ICS 35.030 PREDBEŽNÁ SLOVENSKÁ TECHNICKÁ NORMA December 2023

STN P	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Požiadavky na spôsobilosť laboratórií pri testovaní a hodnotení bezpečnosti IT Časť 1: Hodnotenie pre ISO/IEC 15408**	**STN P ISO/IEC TS 23532-1** 97 4164

Information security, cybersecurity and privacy protection
Requirements for the competence of IT security testing and evaluation laboratories
Part 1: Evaluation for ISO/IEC 15408

Sécurité de l'information, cybersécurité et protection de la vie privée
Exigences relatives aux compétences des laboratoires d'essais et d'évaluation de la sécurité TI
Partie 1: Évaluation pour l'ISO/IEC 15408

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre
Anforderungen an die Kompetenz von IT-Sicherheitstest- und Bewertungslaboren
Teil 1: Bewertung für ISO/IEC 15408

Táto predbežná slovenská technická norma obsahuje anglickú verziu medzinárodnej normy ISO/IEC TS 23532-1: 2021 a má postavenie oficiálnej verzie.

This prestandard includes the English version of the International standard ISO/IEC TS 23532-1: 2021 and has the status of the official version.

137560

Anotácia

Laboratóriá vykonávajúce hodnotenie zhody s normami informačnej bezpečnosti vrátane série ISO/IEC 15408 môžu využívať a vyžadovať zhodu s normou ISO/IEC 17025: 2017.

Tento dokument dopĺňa a doplňuje postupy a všeobecné požiadavky uvedené v norme ISO/IEC 17025: 2017 pre laboratóriá vykonávajúce hodnotenia na základe noriem radu ISO/IEC 15408 a ISO/IEC 18045.

V norme ISO/IEC 17025: 2017 sa uvádzajú všeobecné požiadavky pre širokú škálu skúšobných a kalibračných laboratórií, aby mohli preukázať, že pracujú kompetentne a sú schopné poskytovať platné výsledky.

Laboratóriá, ktoré vykonávajú takéto hodnotenia, majú špecifické požiadavky na spôsobilosť podľa radu ISO/IEC 15408, ktoré im umožnia generovať platné výsledky.

Poskytnutím ďalších podrobností a doplnkových požiadaviek k norme ISO/IEC 17025: 2017, ktoré sú špecifické pre laboratóriá na hodnotenie bezpečnosti informácií, tento dokument uľahčí spoluprácu a lepšiu zhodu a harmonizáciu medzi laboratóriami a inými orgánmi. Tento dokument môžu používať krajiny a akreditačné orgány ako súbor požiadaviek na hodnotenie a akreditáciu laboratórií.

Na uľahčenie implementácie je tento dokument očíslovaný rovnako ako norma ISO/IEC 17025: 2017. Doplnkové požiadavky sú uvedené ako podkapitoly doplňujúce normu ISO/IEC 17025: 2017.

Národný predhovor

Obrázky v tejto norme sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2021 ISO/IEC, ref. č. ISO/IEC TS 23532-1: 2021 E.

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek 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 a TNI možno získať na webovom sídle www.unms.sk.

ISO/IEC 15408-1 prijatá ako STN EN ISO/IEC 15408-1 Informačné technológie. Bezpečnostné metódy. Kritériá na hodnotenie bezpečnosti IT. Časť 1: Predstavenie a všeobecný model (ISO/IEC 15408-1) (36 9776)

ISO/IEC 17000 prijatá ako STN EN ISO/IEC 17000 Posudzovanie zhody. Slovník a všeobecné zásady (ISO/IEC 17000) (01 5202)

ISO/IEC 17025: 2017 prijatá ako STN EN ISO/IEC 17025: 2018 Všeobecné požiadavky na kompetentnosť skúšobných a kalibračných laboratórií (ISO/IEC 17025: 2017) (01 5253)

ISO/IEC 19896-1 prijatá ako STN EN ISO/IEC 19896-1 IT bezpečnostné metódy. Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti. Časť 1: Úvod, koncepty a všeobecné požiadavky (ISO/IEC 19896-1) (97 4138)

ISO/IEC 19896-3 prijatá ako STN EN ISO/IEC 19896-3 IT bezpečnostné metódy. Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti. Časť 3: Požiadavky na znalosti, zručnosti a efektívnosť pre hodnotiteľov ISO/IEC 15408 (ISO/IEC 19896-3) (97 4138)

Vypracovanie slovenskej technickej normy

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

Technická komisia: TK 37 Informačné technológie

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 23532 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

Laboratories performing evaluations for conformance to information security standards including the ISO/IEC 15408 series may utilize and require conformance to ISO/IEC 17025:2017. ISO/IEC 17025:2017 gives generalized requirements for a broad range of testing and calibration laboratories to enable them to demonstrate that they operate competently and are able to generate valid results.

Laboratories that perform such evaluations have specific requirements for competence to the ISO/IEC 15408 series that will enable them to generate valid results.

By providing additional details and supplementary requirements to ISO/IEC 17025:2017 that are specific to information security evaluation laboratories, this document will facilitate cooperation and better conformity and harmonization between laboratories and other bodies. This document may be used by countries and accreditation bodies as a set of requirements for laboratory assessments and accreditations.

To help implementers, this document is numbered identically to ISO/IEC 17025:2017. Supplementary requirements are presented as subclauses additional to ISO/IEC 17025:2017.

TECHNICAL SPECIFICATION **ISO/IEC TS 23532-1:2021(E)**

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories —

Part 1: Evaluation for ISO/IEC 15408

1 Scope

This document complements and supplements the procedures and general requirements found in ISO/IEC 17025:2017 for laboratories performing evaluations based on the ISO/IEC 15408 series 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 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 17000, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17025:2017, *General requirements for the competence of testing and calibration laboratories*

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

ISO/IEC 19896-3, *IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators*