency level 1 ... 7
6.3.2 Competency level 2 ... 8
6.3.3 Competency Level 3 ... 8
7 Measurement of elements of competence ... **8**
7.1 Knowledge ... 8
7.2 Skills ... 8
7.3 Recording elements of competence ... 9
Annex A (informative) **Framework for describing competence requirements** ... **10**
Annex B (informative) **Example records of experience and competence** ... **11**
Bibliography ... **12**

© ISO/IEC 2025 – All rights reserved

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 19896-1:2018), which has been technically revised.

The main changes are as follows:

— the document has been restructured;

  — subclauses related to experience, education and effectiveness have been deleted;

— technical changes have been introduced;

  — competence concepts for the validators and the reviewers have been added;

— deleted elements of competence, experience, education and effectiveness except for knowledge and skills according to comments from ISO/CASCO.

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.

© ISO/IEC 2025 – All rights reserved

Introduction

The objective of the ISO/IEC 19896 series is to provide the fundamental concepts related to the topic of the competence of personnel responsible for performing information technology (IT) product security evaluations and conformance testing as well as those personnel performing review and validations. The ISO/IEC 19896 series provides the framework and the specialized requirements that specify the minimum competence of personnel performing IT product security evaluations and conformance testing, reviews and validation using International Standards. This document provides fundamental information to users of ISO/IEC 19896-2 and ISO/IEC 19896-3.

In pursuit of this objective, the ISO/IEC 19896 series comprises the following:

a) the terms and definitions relating to the topic of competence in IT product security testers and evaluators;

b) the fundamental concepts relating to competence in IT product security and conformance testing and evaluation;

c) the minimum competence requirements for IT product security testers and evaluator to conduct IT product testing/evaluation;

d) the terms and definitions relating to the topic of competence in IT product security validators and reviewers;

e) the fundamental concepts relating to competence in IT product security validation and reviews; and

f) the minimum competence requirements for IT product security validators and reviewers to conduct IT product validation/review.

The ISO/IEC 19896 series is of interest to:

g) information security conformance-testing and evaluation specialists;

h) information security review bodies for evaluation;

i) information security validation authorities for conformance-testing;

j) information security conformance-testing and evaluation laboratories;

k) vendors or technology providers whose IT products can be the subject to information security conformance-testing or evaluations; and

l) organizations offering professional credentials or recognitions.

The ISO/IEC 19896 series is organized into parts to address the competence of testing and evaluation personnel as follows.

This document provides an overview of the definitions, fundamental concepts and a general description of the framework used to communicate the competence concepts for certain specialized areas. This document aims to provide the fundamental knowledge necessary to use the framework presented in the other parts of the ISO/IEC 19896 series.

ISO/IEC 19896-2 describes the minimum set of competence requirements at each competency level for conformance testers and validators working with ISO/IEC 19790 and ISO/IEC 24759.

ISO/IEC 19896-3 describes the minimum set of competence requirements at each competency level for information security evaluators and reviewers working with the ISO/IEC 15408 series and ISO/IEC 18045.

© ISO/IEC 2025 – All rights reserved

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

Part 1: Overview and concepts

1 Scope

This document establishes an organized set of concepts and relationships to understand the competency requirements for information security conformance-testing and evaluation specialists, thereby establishing a basis for shared understanding of the concepts and principles central to the ISO/IEC 19896 series across its user communities.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology 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
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO/IEC 17024:2012, 3.6]

3.2
conformance-tester
tester
individual assigned to perform test activities in accordance with a given conformance testing standard and associated testing methodology

Note 1 to entry: An example of such a standard is ISO/IEC 19790 and the testing methodology specified in ISO/IEC 24759.

© ISO/IEC 2025 – All rights reserved

3.3
evaluation laboratory
testing laboratory
laboratory
organization with a management system providing evaluation or testing work in accordance with a defined set of policies and procedures and utilizing a defined methodology for testing or evaluating the security functionality of IT products

Note 1 to entry: These organizations are often given alternative names by various evaluation authorities. For example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF).

[SOURCE: ISO/IEC TS 23532-1:2021, 3.1, modified — testing laboratory and laboratory have been added as preferred terms; definition has been modified to cover testing; Note 2 to entry has been removed.]

3.4
evaluation method
set of one or more evaluation activities for application in a specific context

[SOURCE: ISO/IEC 15408-1:2022, 3.42]

3.5
evaluation methodology
structured framework or system that organizes and applies various *evaluation methods* (3.4)

3.6
evaluator
individual assigned to perform evaluations in accordance with a given evaluation standard and associated *evaluation methodology* (3.5)

Note 1 to entry: An example of evaluation standards is the ISO/IEC 15408 series. An example of an associated evaluation methodology is given in ISO/IEC 18045.

3.7
knowledge
facts, information, truths, principles or understanding acquired through experience or education

EXAMPLE The ability to describe the various parts of an information assurance standard.

[SOURCE: ISO/IEC TS 17027:2014, 2.56, modified — an example has been added.]

3.8
review body
entity that reviews the evaluation results provided by an evaluation laboratory for conformance to ISO/IEC 15408

Note 1 to entry: A review body is called an evaluation authority in ISO/IEC 15408 and ISO/IEC 18045.

3.9
review scheme
review system related to specified products, to which the same specified requirements, specific rules and procedures apply

3.10
reviewer
individual assigned to perform review of evaluations in accordance with a given evaluation standard and associated *evaluation methodology* (3.5) and make decisions based on this

Note 1 to entry: One example of such an individual could be a certifier who uses the evaluation results to perform a certification.

© ISO/IEC 2025 – All rights reserved

3.11
skill
ability to perform a task or activity with a specific intended outcome acquired through education, training, experience or other means

EXAMPLE The ability to identify and classify the risks associated with a project.

[SOURCE: ISO/IEC TS 17027:2014, 2.74, modified — an example has been added.]

3.12
validation authority
entity that validates the testing results provided by a *testing laboratory* (3.3) for conformance to ISO/IEC 19790

Note 1 to entry: A validation authority can modify, add or delete requirements in ISO/IEC 24759.

Note 2 to entry: A validation authority can issue validation certificates for approved security functions or other conformance tested results.

Note 3 to entry: A validation authority can specify the format of the security policy.

Note 4 to entry: A validation authority can use alternative security functions or standards in ISO/IEC 19790:2025, Annexes C to G.

3.13
validation scheme
validation system related to specified products, to which the same specified requirements, specific rules and procedures apply

3.14
validator
individual assigned to perform validation activities in accordance with a given conformance testing standard and associated testing methodology

Note 1 to entry: An example of such a conformance testing standard is ISO/IEC 19790 and the testing methodology is specified in ISO/IEC 24759.

4 Concepts

In order to support conformity in the evaluation or conformance-testing of IT security products, competence is one factor in ensuring conformity in the evaluation or conformance-testing of IT security products. Despite the provision of standardized conformance-testing or evaluation methods, a minimum competence in performing the necessary activities is required to support achieving conformity and repeatability of the results. This, in turn, supports the mutual recognition of IT product security assurance certifications and validations.

The ISO/IEC 23532 series address the requirements for the competence of IT security testing and evaluation laboratories, which are related to the competencies of testers and evaluators that are required to be met by a laboratory. These related requirements include ensuring the competence of all personnel who can influence the testing or evaluation laboratory's activities.

Examples of such requirements include the following:

— defining and documenting the competence requirements for each function involved in the testing or evaluation laboratory activities;

— ensuring laboratory personnel have the competence to execute the activities for which they are responsible and understand the significance of and response to deviations found with regard to the testing or evaluation laboratory activities;

— having a documented process for the ongoing monitoring of personnel involved in the testing or evaluation laboratory activities; and

© ISO/IEC 2025 – All rights reserved