INTERNATIONAL STANDARD

ISO/IEC 19896-3

First edition
2018-08

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

Part 3:
Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

Techniques de sécurité IT — Exigences en matière de compétences des spécialistes en tests et évaluations de la sécurité de l'information —

Partie 3: Exigences en matière de connaissances, compétences et efficacité des spécialistes en évaluations ISO/IEC 15408

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. 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*.

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.

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 IT products and for assurance measures applied to these IT products during a security evaluation. Many certification and evaluation schemes as well as evaluation authorities 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.

One important factor in assuring comparability of the results of such evaluations is to understand that the evaluation process includes the specification of both objective and subjective assurance measures. Hence, the competence of the individual evaluators is important when the comparability and repeatability of evaluation results are the foundation for mutual recognition.

ISO/IEC 17025, provides general requirements for the competence of testing and calibration laboratories. In ISO/IEC 17025:2017, 5.2.1, it is stated that "*Personnel performing specific tasks shall be qualified on the basis of appropriate education, training, experience and/or demonstrated skills*".

This document establishes a baseline for the minimum competence of ISO/IEC 15408 evaluators with the goal of establishing conformity in the requirements for the training of ISO/IEC 15408 evaluator professionals associated with IT product evaluation schemes and authorities. It provides the specialized requirements to demonstrate the competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045. ISO/IEC 15408-1 describes the general framework for competences including the various elements of competence; knowledge, skills, experience, education and effectiveness. This document includes knowledge and skills especially in the following areas.

— Information security

   Knowledge: Information security principles, information security properties, information security threats and vulnerabilities

   Skills: Understand information security requirements, understand the context

— Information security evaluation

   Knowledge: Knowledge of ISO/IEC 15408 (all parts) 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: Understand 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: Create and manage an information security test plan, design information security tests, prepare and conduct information security tests

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

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

Part 3:
Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

1 Scope

This document provides the specialized requirements to demonstrate competence of individuals in performing IT product security evaluations in accordance with ISO/IEC 15408 (all parts) and ISO/IEC 18045.

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, *IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

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