TECHNICAL SPECIFICATION

ISO/IEC TS 23532-1

First edition
2021-11

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

Reference number
ISO/IEC TS 23532-1:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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.

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.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17000, ISO/IEC 17025:2017, ISO/IEC 15408-1, ISO/IEC 19896-1, ISO/IEC 19896-3 and the following apply.

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

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
evaluation laboratory
organization with a management system providing evaluation in accordance with a defined set of policies and procedures and utilizing a defined methodology for evaluating the security functionality of IT products

Note 1 to entry: These organizations are often given alternative names by various evaluation authorities. For example, IT Security Evaluation Facility (ITSEF), Commercial Evaluation Facility (CLEF).

Note 2 to entry: The defined methodology is given ISO/IEC 18045.

4 General requirements

4.1 Impartiality

4.1.1 ISO/IEC 17025:2017, 4.1.1 applies.

4.1.1.1 ISO/IEC 17025:2017, 4.1.1 applies with the following additions.

The evaluation laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of information technology security evaluations. When conducting evaluations, the laboratory policies and procedures shall ensure that:

a) evaluators cannot both develop and evaluate the same protection profile, security target, or IT product, and

b) evaluators cannot both provide consulting services for and participate in the evaluation or testing of the same protection profile, security target, or IT product.

4.1.2 ISO/IEC 17025:2017, 4.1.2 applies.

4.1.2.1 ISO/IEC 17025:2017, 4.1.2 applies with the following additions.

The organization to which the evaluator belongs shall not be the same as the organization to which the department that develops the target of evaluation (TOE) belongs.

4.1.3 ISO/IEC 17025:2017, 4.1.3 applies.

4.1.4 ISO/IEC 17025:2017, 4.1.4 applies.

4.1.5 ISO/IEC 17025:2017, 4.1.5 applies.

4.1.6 ISO/IEC 17025:2017, 4.1 applies with the following additions.

To maintain impartiality, the laboratory shall maintain proper separation between evaluators and other personnel inside the laboratory or outside the laboratory, but inside the parent organization.

4.2 Confidentiality

4.2.1 ISO/IEC 17025:2017, 4.2.1 applies.

4.2.2 ISO/IEC 17025:2017, 4.2.2 applies.

4.2.3 ISO/IEC 17025:2017, 4.2.3 applies.

4.2.4 ISO/IEC 17025:2017, 4.2.4 applies.

4.2.5 ISO/IEC 17025:2017, 4.2 applies with the following additions.

Confidentiality mechanisms shall be employed to ensure that the evaluation report cannot be disclosed to anyone other than the intended recipient(s).

4.2.6 ISO/IEC 17025:2017, 4.2 applies with the following additions.

Because of confidentiality requirements of the evaluation laboratory and client, some evaluation output may need to exclude:

a) proprietary information (e.g. source code);

b) TOE-specific sampling and test information;

c) effort estimates;

d) commercially sensitive information.

4.2.7 ISO/IEC 17025:2017, 4.2 applies with the following additions.

The evaluation laboratory shall have physical and electronic controls augmented with an explicit policy and a set of procedures for maintaining separation, both physical and electronic, between the laboratory, evaluators and laboratory consultants, product developers, system integrators, and others who may have an interest in and/or may unduly influence the evaluation outcome.

4.2.8 ISO/IEC 17025:2017, 4.2 applies with the following additions.

The management system shall include policies and procedures to ensure the protection of proprietary information. This protection shall specify how proprietary information will be protected from persons outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons. The evaluation laboratory shall possess its own security manual that sets out the procedures and responsibilities to be undertaken by all the evaluators of the evaluation laboratory, to maintain the security required to protect commercially sensitive information.

5 Structural requirements

5.1 ISO/IEC 17025:2017, 5.1 applies.

5.2 ISO/IEC 17025:2017, 5.2 applies.

5.3 ISO/IEC 17025:2017, 5.3 applies.

5.3.1 ISO/IEC 17025:2017, 5.3 applies with the following additions.

The evaluation laboratory shall create and maintain a cross-referenced document mapping Clauses 4 to 8 to the laboratory's management system documentation.

5.4 ISO/IEC 17025:2017, 5.4 applies.

5.5 ISO/IEC 17025:2017, 5.5 applies.

5.6 ISO/IEC 17025:2017, 5.6 applies.

5.7 ISO/IEC 17025:2017, 5.7 applies.

5.8 ISO/IEC 17025:2017, Clause 5 applies with the following additions.

There shall be a nominated person within the evaluation laboratory with overall responsibility for the security of the evaluation laboratory and the production of the evaluation laboratory security manual.

6 Resource requirements

6.1 General

ISO/IEC 17025:2017, 6.1 applies.

6.2 Personnel

6.2.1 ISO/IEC 17025:2017, 6.2.1 applies.

6.2.2 ISO/IEC 17025:2017, 6.2.2 applies.

NOTE Laboratories document the required qualifications for each staff position. The staff information can be kept in the official personnel folders.

6.2.2.1 ISO/IEC 17025:2017, 6.2.2 applies with the following additions.

The evaluation laboratory shall maintain a list of personnel designated to fulfil laboratory requirements including:

a) laboratory director,

b) approved report signatories,

c) evaluation team leaders, and

d) evaluators.

An individual may be assigned or appointed to serve in more than one position; however, to the extent possible, the laboratory director position should be independently staffed.

NOTE Significant change in a laboratory's key technical personnel or facilities can result in a laboratory no longer being deemed proficient by relevant scheme owner(s).

6.2.3 ISO/IEC 17025:2017, 6.2.3 applies.

6.2.4 ISO/IEC 17025:2017, 6.2.4 applies.

6.2.5 ISO/IEC 17025:2017, 6.2.5 applies.

6.2.5.1 ISO/IEC 17025:2017, 6.2.5 applies with the following additions.

The evaluation laboratory shall have procedure(s) and retain records for determining the competence requirements for personnel in ISO/IEC 19896-3.

6.2.5.2 ISO/IEC 17025:2017, 6.2.5 applies with the following additions.

The evaluation laboratory has documented a detailed description of its training program for new and current evaluators. Each new evaluator is trained for assigned duties. The training program is updated and current evaluators shall be retrained when the ISO/IEC 15408 series or ISO/IEC 18045 changes, as new technology specific assurance activities are defined in protection profiles, or when the individuals are assigned new responsibilities. Each evaluator may receive training for assigned duties either through on-the-job training, formal classroom study, attendance at conferences, or another appropriate mechanism. Training materials that are maintained within the laboratory shall be kept up-to-date.

6.2.5.3 ISO/IEC 17025:2017, 6.2.5 applies with the following additions.

The laboratory shall have a procedure(s) and retain records for monitoring of competence of personnel according to ISO/IEC 19896-3.

6.2.5.4 ISO/IEC 17025:2017, 6.2.5 applies with the following additions.

The laboratory reviews annually the competence of each evaluator for each test method the evaluator is authorized to conduct. The evaluator's immediate supervisor, or a designee appointed by the laboratory director, conducts annually an assessment and an observation of performance for each evaluator. A record of the annual review of each evaluator is dated and signed by the supervisor and the employee. A description of competency review programs is maintained in the management system.

6.2.6 ISO/IEC 17025:2017, 6.2.6 applies.

NOTE Laboratory evaluator collectively has knowledge or experience for any specific technologies upon which an evaluation is conducted in ISO/IEC 19896-3.

6.2.7 ISO/IEC 17025:2017, 6.2 applies with the following additions.

The evaluation laboratory shall maintain a competent administrative and technical personnel appropriate for IT security evaluation on the ISO/IEC 15408 series. The laboratory shall maintain position descriptions, training records, and resumes for responsible supervisory personnel and laboratory evaluators who influence the outcome of security evaluations.

6.3 Facilities and environmental conditions

6.3.1 ISO/IEC 17025:2017, 6.3.1 applies.

6.3.1.1 ISO/IEC 17025:2017, 6.3.1 applies with the following additions.

Laboratory networks used to conduct Test Documentation and the Test Activity (ATE) and Vulnerability Assessment Activity (AVA) evaluation activities shall be effectively isolated to ensure that there are no external influences on test results.

6.3.2 ISO/IEC 17025:2017, 6.3.2 applies.

6.3.3 ISO/IEC 17025:2017, 6.3.3 applies.

6.3.4 ISO/IEC 17025:2017, 6.3.4 applies.

6.3.5 ISO/IEC 17025:2017, 6.3.5 applies.

6.3.5.1 ISO/IEC 17025:2017, 6.3.5 applies with the following additions.

If the evaluation laboratory or the evaluator is conducting its evaluation at the client site or other location outside the laboratory facility, the environment shall conform, as appropriate, to the requirements for the laboratory environment. If a client's system on which an evaluation is conducted is potentially open to access by unauthorized entities during evaluation, the evaluation laboratory or the evaluator shall control the evaluation environment. This is to ensure that the systems are in a defined state compliant with the requirements for the evaluation before starting to perform evaluation work and that the systems ensure that unauthorized entities do not gain access to the system during evaluation.