International Standard

ISO/IEC 19896-3

Second edition
2025-11

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

Part 3: Knowledge and skills requirements for evaluators and reviewers according to the ISO/IEC 15408 series and ISO/IEC 18045

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 3: Exigences en matière de connaissances et de compétences pour les évaluateurs et les examinateurs conformément à la série ISO/IEC 15408 et à l'ISO/IEC 18045

Reference number
ISO/IEC 19896-3:2025(en)

COPYRIGHT PROTECTED DOCUMENT

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

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:

— completely reworked the requirements for evaluators, including restructuring of the content;

— added requirements for personnel reviewing IT security conformance assessment activities.

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 and www.iec.ch/national-committees.

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 information technology (IT) products and for assurance measures applied to these IT products during a security evaluation. Many review and evaluation schemes as well as review bodies 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.

The evaluation process usually relies on both pre-defined tests/methods for a type of TOE, and TOE-specific tests/methods that are defined for a given implementation of the TOE. Hence, the competence of the individual evaluators, who are expected not only to apply pre-defined tests/methods but to define and run TOE-specific tests/methods, is key to ensuring the comparability and repeatability of evaluation results which is the foundation for mutual recognition.

This document establishes a baseline for the minimum competence of ISO/IEC 15408 series evaluators and reviewers to ensure harmonized requirements for training ISO/IEC 15408 evaluators and reviewers. It provides specialized requirements for individuals performing IT product security evaluations and reviews to demonstrate their competence according to the ISO/IEC 15408 series and ISO/IEC 18045. ISO/IEC 15408-1 describes the general framework for competences including the various elements thereof: knowledge, skills, experience and education. This document covers knowledge and skills, especially in the following areas.

— Information security

  — Knowledge: information security principles, information security properties, information security threats and vulnerabilities.

  — Skills: understanding information security requirements, the context and the scope of evaluation.

— Information security evaluation

  — Knowledge: knowledge of the ISO/IEC 15408 series 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: understanding 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: creating and managing an information security test plan, designing information security tests, preparing and conducting information security tests.

The audience for this document includes testing laboratory accreditation bodies, organizations implementing evaluation schemes, laboratories, evaluators and organizations offering professional credentialing.

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

Part 3:
Knowledge and skills requirements for evaluators and reviewers according to the ISO/IEC 15408 series and ISO/IEC 18045

1 Scope

This document provides the specialized requirements for individuals to demonstrate competence in performing IT product security evaluations and reviews according to the ISO/IEC 15408 series and ISO/IEC 18045.

NOTE It is possible that evaluators and testers belong to bodies operating under ISO/IEC 17025 and reviewers belong to bodies operating under ISO/IEC 17065.

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, *Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel — Part 1: Introduction and concepts*

ISO/IEC 15408-1:—[1)], *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:—[2)], *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security— Part 2: Security functional components*

ISO/IEC 15408-3:—[3)], *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security— Part 3: Security assurance components*

ISO/IEC 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security— Part 5: Pre-defined packages of security requirements*

ISO/IEC 18045:—[4)], *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

1) Under preparation. Stage at the time of publication: ISO/IEC FDIS 15408-1:2025.

2) Under preparation. Stage at the time of publication: ISO/IEC DIS 15408-2:2025.

3) Under preparation. Stage at the time of publication: ISO/IEC DIS 15408-3:2025.

4) Under preparation. Stage at the time of publication: ISO/IEC FDIS 18045:2025.