INTERNATIONAL STANDARD

ISO/IEC 19896-1

First edition
2018-02

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

Part 1:
Introduction, concepts and general requirements

Techniques de sécurité IT — Exigences de compétence pour l'information testeurs d'assurance et les évaluateurs —

Partie 1: Introduction, concepts et exigences générales

Reference number
ISO/IEC 19896-1:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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. 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 on 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 the following URL: 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.

Introduction

The objective of the ISO/IEC 19896 series is to provide the fundamental concepts related to the topic of the competence of the individuals responsible for performing IT product security evaluations and conformance testing. The ISO/IEC 19896 series provides the framework and the specialized requirements that specify the minimum competence of individuals performing IT product security evaluations and conformance testing using established standards.

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 evaluators and testers;

b) The fundamental concepts relating to competence in IT product security evaluations and conformance testing; and

c) The minimum competence requirements for IT product security evaluators and testers to conduct IT product testing/evaluation.

The ISO/IEC 19896 series is of interest to:

a) Information security evaluation and conformance-testing specialists;

b) Information security evaluation and conformance-testing approval authorities;

c) Information security evaluation and conformance-testing laboratories;

d) Vendors or technology providers whose IT products can be the subject of information security assurance evaluations or conformance-testing;

e) Organizations offering professional credentials or recognitions.

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

In this document, the introduction and concepts, provides an overview of the definitions, fundamental concepts and a general description of the framework used to communicate the competence requirements for certain specialized areas. This material is aimed at providing the fundamental knowledge necessary to use the framework presented in the other parts of the ISO/IEC 19896 series appropriately.

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

ISO/IEC 19896-3 describes the minimum set of competence requirements at each competency level for information security evaluators working with ISO/IEC 15408 (all parts) and associated standards.

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

Part 1:
Introduction, concepts and general requirements

1 Scope

This document defines terms and establishes an organized set of concepts and relationships to understand the competency requirements for information security assurance 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. It provides fundamental information to users of the ISO/IEC 19896 series.

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 17000, *Conformity assessment — Vocabulary and general principles*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17000, ISO/IEC 17025 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://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.

3.3
education
process of receiving or giving systematic instruction, especially at a school or university

3.4
effectiveness
ability to apply knowledge and skills in a productive manner, characterized by attributes of behaviour such as aptitude, initiative, enthusiasm, willingness, communication skills, team participation, and leadership

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

Note 1 to entry: An example of evaluation standards is ISO/IEC 15408 (all parts) with the associated evaluation methodology given in ISO/IEC 18045.

3.6
experience
involvement at a practical level with projects related to the field of competence

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

Note 1 to entry: An example of knowledge is the ability to describe the various parts of an information assurance standard.

[SOURCE: ISO/IEC TS 17027:2014, 2.56, modified — Note 1 to entry has been added.]

3.8
laboratory
organization with a management system providing evaluation and 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 approval authorities. For example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF).

3.9
skill
ability to perform a task or activity with a specific intended outcome acquired through education, training, experience or other means

Note 1 to entry: An example of a skill is the ability to identify and classify the risks associated with a project.

[SOURCE: ISO/IEC 17027:2014, 2.74, modified — Note 1 to entry has been added.]

4 Concepts

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

ISO/IEC 17025 addresses the general requirements for the competence of testing and calibration laboratories and is frequently specified as a basis for conformity amongst security assurance conformance-testing and evaluation laboratories.

ISO/IEC 17025 identifies several requirements relating to competency that need to be met by a laboratory. These include:

- ensuring the competence of all personnel that can influence the laboratory's activities;
- defining and documenting the competence requirements for each function involved in 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 laboratory activities;
- having a documented process for the ongoing monitoring of personnel involved in laboratory activities; and
- maintaining records of competence such as education, training, technical knowledge, skills, experience, authorizations and monitoring for all personnel involved in laboratory activities.

NOTE ISO/IEC 17025 is intended to cover a broad range of calibration and testing laboratories and is not only used in the field of IT product security assurance testing and evaluation.

5 Elements of competence

5.1 Competences

In order to competently provide consistent conformance-testing and evaluation results and to support the goal of conformity in the results provided by different individuals and laboratories, it is necessary for conformance-testers and evaluators to have gained the minimum necessary knowledge, skills, experience and qualifications relevant to the target IT product security assurance standard, and to be able to perform their duties with effectiveness.

This clause defines the minimum elements of competence that should be used by the ISO/IEC 19896 series when considering the requirements for competence in conformance-testers and/or evaluators for specific IT product security assurance standards.

Training may be provided in order to increase some elements of competence in individuals. For example, training is often performed in order to acquire or enhance existing skills, increase knowledge or for increasing effectiveness.

Additional elements of competence such as aptitude, enthusiasm, initiative, leadership, teamwork and willingness can be specified by laboratories or accreditation bodies. They can also be defined in other parts of the ISO/IEC 19896 series.

5.2 Knowledge

The possession of knowledge by testers and evaluators is one of the elements of competence. The following form the basis of providing an appropriate and testable body of knowledge relevant for that product security assurance standard:

a) knowledge of the relevant IT product security assurance standard;

b) any associated testing or evaluation methods;

c) policies and procedures of relevant approval authorities, accreditation bodies and laboratories; and

d) knowledge of IT product architecture and design in relevant technology areas.

When considering IT products, a variety of technologies can be pertinent to the scope of work of a laboratory, and knowledge of these technologies should be considered when defining minimum competency levels. For a particular technology area, the following are important relevant knowledge classes:

a) The technology used in the design, development and deployment of the products being tested;

b) The way in which the products are used or intended to be used;

c) The typical vulnerabilities and weaknesses which may occur in that technology; and

d) The domain in which the products are used or intended to be used.

Examples of technology areas include cryptography, biometrics, integrated circuits, operating systems, network devices, databases, smartcards and embedded systems. Technology areas are sometimes defined by the approval authority, amongst others.

5.3 Skills

Skills typically required of testers and evaluators of IT security products according to the competency levels defined in Clause 6 include:

a) understanding the scope and basis of an evaluation or a conformance-testing project;

b) understanding the boundaries of the implementation under test or the target of evaluation;

c) being able to select or adapt appropriate evaluation or testing method;

d) performing documentation analysis;

e) understanding the source code, schematics and base components used in specifying and implementing products;

f) developing and performing functional and non-functional testing;

g) determining if test conditions are within stated parameters to allow for repeatable testing;

h) calibrating and using testing tools;

i) using proper storage, including appropriate integrity, availability and confidentiality, of test evidence, test results, and test records, including interpretations and test reports;

j) interpreting the test results;

k) being able to write understandable reports detailing the results of their work;

l) being able to repeat a test, or replay an archived test, and obtain the same results; and

m) being able to build a testing environment to achieve a proper running condition for it security products.

At higher competence levels, skills such as the ability to communicate effectively and perform project management, can also be expected.

At competence levels 1 and 2 these skills may be performed under supervision.

5.4 Experience

Experienced individuals have performed evaluations or conformance-testing, and perhaps taught or mentored others over many conformance-testing or evaluation projects. Experienced individuals have a deep understanding of the requirements for conformance-testing or evaluation projects, as well as any interpretations and policies of the accreditation body, approval authorities and laboratories.

5.5 Education

The specification of particular educational qualifications such as an Associate, Bachelor's, or higher degree can help to determine an individual's ability to follow a formal program or work independently. Some higher education programs and concentrations related to evaluation and conformance-testing can offer an individual the chance to gain appropriate knowledge as an information security assurance professional.

In some cases, it may be acceptable to substitute appropriate and relevant experience in lieu of education or qualifications.

5.6 Effectiveness

Effectiveness as a tester or evaluator varies depending on the goals and structure of the laboratory as well as those of the approval authority. In particular, effectiveness should consider the accuracy of test results or evaluations obtained, the ability to repeat evaluation or test methods and activities performed by other competent testers and evaluators, and obtain the same results, and the ability to communicate testing and evaluation results in a manner that is easily understood by the intended audience.

6 Competency levels

6.1 General

Evaluators and testers may be assigned a competence level for each specific competence area given in the other parts of the ISO/IEC 19896 series. These are described in 6.2 to 6.5 by a level number and a typical descriptor.

Overall levels of competency may be used to support different designations of professional capability such as:

a) Technician;

b) Evaluator/Tester;

c) Senior Evaluator/Tester; and

d) Lead Evaluator/Tester.

6.2 Level 1 (Associate)

- Provides support for some activities required by the conformance-testing or evaluation methods; and
- Can perform testing or evaluation work under supervision.

6.3 Level 2 (Professional)

- Is competent to work unsupervised in many testing or evaluation areas but can require supervision in a few areas; and
- Is able to understand the significance of and response to deviations found with regard to the laboratory's activities.

6.4 Level 3 (Manager)

- Is competent to work unsupervised in most testing or evaluation areas;
- Is able to understand the significance of and response to deviations found with regard to the laboratory's activities; and

— Is able to supervise the testing or evaluation work of those at Levels 1 and 2.

6.5 Level 4 (Principal)

— Is competent in testing all aspects of the testing or evaluation according to the defined standards and methods for at least one technology area;

— Is competent in communicating with stakeholders including approval authorities and vendors and can provide project management for an evaluation or conformance-testing project;

— Is competent to work unsupervised in all testing/evaluation methods specified for the project;

— Is able to understand the significance of and response to deviations found with regard to the laboratory's activities; and

— Is able to supervise and provide mentorship in regard to the testing or evaluation work of those at Levels 1, 2, and 3.

7 Measurement of elements of competence

7.1 Knowledge

The knowledge areas defined in the ISO/IEC 19896 series provide, for each IT product security assurance standard, a body of knowledge that is measurable. Such tests of knowledge can include professional qualifications gained through third parties or through testing developed and performed by approval authorities or the laboratory itself.

7.2 Skills

Various skills are required for testers and evaluators of IT security products, which are presented in the subsequent parts of the ISO/IEC 19896 series. These skills should be measured.

Examples of methods for measurement of skills include:

— aspects of the laboratories proficiency-testing programme performed as part of the requirements for conformance to ISO/IEC 17025;

— the use of training records, maintained in accordance with ISO/IEC 17025, in the specification of measures of training effectiveness, which, in turn, can demonstrate the mastery of a skill;

— professional certifications in regard to particular skills;

— feedback from other personnel already deemed competent in a skill.

7.3 Experience

Experience should be measured through maintaining records of the number of projects completed, and their description, including the technical domain, in terms of project complexity, technologies and testing methods employed during the projects.

NOTE The number of years spent in relevant roles is not, by itself, an adequate measure since experience reflects the volume and variety of projects undertaken at least as much as their duration.

7.4 Education

An individual's education and qualifications are typically demonstrated by the possession of authentic certificates issued by organizations recognized as legitimate by the approval authority.

7.5 Effectiveness

Measurement criteria for the effectiveness of evaluators and testers should be established by a laboratory. Relevant criteria include:

- time needed to make a test or evaluation plan;
- time needed to execute a test or evaluation plan and complete it;
- number, type and severity of comments received during internal quality assurance activities;
- number, type and severity of comments received during the validation phase;
- being able to repeat tests from the test documentation produced by other competent testers or evaluators;
- being able to understand new tools and technologies;
- being able to explain failures and testing status to vendors, validators and other team members;
- accuracy of the evaluation or testing results;
- use of direct and focused language in test reports.

7.6 Recording elements of competence

ISO/IEC 17025 requires that records of competence are maintained by a laboratory. Annexes A and B provide example frameworks for recording this information.

Annex A
(informative)

Framework for describing competence requirements

Tables A.1 to A.4 describe a structure that can be used by laboratories to define specific competency requirements using the criteria of knowledge, skills, experience, and educations, for each competency level. The information in the tables is in addition to the minimum requirements defined in Clause 7.

ISO/IEC 19896-2 and ISO/IEC 19896-3 provide the specific competence criteria for ISO/IEC 19790 testers and ISO/IEC 15408 (all parts) evaluators that can be used in completing the tables.

Table A.1 — Competence requirements record for Level 1

Level 1 (Associate)	
Knowledge area name	**Knowledge area description**
Skill name	**Skill description**
Experience required	
Education required	
Effectiveness criteria	

Table A.2 — Competence requirements record for Level 2

Level 2 (Professional)	
Knowledge area name	**Knowledge area description**
Skill name	**Skill description**
Experience required	
Education required	
Effectiveness criteria	