IT security techniques - Competence requirements for information security testers and evaluators - Part 1: Introduction, concepts and general requirements (ISO/IEC 19896-1:2018)

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 19896-1:2023 sisaldab Euroopa standardi EN ISO/IEC 19896-1:2023 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 19896-1:2023 consists of the English text of the European standard EN ISO/IEC 19896-1:2023.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 25.01.2023.	Date of Availability of the European standard is 25.01.2023.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 19896-1

January 2023

ICS 35.030

English version

IT security techniques - Competence requirements for information security testers and evaluators - Part 1: Introduction, concepts and general requirements (ISO/IEC 19896-1:2018)

Techniques de sécurité IT - Exigences de compétence pour l'information testeurs d'assurance et les évaluateurs - Partie 1: Introduction, concepts et exigences générales (ISO/IEC 19896-1:2018)

IT-Sicherheitstechniken - Kompetenzanforderungen an Tester und Evaluatoren von Informationssicherheit - Teil 1: Einführung, Konzepte und allgemeine Anforderungen (ISO/IEC 19896-1:2018)

This European Standard was approved by CEN on 9 January 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

European foreword

The text of ISO/IEC 19896-1:2018 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 19896-1:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2023, and conflicting national standards shall be withdrawn at the latest by July 2023.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 19896-1:2018 has been approved by CEN-CENELEC as EN ISO/IEC 19896-1:2023 without any modification.

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