

STN	IT bezpečnostné techniky Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti Časť 1: Úvod, koncepty a všeobecné požiadavky	STN ISO/IEC 19896-1 97 4138
------------	---	---

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

IT-Sicherheitsverfahren
Kompetenzanforderungen für Informationssicherheits-Tester und -Gutachter
Teil 1: Einführung, Konzept und allgemeine Anforderungen

Táto norma obsahuje anglickú verziu ISO/IEC 19896-1: 2018.

This standard includes the English version of ISO/IEC 19896-1: 2018.

133064

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2021
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii.

Anotácia

Tento dokument definuje termíny a ustanovuje súbor konceptov a vzťahov na pochopenie kompetenčných požiadaviek na odborníkov na testovanie a hodnotenie zhody v oblasti zabezpečenia informačnej bezpečnosti, čím vytvára základňu pre spoločné porozumenie konceptov a princípov ústredných pre súbor ISO/IEC 19896. Poskytuje základné informácie používateľom súboru ISO/IEC 19896.

Národný predhovor

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN možno získať na webovej stránke www.unms.sk.

ISO/IEC 17000 zavedená v STN EN ISO/IEC 17000 Posudzovanie zhody. Slovník a všeobecné zásady (ISO/IEC 17022) (01 5202)

ISO/IEC 17025 zavedená v STN EN ISO/IEC 17025 Všeobecné požiadavky na kompetentnosť skúšobných a kalibračných laboratórií (ISO/IEC 17025) (01 5253)

Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Concepts	2
5 Elements of competence	3
5.1 Competences.....	3
5.2 Knowledge.....	3
5.3 Skills.....	4
5.4 Experience.....	4
5.5 Education.....	5
5.6 Effectiveness.....	5
6 Competency levels	5
6.1 General.....	5
6.2 Level 1 (Associate).....	5
6.3 Level 2 (Professional).....	5
6.4 Level 3 (Manager).....	5
6.5 Level 4 (Principal).....	6
7 Measurement of elements of competence	6
7.1 Knowledge.....	6
7.2 Skills.....	6
7.3 Experience.....	6
7.4 Education.....	6
7.5 Effectiveness.....	7
7.6 Recording elements of competence.....	7
Annex A (informative) Framework for describing competence requirements	8
Annex B (informative) Example records of experience and competence	10
Bibliography	11

ISO/IEC 19896-1:2018(E)

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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN