TECHNICAL SPECIFICATION

ISO/IEC TS 23532-2

First edition
2021-11

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

Part 2: Testing for ISO/IEC 19790

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 2: Essais pour l'ISO/IEC 19790

Reference number
ISO/IEC TS 23532-2:2021(E)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2021 – All rights reserved

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 General Requirements **2**
4.1 Impartiality 2
4.2 Confidentiality 3

5 Structural requirements **3**

6 Resource requirements **4**
6.1 General 4
6.2 Personnel 4
6.3 Facilities and environmental conditions 6
6.4 Equipment 8
6.5 Metrological traceability 11
6.6 Externally provided products and services 12

7 Process requirements **12**
7.1 Review of requests, tenders and contracts 12
7.2 Selection, verification and validation of methods 13
7.2.1 Selection and verification of methods 13
7.2.2 Validation of methods 14
7.3 Sampling 15
7.4 Handling of test or calibration items 15
7.5 Technical records 16
7.6 Evaluation of measurement of uncertainty 16
7.7 Ensuring the validity of results 17
7.8 Reporting of results 17
7.8.1 General 17
7.8.2 Common requirements for reports (test, calibration or sampling) 17
7.8.3 Specific requirements for test reports 18
7.8.4 Specific requirements for calibration certificates 18
7.8.5 Reporting sampling – specific requirements 18
7.8.6 Reporting statements of conformity 18
7.8.7 Reporting opinions and interpretations 19
7.8.8 Amendments to reports 19
7.9 Complaints 19
7.10 Nonconforming work 19
7.11 Control of data information management 20

8 Management system requirements **20**
8.1 Options 20
8.1.1 General 20
8.1.2 Option A 20
8.1.3 Option B 20
8.2 Management system documentation (option A) 20
8.3 Control of management system documents (option A) 21
8.4 Control of records (option A) 21
8.5 Actions to address risks and opportunities (option A) 22
8.6 Improvement (option A) 22
8.7 Corrective actions (option A) 22
8.8 Internal audits (option A) 22
8.9 Management reviews (option A) 22

© ISO/IEC 2021 – All rights reserved

Annex A (informative) **Metrological traceability** **23**
Annex B (informative) **Management system options** **24**
Annex C (informative) **Standards relation in cryptographic module testing** **25**
Bibliography **26**

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

Introduction

Laboratories performing testing for conformance to ISO/IEC 19790 and the test requirements in ISO/IEC 24759 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 validations have specific requirements for competence to ISO/IEC 19790 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 testing and 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 lab 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.

© ISO/IEC 2021 – All rights reserved

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

Part 2:
Testing for ISO/IEC 19790

1 Scope

This document complements and supplements the procedures and general requirements found in ISO/IEC 17025:2017 for laboratories performing testing based on ISO/IEC 19790 and ISO/IEC 24759.

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

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

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

ISO/IEC 19896-2, *IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in in ISO/IEC 17000, ISO/IEC 17025:2017, ISO/IEC 19790, ISO/IEC 19896-1, ISO/IEC 19896-2 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
cryptographic security testing laboratory
testing laboratory
laboratory performing cryptographic module security testing and/or cryptographic algorithms conformance testing

Note 1 to entry: See ISO/IEC 24759 for cryptographic module security testing.

Note 2 to entry: See ISO/IEC 18367 for cryptographic algorithms conformance testing.

© ISO/IEC 2021 – All rights reserved

3.2
implementation under test
IUT
implementation which is tested based on methods specified in this document

[SOURCE: ISO/IEC 17825:2016, 3.9, modified — "International Standard" changed to "document".]

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 laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of cryptographic testing. To avoid any conflict of interest, laboratory policies and procedures shall ensure that the laboratory cannot perform conformance testing if it is currently providing, or has previously provided consulting services, to the vendor for the implementation under test (IUT) (e.g. develop testing evidence, design advice).

NOTE A laboratory can provide clarification of the standards, the test requirements, and other associated documents at any time during the life cycle of the IUT which is not deemed a conflict of interest.

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 laboratory shall have no financial interest for the work performed other than its conformance testing and/or validation fees.

4.1.3 ISO/IEC 17025:2017, 4.1.3 applies.

4.1.3.1 ISO/IEC 17025:2017, 4.1.3 applies with the following additions.

The laboratory shall not perform conformance testing on a module for which the laboratory has:

a) designed any part of the IUT;

b) developed original documentation for any part of the IUT;

c) built, coded or implemented any part of the IUT;

d) had any ownership or vested interest in the IUT; or

e) provided consulting for any part of the IUT.

NOTE The laboratory can perform conformance testing on an IUT produced by a company when:

— the laboratory has no ownership in the company;

— the laboratory has a separate management from the company; and

— business between the cryptographic security testing laboratory and the company is performed under contractual agreements, as done with other clients.

© ISO/IEC 2021 – All rights reserved