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

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. 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

