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 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 ..... **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.

3) type(s) of cryptographic modules;

EXAMPLE 4 Such as a software (cryptographic) module.

b) laboratory's permanent facility.

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

The laboratory should define and state the scope of laboratory activities including the following:

a) categories of cryptographic algorithms and protocols which the laboratory is competent to test;

EXAMPLE 1 Such as symmetric key cryptographic algorithms and dedicated hash functions.

EXAMPLE 2 Such as various cryptographic algorithms employed in Transport Layer Security (TLS) protocol.

b) product technology types which the laboratory is competent to test.

EXAMPLE 3 Such as USB flash drives.

EXAMPLE 4 Such as Self-Encrypting Drives with SATA interface.

EXAMPLE 5 Such as network encryption devices with IPsec protocol.

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.

6 Resource requirements

6.1 General

ISO/IEC 17025:2017, 6.1 applies.

6.1.1 ISO/IEC 17025:2017, 6.1 applies with the following additions.

The management system documentation shall contain all documentation that describes and details the laboratory's implementation of procedures covering all the technical requirements in ISO/IEC 17025:2017 and this document.

6.2 Personnel

6.2.1 ISO/IEC 17025:2017, 6.2.1 applies.

6.2.1.1 ISO/IEC 17025:2017, 6.2.1 applies with the following additions.

The laboratory shall maintain responsible supervisory personnel and competent technical staff that are:

a) knowledgeable of all scheme-specific test methods, test metrics and implementation guidance;

b) knowledgeable of all relevant international standards, and references in this document;

c) familiar with cryptographic terminology and families of cryptographic algorithms and security functions; and

d) familiar with the cryptographic testing tools.

6.2.1.2 ISO/IEC 17025:2017, 6.2.1 applies with the following additions.

The laboratory shall continuously maintain competent testers.

NOTE See ISO/IEC 19896-2 for a definition of areas that constitute required proficiency.

6.2.2 ISO/IEC 17025:2017, 6.2.2 applies.

NOTE 1 The "technical knowledge" in ISO/IEC 17025:2017, 6.2.2 is described in ISO/IEC 19896-2:2018, Clause 6.

NOTE 2 The "skills" in ISO/IEC 17025:2017, 6.2.2 are described in ISO/IEC 19896-2:2018, Clause 7.

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

The laboratory shall maintain a list of the key personnel, including their assigned roles and a summary of their latest training qualifications. The list shall include, but shall not be limited to:

a) laboratory director;

b) laboratory manager(s);

c) staff members(s) responsible for maintaining management system;

d) authorized representative;

e) approved signatories; and

f) other key technical persons in the laboratory (e.g. testers).

NOTE 1 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).

NOTE 2 In order to perform objective and meaningful reviews of reported results in ISO/IEC 17025:2017, 7.7.1, item i), the laboratory can employ multiple testers to ensure that another qualified and competent tester is in charge of the review, who is not involved in testing the IUT subject to review.

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

Laboratories shall document the required qualifications for each staff position.

NOTE Staff information can be kept in the official personnel folders.

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

The number of qualified testers within the laboratory shall be greater than or equal to the scheme-specific minimum required number of testers.

EXAMPLE Such as a minimum of two qualified testers.

6.2.3 ISO/IEC 17025:2017, 6.2.3 applies.

6.2.3.1 ISO/IEC 17025:2017, 6.2.3 applies with the following additions.

If the mechanism by which the laboratory employs staff members is through contracting of personnel, any key personnel who are contractors shall be identified and listed.

6.2.4 ISO/IEC 17025:2017, 6.2.4 applies.

6.2.4.1 ISO/IEC 17025:2017, 6.2.4 applies with the following additions.

An individual may be assigned or appointed to serve in more than one position provided it does not create a conflict of interest and maintains impartiality. To the extent possible, the laboratory director and the person responsible for implementing and maintaining the management system should be independently staffed.

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 laboratory person(s) responsible for implementing and maintaining the management system shall receive management system training preferably in ISO/IEC 17025:2017. If training is not available in ISO/IEC 17025:2017, minimum training shall be acquired in the ISO 9000 family of standards, especially ISO 9001, or equivalent with emphasis for internal auditing.

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

The laboratory shall have a competency review program and procedures for the evaluation and maintenance of the competency of each staff member for each test method the staff member is authorized to conduct. An evaluation and an observation of performance shall be conducted annually for each staff member by the immediate supervisor or a designee appointed by the laboratory director. A record of the annual evaluation of each staff member shall be dated and signed by the supervisor and the employee.

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

The laboratory management shall ensure adequate training for the laboratory staff as directed in 6.2.5.1. The personnel shall possess knowledge of or be trained in ISO/IEC 19896-2.

6.2.6 ISO/IEC 17025:2017, 6.2.6 applies.

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.

The laboratory shall have its internal networks protected from unauthorized access by external entities, as well as protection against malicious software.

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

Within the internal networks, information/data shall be protected commensurate with their classification and/or sensitivity, and access to them shall be given only to authorized personnel.

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

NOTE In considering a test setup of an IUT, the test harness and supporting/surrounding test apparatus can impose constraints such as performance and availability. Such equipment is appropriately selected.

EXAMPLE Network throughput may affect the determination of pass/fail of assertion [04.50] (the strength of the authentication objective), because the number of authentication requests can be limited by the network throughput.

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

The laboratory shall have Internet access for obtaining the most current documentation and test tools and secure communication capabilities.

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.

6.3.4.1 ISO/IEC 17025:2017, 6.3.4 applies with the following additions.

The laboratory shall have appropriate areas, including ventilation and safety, for the use of test methods using chemical solvents and heating/cooling apparatus.

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.

Temporary off-site locations may be used for performing physical testing (e.g. vendor sites or specialized physical testing facility such as a university lab).

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

If a laboratory conducts conformance testing at a location outside the laboratory facility, the environment shall conform, as appropriate, to the requirements of this document.

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

Testing activities may also be conducted at the vendor site. When testing is performed at a vendor site, all requirements in this document pertaining to equipment and environment as they apply to the tests scheduled outside the laboratory's permanent location, shall apply. Only the personnel of the laboratory shall perform all actions necessary to conduct the tests and record the results, including the loading, compiling, configuring, and execution of any of the mandated testing tools.

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

IUT specific documentation, specific test jigs, harnesses, supporting test apparatus or test results, shall be protected (e.g. from physical, logical, or visual access) from persons outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons.

a) The laboratory manager shall identify and document for each specific IUT the laboratory personnel who either have a need to know or have authorized access of the IUT, documentation and testing related apparatus including rationale for such access.

b) An audit log shall be maintained documenting personnel who have had access to each IUT during the contracted timeframe and all supporting documentation and testing related apparatus. Authorized vendor personnel for the IUT under contract may be granted access by the laboratory per the contract.

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

If a vendor's system on which testing is conducted is potentially open to access by third parties, the laboratory shall ensure that the testing environment is controlled so that the third parties do not gain access to that system during testing.

6.4 Equipment

6.4.1 ISO/IEC 17025:2017, 6.4.1 applies.

NOTE 1 Special equipment can be necessary for particular test methods. For more information regarding types of equipment and information required for conducting the conformance tests, see ISO/IEC 24759 and ISO/IEC 19896-2.

NOTE 2 Test equipment refers to software and hardware products and/or other assessment mechanisms used by the laboratory to support the cryptographic testing of the IUT.

6.4.1.1 ISO/IEC 17025:2017, 6.4.1 applies with the following additions.

The laboratory shall ensure that, when applicable, the correct version of testing tools is used and that the tools have not been altered in any way that might lead to incorrect results.

6.4.1.2 ISO/IEC 17025:2017, 6.4.1 applies with the following additions.

The laboratory shall have appropriate hardware, software, test tools and computer facilities to conduct cryptographic testing. This includes, but is not limited to:

a) required software test suites;

b) testing equipment for physical tests; and

c) all special equipment necessary to perform all tests derived from the most current version of the standard.

6.4.1.2.1 The laboratory shall own at least one designated workstation and shall have Internet access and e-mail capability. Workstations shall have interfaces for loading images from a digital camera and acquiring scanned document images and/or hard copy printouts. Workstations shall have sufficient storage capability, performance and features as specified by the tool provider.

EXAMPLE In case that maintenance of workstations is required, it is recommended to select "keep your HDD" service option in purchasing the workstations so that maintenance service operators do not access the HDD containing sensitive data.

6.4.1.2.2 The laboratory shall also meet the following minimum requirements for hardware, software and firmware components:

a) hardware components: security levels 1 to 4:

   1) tools to conduct testing of tamper evidence on coatings;

   2) tools to conduct enclosure removal/penetration test;

   3) tools to conduct physical and thermal coating/potting removal/penetration tests;

   4) tools to conduct opacity and probing tests;

   5) tools to conduct tests on locks;

   6) tools to conduct mechanical/thermal/chemical tests on tamper evidence label removability;

   7) tools to test tamper detection mechanisms/switches on doors and removable covers;

   8) digital camera with flash and macro (near focus) features (phones are not acceptable);

   9) tools to conduct tests on fasteners (e.g. drills);

   10) tools to monitor/capture/exercise the data input/output of cryptographic module interfaces, at logical level (procured, rented, or leased, as needed).

EXAMPLE 1 Such as network analyser, packet analyser, USB protocol analyser/exerciser, SATA protocol analyser/exerciser, PCI express protocol analyser.

NOTE 1 This is also related to ISO/IEC 17025:2017, 6.4.5.

NOTE 2 The cryptographic module interfaces would be specified from a high-level layer, e.g. application layer ultimately down to physical layer for hardware modules. Cryptographic module security requirements about cryptographic module interfaces are applicable several layers, therefore it is possible that this is not enough just to test only at very high-level layer from cryptographic module validation perspective.

EXAMPLE 2 Such as testing cryptographic modules of layer 3 encryptor by using layer 7 (i.e. application layer) commands.

b) hardware components: additional requirements for security levels 3 to 4:

   1) variable power supply;

   2) temperature chamber (procured, rented, or leased, as needed);

   3) digital storage oscilloscope or logic analyser (procured, rented, or leased, as needed);

   4) non-invasive security:

      i) digital oscilloscope with enough band width (procured, rented, or leased, as needed);

      NOTE 3 Here the band width will be at least greater than or equal to the clock frequency of the IUT. It is said that digital oscilloscopes with band width of 2,5 GHz or higher have built-in preamplifiers superior to those of narrower band width. Also, high resolution (i.e. A/D conversion bits with more than 8-bit) can be used to discriminate subtle difference in information leakage, which would affect the number of waveforms required to perform side-channel analysis.

      ii) tools to acquire voltage drop, or electromagnetic emanation (e.g. differential probe, pick-up coil) for side-channel analysis;

      NOTE 4 Near-field microprobes can be characterised by their diameter and gain characteristic curve. It can be required to select which microprobes are to be used depending on the characteristic of an IUT.

c) hardware components: additional requirements for security level 4:

   1) tools to conduct enclosure testing (e.g. grilling, milling);

   2) tools to test tamper detection envelope;

   3) solvents to conduct chemical coating removal tests;

d) software components (security levels 1 to 2) and firmware components (security levels 1 to 4):

   1) tools to conduct software testing - appropriate compilers, debuggers, and binary editors;

e) reporting tools:

   1) ISO/IEC 19790 and ISO/IEC 24759 tools (latest version).

6.4.1.2.3 Chemical solvents and adhesive remover will likely have their own expiry date for their quality. Such consumables shall be checked periodically for validity, or newly purchased on-demand for IUT testing.

6.4.1.2.4 If non-invasive security area with security level 3 or 4 is included in the scope of laboratory activity, a Faraday cage or EMI shield box shall be required with temperature control.

6.4.2 ISO/IEC 17025:2017, 6.4.2 applies.

EXAMPLE Digital oscilloscopes shipped to a calibration service, or equipment taken out from the laboratory but still inside the company to be used for other purpose or used by an intern.

6.4.3 ISO/IEC 17025:2017, 6.4.3 applies.

6.4.3.1 ISO/IEC 17025:2017, 6.4.3 applies with the following additions.

Confirmation of the use of the most current version of testing tools shall be assured before conducting a test. Records of these confirmations shall be maintained.

6.4.3.2 ISO/IEC 17025:2017, 6.4.3 applies with the following additions.

The equipment used for conducting cryptographic testing shall be maintained in accordance with the manufacturer's recommendations and in accordance with internally documented laboratory procedures, as applicable.

6.4.3.3 ISO/IEC 17025:2017, 6.4.3 applies with the following additions.

Whenever major or minor changes are made to any testing tool, a laboratory shall have procedures to assure the accurate execution and correct performance of the test tool. The procedures shall include, at a minimum, the complete set of regression testing of the test tool. This is necessary to ensure that consistency is maintained, as appropriate, with other laboratories and that correctness is maintained with respect to the relevant standard(s) or specification(s).

6.4.3.4 ISO/IEC 17025:2017, 6.4.3 applies with the following additions.

If applicable, the equipment used for conducting the conformance tests shall be maintained and calibrated in accordance with the manufacturer's recommendation, as specified in the test method, or as specified in the annex associated with the specific test method(s).

6.4.4 ISO/IEC 17025:2017, 6.4.4 applies.

6.4.4.1 ISO/IEC 17025:2017, 6.4.4 applies with the following additions.

The laboratory shall ensure that any test tool used to conduct cryptographic testing is performing properly according to specifications. The laboratory shall also ensure that the tool does not interfere with the conduct of the test and does not modify or impact the IUT.

6.4.5 ISO/IEC 17025:2017, 6.4.5 applies.

6.4.6 ISO/IEC 17025:2017, 6.4.6 applies.

6.4.7 ISO/IEC 17025:2017, 6.4.7 applies.

6.4.7.1 ISO/IEC 17025:2017, 6.4.7 applies with the following additions.

For calibrations performed in-house, the reference standards used and the environmental conditions at the time of calibration shall be documented for all calibrations. Calibration records and evidence of the traceability of the reference standards used shall be readily available.

6.4.8 ISO/IEC 17025:2017, 6.4.8 applies.

6.4.9 ISO/IEC 17025:2017, 6.4.9 applies.

6.4.9.1 ISO/IEC 17025:2017, 6.4.9 applies with the following additions.

The laboratory shall document and follow appropriate procedures whenever a test tool suspected or found to contain errors that make the tool defective or unfit for use. These procedures shall include establishing that there is a genuine error, reporting the error to the appropriate maintenance authority. If the conformance testing results change for an IUT after correcting the test tool, then the information shall be clearly identified.

6.4.10 ISO/IEC 17025:2017, 6.4.10 applies.

6.4.11 ISO/IEC 17025:2017, 6.4.11 applies.

6.4.12 ISO/IEC 17025:2017, 6.4.12 applies.

6.4.13 ISO/IEC 17025:2017, 6.4.13 applies.

6.4.13.1 ISO/IEC 17025:2017, 6.4.13 applies with the following additions.

The laboratory shall maintain a record of the tools used for each test report involving physical testing.

6.4.13.2 ISO/IEC 17025:2017, 6.4.13 applies with the following additions.

Laboratories shall maintain records of the configuration of test equipment (hardware and software) and all analyses to ensure the suitability of test equipment to perform the desired testing.

6.4.13.3 ISO/IEC 17025:2017, 6.4.13 applies with the following additions.

Records shall be kept of the date, extent of all hardware and software upgrades and updates, and periods of use.

6.5 Metrological traceability

6.5.1 ISO/IEC 17025:2017, 6.5.1 applies.

NOTE See Annex A for additional information on metrological traceability.

6.5.1.1 ISO/IEC 17025:2017, 6.5.1 applies with the following additions.

For cryptographic testing, “traceability” is interpreted to mean that the test tools shall be traceable back to the underlying requirements in ISO/IEC 19790 and ISO/IEC 24759. This means that each abstract test case and the associated testing methodology are traceable to a specific cryptographic requirement listed in the governing documentary standard. Test results produced by the laboratory shall be traceable to standard test suites when appropriate, or otherwise to the applicable authoritative test suite.

NOTE Traceability to the International Standards requirements is achieved via the assertions, the associated test requirement documents and provided validation authorities test reporting tools. ISO/IEC 24759 is divided into two sets of requirements: one levied on the vendor and one levied on the tester of the cryptographic module.

6.5.2 ISO/IEC 17025:2017, 6.5.2 applies.

6.5.3 ISO/IEC 17025:2017, 6.5.3 applies.

6.5.4 ISO/IEC 17025:2017, 6.5 applies with the following additions.

6.5.4.1 Test vectors and results for cryptographic algorithm testing shall be generated and checked using a validation authorities' tool if provided.

NOTE 1 Tools for cryptographic algorithm testing can be purposely designed to detect well-known or foreseen nonconforming implementations of cryptographic algorithms selected. However, there can be a limit in the capability of detecting such nonconforming implementations, e.g. due to limited number of test vectors provided to each IUT, and/or due to the limited test coverage of requirements in the cryptographic algorithm standards selected.

NOTE 2 There can be tools for estimating entropy for the raw output of non-deterministic random bit generators. Specifications of non-deterministic random bit generators are diverse, and therefore there would be no "standard" to which designs of non-deterministic random bit generators trace back. From the viewpoint of cryptographic module security requirements, only the value of entropy is essential for non-deterministic random bit generators. In that sense, it is possible that "traceability" cannot be applied to tools for estimating entropy, and instead ISO/IEC 17025:2017, 7.3 and ISO/IEC 17025:2017, 7.6 can be applied.

6.5.5 ISO/IEC 17025:2017, 6.5 applies with the following additions.

6.5.5.1 In those technical areas where there is a difference between validation authorities test objectives and the testing tool's abstract test cases, the laboratory shall show how each realization of a test case is derived faithfully from the governing document with preservation of assignment of verdicts or measurements to the corresponding sets of observations.

6.6 Externally provided products and services

6.6.1 ISO/IEC 17025:2017, 6.6.1 applies.

6.6.2 ISO/IEC 17025:2017, 6.6.2 applies.

6.6.3 ISO/IEC 17025:2017, 6.6.3 applies.

6.6.4 ISO/IEC 17025:2017, 6.6 applies with the following additions.

If externally provided testing activities (i.e. subcontract) is used as a mechanism by which the laboratory fulfils and/or enhances the conformance testing process, the external laboratory shall meet the requirements of ISO/IEC 17025:2017 and this document.

7 Process requirements

7.1 Review of requests, tenders and contracts

7.1.1 ISO/IEC 17025:2017, 7.1.1 applies.

NOTE The laboratory can use checklists and/or contract agreements to satisfy this requirement.

7.1.1.1 ISO/IEC 17025:2017, 7.1.1 applies with the following additions.

The laboratory and vendor shall agree, in writing, what constitutes the IUT and what constitutes the environment within the IUT. For some schemes, the environment includes, but it is not limited to:

a) the specific test platform;

b) the test configuration; and

c) the external environment.

7.1.1.2 ISO/IEC 17025:2017, 7.1.1 applies with the following optional additions.

The laboratory and vendor shall agree on which party is responsible for developing or providing test jigs, test harness, or test environment.

7.1.2 ISO/IEC 17025:2017, 7.1.2 applies.

7.1.3 ISO/IEC 17025:2017, 7.1.3 applies.

7.1.3.1 ISO/IEC 17025:2017, 7.1.3 applies with the following additions.

The requirement in ISO/IEC 17025:2017, 7.1.3 applies to the case where the decision rule is not clearly defined in the relevant standards or implementation guidance provided by the cryptographic module validation scheme. Examples are tamper-evident seals/labels testing where a trace can remain for some seals/labels and not for others, and non-invasive security testing where pass/fail metrics are not specified by ISO/IEC 19790 and ISO/IEC 24759.

7.1.4 ISO/IEC 17025:2017, 7.1.4 applies.

7.1.5 ISO/IEC 17025:2017, 7.1.5 applies.

7.1.6 ISO/IEC 17025:2017, 7.1.6 applies.

7.1.7 ISO/IEC 17025:2017, 7.1.7 applies.

7.1.8 ISO/IEC 17025:2017, 7.1.8 applies.

7.1.8.1 ISO/IEC 17025:2017, 7.1.8 applies with the following additions.

Policies for documents storage and maintenance of contracts under confidentiality, nondisclosure agreements, marked as secret, or copyright protected, shall be well defined according to the document's status. These documents shall be protected commensurate with their classification and/or sensitivity, and access to them shall be given only to authorized personnel. When cryptography is utilized as the mechanism for protection of information, the cryptographic module used shall be validated and operating in an approved mode of operation.

7.1.9 ISO/IEC 17025:2017, 7.1 applies with the following additions.

Additional requirements for the selection, verification and validation of methods are the following:

a) laboratories shall use the test methods described in ISO/IEC 24759;

b) when exceptions are deemed necessary for technical reasons, details shall be described in the test report.

7.2 Selection, verification and validation of methods

7.2.1 Selection and verification of methods

NOTE 1 In the course of physical security testing of tamper-evident seals/labels, it is possible that testers simulate the procedure to apply tamper-evident seals/labels before trying to open a cover or door without breaking or removing the seals/labels. In this case, it is possible that the procedure to apply seal/labels is accurately simulated but the environmental conditions to apply seals (e.g. humidity) could be different from those of manufacturing site of the IUTs. This can be one of the factors affecting the results of physical security testing.

NOTE 2 In the course of non-invasive security testing, there can be multiple factors including but not limited to the following, which are affecting the measurement uncertainty and the test results:

— A/D conversion bits of digital oscilloscopes;

— bandwidth of digital oscilloscopes;

— sampling rate of digital oscilloscopes;

— externally provided clock input (e.g. sinusoidal wave or rectangular wave);

— pre-amplifiers applied to acquire waveforms;

— analogue and/or digital filters applied to acquire waveforms;

— digital filters applied to acquired waveforms;

— precision of floating-point arithmetic employed in the analysis of side-channel leakage.

7.2.1.1 ISO/IEC 17025:2017, 7.2.1.1 applies.

7.2.1.2 ISO/IEC 17025:2017, 7.2.1.2 applies.

7.2.1.3 ISO/IEC 17025:2017, 7.2.1.3 applies.

7.2.1.4 ISO/IEC 17025:2017, 7.2.1.4 applies.

7.2.1.5 ISO/IEC 17025:2017, 7.2.1.5 applies.

7.2.1.6 ISO/IEC 17025:2017, 7.2.1.6 applies.

7.2.1.7 ISO/IEC 17025:2017, 7.2.1.7 applies.

7.2.1.7.1 ISO/IEC 17025:2017, 7.2.1.7 applies with the following additions.

Laboratories shall use the test methods described in ISO/IEC 24759 associated with that specific test method(s). When exceptions to the test methods are deemed necessary for technical reasons, the vendor shall be informed, and details shall be described in the test report. Documentation shall be provided on the test method exceptions taken to ensure that the correct and required precision and interpretation of the validation authorities test method is maintained.

7.2.1.8 ISO/IEC 17025:2017, 7.2.1 applies with the following additions.

Tools for cryptographic algorithm testing may be updated so that they can purposely detect newly discovered nonconforming implementations of cryptographic algorithm(s) selected. If the testing procedures/testing methodology employed in the tools are revised to the extent where test harnesses have to be revised to accommodate the revision, the laboratory shall share the fact with its customers.

7.2.2 Validation of methods

NOTE There can be tools for estimating entropy for the raw output of non-deterministic random bit generators and tools for determining pass/fail for non-invasive security. The requirements of ISO/IEC 17025:2017, 7.2.2 apply to such tools, where NOTE 2 f) plays an important role.

7.2.2.1 ISO/IEC 17025:2017, 7.2.2.1 applies.

7.2.2.1.1 ISO/IEC 17025:2017, 7.2.2.1 applies with the following additions.

For a given test tool, there may be no suitable validation service available outside the laboratory, and no suitable reference implementation that could be used by the laboratory to validate the test tool. In this situation, the laboratory shall define and document the procedures and methods that it uses to check on the correct operation of the test tool and provide evidence that these procedures and methods are applied whenever the test tool is modified.

7.2.2.2 ISO/IEC 17025:2017, 7.2.2.2 applies.

7.2.2.3 ISO/IEC 17025:2017, 7.2.2.3 applies.

7.2.2.4 ISO/IEC 17025:2017, 7.2.2.4 applies.

7.3 Sampling

NOTE There are cryptographic modules with non-deterministic random bit generators. It is often the case that analogue information inside the cryptographic module is quantised/digitised and the digitised value is used as a seed of deterministic random bit generator. Here the characteristics of analogue information can be affected to some extent by the characteristics of the cryptographic module and by the environmental conditions. There can be a need to assess the difference in the variation/dispersion of seed values, by sampling multiple instances of the same model of cryptographic module, unless the customer/vendor is solely responsible for the variation/dispersion or the customer/vendor asks the laboratory to test by using a specific IUT sample.

EXAMPLE 1 When multiple instances of the same model of cryptographic module are provided for tests, sampling a singular part from the set to perform physical security testing.

EXAMPLE 2 When a model of cryptographic module is subject to testing but some of its security related internal components are from multiple sources, sampling only a few instances from the possible combination.

7.3.1 ISO/IEC 17025:2017, 7.3.1 applies.

7.3.2 ISO/IEC 17025:2017, 7.3.2 applies.

7.3.3 ISO/IEC 17025:2017, 7.3.3 applies.

7.4 Handling of test or calibration items

7.4.1 ISO/IEC 17025:2017, 7.4.1 applies.

7.4.1.1 ISO/IEC 17025:2017, 7.4.1 applies with the following additions.

The testing laboratory shall have procedures to ensure proper retention, disposal or return of software and hardware after the completion of testing.

7.4.2 ISO/IEC 17025:2017, 7.4.2 applies.

NOTE It is a good practice to use a configuration management system to trace samples of IUTs and parts of IUTs, which enables mapping between identifiers within the laboratory and identifiers used by vendors.

7.4.2.1 ISO/IEC 17025:2017, 7.4.2 applies with the following additions.

If the laboratory is conducting multiple simultaneous testing activities, a system of separation between IUTs of different vendors and conformance testing activities shall be maintained as necessary.

7.4.3 ISO/IEC 17025:2017, 7.4.3 applies.

7.4.4 ISO/IEC 17025:2017, 7.4.4 applies.

7.4.5 ISO/IEC 17025:2017, 7.4 applies with the following additions.

Laboratories shall protect all IUTs from modifications of any kind or unauthorized access and use. Cryptographic mechanisms utilized to protect information shall be validated and operating in an approved mode of operation.

7.4.6 ISO/IEC 17025:2017, 7.4 applies with the following additions.

When the IUT consists of software/firmware components, and/or when any documents are provided by the vendor associated with the IUT, the laboratory shall ensure that a configuration management system is in place to prevent inadvertent modifications. This configuration management system shall uniquely identify each IUT and control and document modifications to any of the software components.

7.5 Technical records

7.5.1 ISO/IEC 17025:2017, 7.5.1 applies.

7.5.2 ISO/IEC 17025:2017, 7.5.2 applies.

7.5.3 ISO/IEC 17025:2017, 7.5 applies with the following additions.

The final test results and/or the test reports generated for the IUT shall be kept by the laboratory following the completion of testing for the life of the IUT, or as specified by the vendor in writing. Records may include hard or digital copies of the official test results and the test results error file(s). Records shall be stored in a manner that assures survivability, confidentiality, integrity, and accessibility. When cryptography is utilized as the mechanism for protection of information, the cryptographic module used shall be validated and operating in an approved mode of operation.

7.6 Evaluation of measurement of uncertainty

7.6.1 ISO/IEC 17025:2017, 7.6.1 applies.

7.6.2 ISO/IEC 17025:2017, 7.6.2 applies.

7.6.3 ISO/IEC 17025:2017, 7.6.3 applies.

7.6.3.1 ISO/IEC 17025:2017, 7.6.3 applies with the following additions.

In the course of sensitive security parameter testing, the laboratory should assess the amount of entropy collected / generated inside the IUTs. Although the collection / generation mechanism would be perfectly managed by the IUTs, there would be still a little room to estimate the value of entropy in bits. For example, the following factors could be considered:

— number of times to collect entropy inputs for estimating entropy in bits;

— operating temperature of the IUT when the entropy source is based on the thermal noise;

— elapsed time from power-on;

— precision of floating-point arithmetic employed in estimating entropy.

7.6.3.2 ISO/IEC 17025:2017, 7.6.3 applies with the following additions.

In the course of non-invasive security testing, the laboratory should evaluate/estimate measurement uncertainty. Practically this could be demonstrated by the various sets of tool(s), input file(s), output file(s), and their associated parameters.

7.7 Ensuring the validity of results

7.7.1 ISO/IEC 17025:2017, 7.7.1 applies.

7.7.2 ISO/IEC 17025:2017, 7.7.2 applies.

7.7.3 ISO/IEC 17025:2017, 7.7.3 applies.

7.8 Reporting of results

7.8.1 General

7.8.1.1 ISO/IEC 17025:2017, 7.8.1.1 applies.

7.8.1.1.1 ISO/IEC 17025:2017, 7.8.1.1 applies with the following additions.

The laboratory shall perform an independent technical quality review of the test report submission documents prior to submission to the validation program. This shall address accuracy, completeness, sufficient evidence of test results and consistency. A record of this review shall be maintained.

7.8.1.2 ISO/IEC 17025:2017, 7.8.1.2 applies.

7.8.1.2.1 ISO/IEC 17025:2017, 7.8.1.2 applies with the following additions.

The laboratory shall ensure that an integrity and confidentiality mechanism commensurate with the data sensitivity and/or government requirements when electronic delivery of the test reports is employed, to ensure that the test report cannot be disclosed to anyone other than the intended recipient(s) and an integrity mechanism exists to ensure that the test report is not modified.

7.8.1.3 ISO/IEC 17025:2017, 7.8.1.3 applies.

7.8.1.4 ISO/IEC 17025:2017, 7.8.1 applies with the following additions.

The laboratory shall issue test reports of its work that accurately, clearly and unambiguously present the test conditions, the test setup when it varies from the standard protocol, the test results, and all other information necessary to reproduce the test. Any deviations or omissions shall be clearly indicated. Test reports to customers shall meet contractual requirements in addition to meeting the requirements of ISO/IEC 17025:2017 and this document. Test reports shall provide all necessary information to permit reproduction of the test and to obtain consistent results.

7.8.2 Common requirements for reports (test, calibration or sampling)

7.8.2.1 ISO/IEC 17025:2017, 7.8.2.1 applies.

7.8.2.1.1 ISO/IEC 17025:2017, 7.8.2.1 applies with the following additions.

If test report tools or other reporting methodologies are provided, the laboratory shall follow those requirements and use those supplied test tools.

7.8.2.2 ISO/IEC 17025:2017, 7.8.2.2 applies.

7.8.2.2.1 ISO/IEC 17025:2017, 7.8.2.2 applies with the following additions.

The laboratory shall clearly identify opinions, interpretations, or results which are outside the scope of ISO/IEC 24759.

7.8.2.3 ISO/IEC 17025:2017, 7.8.2 applies with the following additions.

Whenever test cases are such that an analysis of the observations by the testing staff is required to interpret the results before stating them in a test report, the laboratory shall have objective procedures to be followed by the test operators performing the analysis, sufficient to ensure that the repeatability, reproducibility, and objectivity of the test results can be maintained.

7.8.2.4 ISO/IEC 17025:2017, 7.8.2 applies with the following additions.

Test reports shall meet the requirements of ISO/IEC 24759 as well as the requirements of ISO/IEC 17025:2017 and this document.

7.8.2.5 ISO/IEC 17025:2017, 7.8.2 applies with the following additions.

The test reports for each project shall identify the work performed at each laboratory's permanent facility, or in associated each temporary or mobile facility, if applicable.

7.8.2.6 ISO/IEC 17025:2017, 7.8.2 applies with the following additions.

The opacity and/or strength of the epoxy covering is subject to the manufacturing process, and vendors may provide the laboratory with vendor-sampled multi-chip embedded cryptographic modules with epoxy covering. In this case, the laboratory shall state that the results relate only to the cryptographic modules sampled.

7.8.3 Specific requirements for test reports

7.8.3.1 ISO/IEC 17025:2017, 7.8.3.1 applies.

7.8.3.2 ISO/IEC 17025:2017, 7.8.3.2 applies.

7.8.4 Specific requirements for calibration certificates

7.8.4.1 ISO/IEC 17025:2017, 7.8.4.1 applies.

NOTE See Annex A for additional information on metrological traceability.

7.8.4.2 ISO/IEC 17025:2017, 7.8.4.2 applies.

7.8.4.3 ISO/IEC 17025:2017, 7.8.4.3 applies.

7.8.5 Reporting sampling – specific requirements

ISO/IEC 17025:2017, 7.8.5 applies.

7.8.6 Reporting statements of conformity

7.8.6.1 ISO/IEC 17025:2017, 7.8.6.1 applies.

EXAMPLE 1 Such as a heuristic analysis for an entropy source based on human interaction (e.g. key strokes, mouse movement).

EXAMPLE 2 Such as a heuristic analysis for an entropy source based on a result from speculative execution combined with conditional branching.

7.8.6.2 ISO/IEC 17025:2017, 7.8.6.2 applies.

7.8.7 Reporting opinions and interpretations

7.8.7.1 ISO/IEC 17025:2017, 7.8.7.1 applies.

7.8.7.2 ISO/IEC 17025:2017, 7.8.7.2 applies.

7.8.7.3 ISO/IEC 17025:2017, 7.8.7.3 applies.

7.8.8 Amendments to reports

7.8.8.1 ISO/IEC 17025:2017, 7.8.8.1 applies.

7.8.8.2 ISO/IEC 17025:2017, 7.8.8.2 applies.

7.8.8.2.1 ISO/IEC 17025:2017, 7.8.8.2 applies with the following additions.

For test reports created for purposes other than official IUT validation, the laboratory shall issue corrections or additions to a test report only by a supplementary document suitably marked; e.g. “Supplement to test report serial number [...]”. If the change involves a test assertion, this supplementary document shall specify which test assertion is in question, the content of the result, the explanation of the result and the reason for acceptance of the result.

7.8.8.3 ISO/IEC 17025:2017, 7.8.8.3 applies.

7.9 Complaints

7.9.1 ISO/IEC 17025:2017, 7.9.1 applies.

7.9.2 ISO/IEC 17025:2017, 7.9.2 applies.

7.9.3 ISO/IEC 17025:2017, 7.9.3 applies.

7.9.4 ISO/IEC 17025:2017, 7.9.4 applies.

7.9.5 ISO/IEC 17025:2017, 7.9.5 applies.

7.9.6 ISO/IEC 17025:2017, 7.9.6 applies.

7.9.7 ISO/IEC 17025:2017, 7.9.7 applies.

7.10 Nonconforming work

7.10.1 ISO/IEC 17025:2017, 7.10.1 applies.

7.10.2 ISO/IEC 17025:2017, 7.10.2 applies.

7.10.3 ISO/IEC 17025:2017, 7.10.3 applies.

7.11 Control of data information management

7.11.1 ISO/IEC 17025:2017, 7.11.1 applies.

7.11.2 ISO/IEC 17025:2017, 7.11.2 applies.

7.11.3 ISO/IEC 17025:2017, 7.11.3 applies.

NOTE See 7.1.1.2, 7.5.3, and 7.8.1.2.1.

7.11.4 ISO/IEC 17025:2017, 7.11.4 applies.

7.11.5 ISO/IEC 17025:2017, 7.11.5 applies.

7.11.6 ISO/IEC 17025:2017, 7.11.6 applies.

7.11.7 ISO/IEC 17025:2017, 7.11 applies with the following additions.

For all conformance testing and validations, the laboratory shall ensure that any file containing past results or past test programs on the IUT is isolated from the current test programs and test or validation results.

8 Management system requirements

8.1 Options

8.1.1 General

ISO/IEC 17025:2017, 8.1.1 applies.

NOTE See Annex B for more information.

8.1.2 Option A

ISO/IEC 17025:2017, 8.1.2 applies.

8.1.3 Option B

ISO/IEC 17025:2017, 8.1.3 applies.

8.2 Management system documentation (option A)

8.2.1 ISO/IEC 17025:2017, 8.2.1 applies.

8.2.1.1 ISO/IEC 17025:2017, 8.2.1 applies with the following additions.

The management system shall include policies and procedures to ensure the protection of proprietary information. The policies and procedures 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.

8.2.2 ISO/IEC 17025:2017, 8.2.2 applies.

8.2.3 ISO/IEC 17025:2017, 8.2.3 applies.

8.2.3.1 ISO/IEC 17025:2017, 8.2.3 applies with the following additions.

The reference documents listed in Clause 2 and the annex associated with the specific test methods shall always be available to all appropriate personnel.

8.2.4 ISO/IEC 17025:2017, 8.2.4 applies.

8.2.5 ISO/IEC 17025:2017, 8.2.5 applies.

8.2.6 ISO/IEC 17025:2017, 8.2 applies with the following additions.

The reference documents, standards and publications listed in Clause 2, Annex C and the Bibliography shall be available for use by laboratory staff developing and maintaining the management system and conducting testing.

8.2.7 ISO/IEC 17025:2017, 8.2 applies with the following additions.

The laboratory shall have written and implemented procedures for testing.

8.3 Control of management system documents (option A)

8.3.1 ISO/IEC 17025:2017, 8.3.1 applies.

8.3.2 ISO/IEC 17025:2017, 8.3.2 applies.

8.4 Control of records (option A)

8.4.1 ISO/IEC 17025:2017, 8.4.1 applies.

8.4.1.1 ISO/IEC 17025:2017, 8.4.1 applies with the following additions.

The laboratory shall maintain a functional record-keeping system for each customer. Records shall be readily accessible and complete. Digital media shall be logged and properly marked. They shall be properly and securely backed-up, and disposed of once the retention period has been exceeded. Entries in paper-based laboratory notebooks shall be dated and signed or initialled.

8.4.2 ISO/IEC 17025:2017, 8.4.2 applies.

8.4.2.1 ISO/IEC 17025:2017, 8.4.2 applies with the following additions.

Software and data protected by nondisclosure agreements or classified as confidential shall be stored according to the vendor and/or government requirements and commensurate with the data sensitivity, and access shall be granted only to the authorized personnel. An access log file shall be maintained.

8.4.3 ISO/IEC 17025:2017, 8.4 applies with the following additions.

Records of all management system activities including training, internal audits, and management reviews shall be securely saved for future reviews. The integrity of electronic documents shall be assured by means commensurate with the data sensitivity. Documents in hard copy form shall be marked and stored in a secure location and, if necessary, a file logging any access, change, or addition shall be maintained to preserve a document's integrity and prevent unauthorized changes.