



BSI Standards Publication

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

Part 2: Testing for ISO/IEC 19790

National foreword

This Published Document is the UK implementation of CEN/CLC ISO/IEC/TS 23532-2:2024. It is identical to ISO/IEC TS 23532-2:2021. It supersedes PD ISO/IEC TS 23532-2:2021, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/3, Security Evaluation, Testing and Specification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 33655 9

ICS 35.030

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2021.

Amendments/corrigenda issued since publication

Date	Text affected
31 October 2024	This corrigendum rennumbers PD ISO/IEC TS 23532-2:2021 as PD CEN/CLC ISO/IEC/TS 23532-2:2024

English version

Information security, cybersecurity and privacy protection
- Requirements for the competence of IT security testing
and evaluation laboratories - Part 2: Testing for ISO/IEC
19790 (ISO/IEC/TS 23532-2:2021)

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 (ISO/IEC/TS
23532-2:2021)

Informationssicherheit, Cybersicherheit und Schutz
der Privatsphäre - Anforderungen an die Kompetenz
von Prüf- und Evaluierungsstellen für IT-Sicherheit -
Teil 2: Prüfung für ISO/IEC 19790 (ISO/IEC/TS 23532-
2:2021)

This Technical Specification (CEN/TS) was approved by CEN on 16 September 2024 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN and CENELEC will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN and CENELEC members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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.



European foreword

The text of ISO/IEC TS 23532-2:2021 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 CEN/CLC ISO/IEC/TS 23532-2:2024 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

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 announce this Technical Specification: 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 TS 23532-2:2021 has been approved by CEN-CENELEC as CEN/CLC ISO/IEC/TS 23532-2:2024 without any modification.

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

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

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 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.

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.

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.

4.1.4 ISO/IEC 17025:2017, 4.1.4 applies.

4.1.4.1 ISO/IEC 17025:2017, 4.1.4 applies with the following additions.

A laboratory may take existing vendor documentation for an IUT (post-design and post-development) and consolidate or reformat the information (from multiple sources) into a set format.

4.1.5 ISO/IEC 17025:2017, 4.1.5 applies.

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.

5 Structural requirements

5.1 ISO/IEC 17025:2017, 5.1 applies.

5.1.1 ISO/IEC 17025:2017, 5.1 applies with the following additions.

Laboratories shall ensure separation between laboratory testers and the company's resources who may have an interest in or may influence testing outcome.

5.1.2 ISO/IEC 17025:2017, 5.1 applies with the following additions.

For any other services of the laboratory's parent corporation not listed in [5.1](#), the laboratory shall have an explicit policy and a set of procedures for maintaining a strict separation, both physical and electronic, between the laboratory testers and company's consultant teams, product developers, system integrators, and others who may have an interest in and/or may unduly influence the testing outcome.

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 laboratory shall define and state the scope of laboratory activities including the following:

a) selected standard(s);

EXAMPLE 1 Such as ISO/IEC 19790 and ISO/IEC 24759 which address cryptographic module requirements and testing.

1) security level(s) and area(s);

EXAMPLE 2 Such as up to overall security rating 2 and physical security level 3.

2) physical embodiment(s);

EXAMPLE 3 Such as multi-chip embedded cryptographic modules and multi-chip standalone cryptographic modules.