EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME

Version 1.1, October 2023

DOCUMENT HISTORY

Date	Version	Modification	Author's comments
June 2023	0.9	Creation	Version submitted to the ECCG
August 2023	1.0	Addition of a document history section with a link to the SOG-IS document the state-of-the-art document is based on, where applicable Rephrasing of subcontracting and non compliance conditions Addition of cryptography in Annex	Based on comments received
October 2023	1.1		Approved for publication on 20/10/2023 by the ECCG and the European Commission

CONTENTS

1 INTRODUCTION

This state-of-the-art document supporting the EUCC scheme provides requirements related to the accreditation of ITSEFs, that shall establish they are technically competent for their related tasks according to the Common Criteria in conjunction with the Common Evaluation Methodology.

This technical competence shall be assessed through the accreditation of the ITSEFs by a National Accreditation Body (NAB) as per ISO/IEC 17025:2017, the standard selected for the accreditation of ITSEFs by the EUCC scheme,.

As ISO/IEC 17025:2017applies to a very general and wide range of testing activities, this document provides necessary interpretations of the standard and of EUCC specific requirements for ITSEFs whose conformity is to be assessed during their accreditation.

This document shall be used by National Accreditation Bodies to support their compliance assessments.

2 NORMATIVE REFERENCES

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

EUCC, the Commission Implementing Regulation (EU) XX/XXXX on establishing the Common Criteria - based cybersecurity certification scheme

ISO/IEC 15408:2022 - Information technology - Security techniques - Evaluation criteria for IT security, further referenced as Common Criteria for Information Technology Security, or CC

ISO/IEC 18045:2022 - Information technology - Security techniques - Methodology for IT security evaluation, further referenced as Common Evaluation Methodology, or CEM

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

ISO/IEC 17065:2012 - Conformity assessment - Requirements for bodies certifying products, processes and services

ISO/IEC 19896-1:2018 - IT security techniques - Competence requirements for information security testers and evaluators - Part 1: Introduction, concepts and general requirements

ISO/IEC 19896-3:2018 - IT security techniques - Competence requirements for information security testers and evaluators - Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

ISO/IEC TS 23532-1:2021 - Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 1 Testing and evaluation for ISO/IEC 15408

3 ACRONYMS AND DEFINITIONS

3.1 ACROMNYMS

CAB	Conformity Assessment Body
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation.
CEM	Common Methodology for Information Technology Security Evaluation
CSA	Cybersecurity Act
EAL	Evaluation Assurance Level
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation Technical Report
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and communications technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NAB	National Accreditation Body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008;
NCCA	National Cybersecurity Certification Authority
SMEs	Small and Medium Enterprises
SOG-IS	Senior Officials Group Information Systems Security
TOE	Target of evaluation
TS	Technical Specification

3.2 DEFINITIONS

The definitions used under Article 2 of Regulation (EU) 2019/881 (hereinafter referred to as CSA) and under Article 2 of the Commission Implementing Regulation (EU) XX/XXXX on establishing the Common Criteria -based cybersecurity certification scheme (EUCC) - hereinafter the Regulation is referred to as IA EUCC - apply to this document, in particular the following definitions

Conformity Assessment Body
“Conformity assessment body (CAB)” means a conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008: ‘conformity assessment body’ shall mean a body that performs conformity assessment activities including calibration, testing, certification and inspection;

Certification Body
“Certification Body (CB)” means and entity of a CAB described under Article 2 (13) of Regulation (EC) No 765/2008 performing certification activities or activities of the national cybersecurity certification authority (NCCA) related to the issuance of European cybersecurity certificates referred to in Article 56(5)(a) CSA (see Article 2 (4) EUCC)).

Under provisions of Art. 58(4), a NCCA responsible for, or issuing certifications is considered to be a CB when it is involved in certification under assurance level ‘high’. The CB can therefore be a private entity or public body under EUCC.

Evaluation
“Evaluation” means an assessment of the applicant’s claimed Security Funtional Requirements associated with the assessed ICT product or a Protection Profile by the use of Security Assurance Requirements as referred to in the EUCC, in order to determine whether the claims made are justified. This implies under ISO/IEC the combination of the selection and determination functions of conformity assessment activities (ISO/IEC 17065:2012).

Evaluation tasks can include activities such as design and documentation review, sampling, testing, inspection and audit (ISO/IEC 17065:2012).

In the context of the EUCC, evaluation can be defined as assessment of an ICT product or a protection profile against the security evaluation criteria and security evaluation methods to determine whether or not the claims made are justified (CC Part 1).

Evaluation activities are performed by an ITSEF, while the Certification Body is focusing on the performance of review, decision making related to issuance, extension and reduction of the scope of certifications, suspension and withdrawal of a certificate, attestation, complaint handling and monitoring of certain compliance obligations of holders of a certificate.

ITSEF
"ITSEF" means an Information Technology Security Evaluation Facility, which is an entity of a CAB described under Article 2(13) Regulation (EC) 765/2008 performing calibration, testing or sampling activities associated with subsequent calibration or testing and related to necessary inspection activities. Third-party CAB that performs one or more of the following activities: - calibration - testing - sampling, associated with subsequent calibration or testing (ISO/IEC 17025:2017).

In the context of the EUCC, an ITSEF carries out selection and determination functions as a part of conformity assessment evaluation activities.

The ITSEF can be a body that together with the CB forms one legal entity. It can also be a separate legal entity that is subcontracted by a CB to perform the activities described in the definition.

Where requirements are defined in the EUCC for an ITSEF, they shall apply to both the body that together with the CB forms one legal entity and as well to the ITSEF that is a subcontracted legal entity.

In the context of the EUCC, the ITSEF is required to meet the requirements of standard ISO/IEC 17025:2017 and the CB needs to meet the requirements of standard ISO/IEC 17065:2012.

Evaluator
ITSEF personnel performing evaluation activities.

4 APPLICABILITY OF INTERNATIONAL STANDARDS TO THE ACCREDITATION OF ITSEFS

The CSA prescribes the obligation that schemes refer to international, European, or national standards that are to be applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme.

In this respect, it shall be taken into account that the following standards apply to the accreditation of ITSEFs:

- ISO/IEC 17025:2017 - General requirements for the competence of testing and calibration laboratories: meeting this standard is mandatory for ITSEF accreditation.
- ISO/IEC TS 23532-1:2021 - Information security, cybersecurity and privacy protection - Requirements for the competence of IT security testing and evaluation laboratories - Part 1 Testing and evaluation for ISO/IEC 15408: this standard that provides an interpretation of ISO/IEC 17025:2017 shall also apply for ITSEF accreditation.

Note: ISO/IEC TS 23532-1:2021 references to "scheme owner(s)" should be understood in this context as referring to the related accredited and, if applicable authorized CB and NCCA.

- Additions to some ISO/IEC TS 23532-1:2021 requirements are defined in this document, that are also mandatory for ITSEF accreditation.
- Additional competence requirements are defined in this document, based on ISO/IEC 19896:2018 - IT security techniques - Competence requirements for information security testers and evaluators, both parts 1 and 3, that provide the definition of elements of competence, competency levels and the measurement of the elements of competence, that are to be applied by ITSEFs.

Note: ISO/IEC 19896:2018 provides some informative annexes that provide guidance on the competence requirements for information security evaluators. Some of these annexes are identified as mandatory in this document as detailed in the chapter “Accreditation requirements”.

EUCC scheme requirements that apply to ITSEFs are also included in this document, so that their compliance can be assessed during the accreditation process.

5 SCOPE OF ITSEF ACCREDITATION

The scope of the ISO/IEC 17025:2017 accreditation for EUCC ITSEFs shall be based on the following standards:

- the CC
- the CEM

These standards define security functional and assurance components and corresponding evaluation activities. Such components and activities are packaged in the so-called Evaluation Assurance Levels.

The scope of the accreditation shall include the evaluation activities from the CC in which the ITSEF has proven technical competence, named and grouped by the rules of the referred standards.

Only the information described as “Type of test and test parameter” shall vary depending on the scope of accreditation that is requested and granted.

The requirements for accreditation do not deal directly with different types of technology being tested but focus on an assessment of the specific competences that the ITSEF needs to define and demonstrate in accordance with the applicable standards and the requirements defined under Annex I CSA.

An example of the scope of accreditation may be:

- Testing field:
  - ICT Cybersecurity Evaluation
- Test object or product:
  - Information and Communication Technology Products
- Type of test and Test parameter:
  - IT security evaluation up to EAL3 augmented with ALC_FLR.2
- Reference to requirements and method:
  - EUCC Implementing Act (to be published).
  - CC
  - CEM

6 ACCREDITATION REQUIREMENTS

The EUCC scheme ITSEF accreditation requirements that shall apply are the following:

1. The requirements for the competence of testing and calibration laboratories defined in ISO/IEC 17025:2017 complemented by the requirements defined in ISO/IEC TS 23532-1:2021.
2. Those requirements that are to be met by conformity assessment bodies indicated in the Annex of the CSA, to the extent applicable to the ITSEF activities. These are provided in section “General accreditation requirements from the [CSA]”.
3. The requirements specified in this document, as provided in section “Specific accreditation requirements”, based on those requirements applicable to ITSEFs indicated in the EUCC - except those related to authorization.

6.1 GENERAL ACCREDITATION REQUIREMENTS FROM THE CSA

Conformity assessment bodies that wish to be accredited shall meet the requirements indicated in the Annex of the CSA, included in the following table.

For information purposes, links to related requirements from ISO/IEC 17025:2017 that may support compliance of the indicated CSA requirements are provided in the second column of the table.

Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES"		Supporting ISO/IEC 17025:2017 requirement
1.	A conformity assessment body shall be established under national law and shall have legal personality.	ISO/IEC 17025:2017, 5.1
2.	A conformity assessment body shall be a third-party body that is independent of the organisation or the ICT products, ICT services or ICT processes that it assesses.	ISO/IEC 17025:2017, 4.1
3.	A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services or ICT processes which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated.	ISO/IEC 17025:2017, 4.1
4.	The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes.	ISO/IEC 17025:2017, 4.1 Impartiality
5.	The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of the ICT products, ICT services or ICT processes which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services.	ISO/IEC 17025:2017, 4.1 Impartiality
6.	If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented.	
7.	Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.	ISO/IEC 17025:2017, 4.1 ISO/IEC 17025:2017, 4.2 ISO/IEC 17025:2017, 6.6.2 Impartiality Confidentiality

Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES"		Supporting ISO/IEC 17025:2017 requirement
8.	Conformity assessment bodies and their staff shall carry out conformity assessment activities with the highest degree of professional integrity and the requested technical competence in the specific field, and shall be free from all pressures and inducements which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities.	ISO/IEC 17025:2017, 4.1 Impartiality ISO/IEC 17025:2017, 6.2.3 Competence
9.	A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.	ISO/IEC 17025:2017, 6.6
10.	At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services or ICT processes, a conformity assessment body shall have at its disposal the necessary:	ISO/IEC 17025:2017, 6.2 ISO/IEC 17025:2017, 7.2
(a)	staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;	
(b)	descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities;	
(c)	procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service or ICT process in question and the mass or serial nature of the production process.	
11.	A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.	ISO/IEC 17025:2017, 6.3 ISO/IEC 17025:2017, 6.4
12.	The persons responsible for carrying out conformity assessment activities shall have the following:	ISO/IEC 17025:2017, 6.2
(a)	sound technical and vocational training covering all conformity assessment activities;	Competence

Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES"	Supporting ISO/IEC 17025:2017 requirement
(b) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments;	
(c) appropriate knowledge and understanding of the applicable requirements and testing standards;	
(d) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out.	
13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed.	ISO/IEC 17025:2017, 4.1 Impartiality
14. The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments.	ISO/IEC 17025:2017, 4.1
15. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with its national law, or the Member State itself is directly responsible for the conformity assessment.	
16. The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.	ISO/IEC 17025:2017 4.2 ISO/IEC TS 23532-1:2021 Confidentiality
17. With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for certification or who is considering whether to apply for certification.	
18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.	
19. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes.	

Requirement from CSA Annex "REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES"	Supporting ISO/IEC 17025:2017 requirement
20. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing.	

6.2 SPECIFIC ACCREDITATION REQUIREMENTS

In addition to the requirements included in ISO/IEC 17025:2017 and ISO/IEC TS 23532-1:2021, the following requirements apply to the accreditation of an EUCC ITSEF.

6.2.1 Impartiality

ISO/IEC 17025:2017, "4.1 Impartiality"

Generic training (from a public list of pre-established training) with safeguards on trainings carried out in-house for a single company (generic training with adaptation deletion/addition of a part, no case studies from the party, no workshop demonstration) shall not be considered consultancy.

Bespoke training on the party's specific activities is not allowed.

6.2.2 Confidentiality

EUCC, "24.2 SECURITY OF INFORMATION"
ISO/IEC 17025:2017, "4.2 Confidentiality"

Additional requirement to ISO/IEC TS 23532-1:2021, 4.2.6

The exclusions indicated by ISO/IEC TS 23532-1:2021 4.2.6 need to be noted and justified in the ETR to the responsible CB. If the responsible CB considers that access to this information is relevant to perform the certification decision, it can be a cause for rejecting the requested certificate.

The ETR for composition needs to include all information necessary for the composition, it has to be technically relevant, while taking into account the confidentiality of sensitive information.

Additional requirement to ISO/IEC TS 23532-1:2021, 4.2.8

The scope of the policies, procedures and security manual to ensure the protection of proprietary information shall also cover and protect the following:

a) Handling of personal data, where applicable.
b) Information necessary for
   - the effective implementation of the EUCC scheme, in particular for the purpose of accreditation assessments,
   - effective collaboration between the involved authorities and bodies,
   - the handling of publicly unknown and subsequently detected vulnerabilities in the TOE in the process of, or after certification, and
   - the handling of complaints.
c) The case of subcontracting, and in the situation where the ITSEF uses other facilities (e.g., third parties independent of both the ITSEF and the company(ies) developing and producing the TOE), appropriate security measures shall be applied to protect the vendor's information and samples as well as the relevant the know-how and evaluation and testing approaches and their results of the ITSEF.
d) Protection under scenarios of unavailability or lack of accessibility of the ITSEF main location, remote evaluation activities, both from home-office of the evaluators, or from the manufacturer site.

e) The ITSEF should ensure that information that is required by a user or users (i.e. those accessing the evaluation information) for a short period, is retrievable when this period expires.
f) The ITSEF shall implement mechanisms that allow setting a fixed duration for users' access to confidential information.

Confidential information that requires temporary access to be given to a set of users to perform a specific task such as assessments from NABs should not be permanently handed to the possession such temporary users. They should only have access for the duration of the activity.

g) Confidential information about an evaluation activity should be restricted to the ITSEF staff involved in the specific evaluation activity.

In particular, the policies, procedures and security manual to ensure the protection of proprietary information shall also cover and include the following measures:

a) The information system shall include tools that provide encryption functionalities for non-public Information at rest. These tools should be referenced by an ENISA or a National guidance document.
   Encryption tools that are deployed for security of information are expected to be in compliance with, by order of precedence:
   – EU and national regulation regarding the protection of sensitive information,
   – recommendations, guidance and opinions from the competent cybersecurity authorities of the member state,
   – recommendations from the ECCG.
b) Secure electronic storage and communication must be achieved for non-public Information through accepted and recognised cryptographic methods and algorithms. The ITSEF shall refer to and comply with ENISA or National cryptography guidelines for further guidance.
c) ITSEF staff shall be trained on information handling and sign agreements of compliance with information security obligations to maintain data secrecy. The ITSEF shall keep these agreements as per Retention of records.
   Every staff member shall sign an NDA before he/she is granted access to non-public information. In governmental organizations where there are binding legal regulations on information secrecy, these rules shall be leading, unless they interfere with EU law.
   The ITSEF shall maintain a updated information security workshop schedule for staff involved in the EUCC scheme process. The workshop shall be performed on a regular basis and include updates on relevant regulatory changes.

Evaluation contracts between ITSEFs and their customers shall identify which parties will have access to the evaluation evidence and findings that are part of the certification process and that have for the purpose of certification and certification maintenance of the ICT product and compliance, a need-to-know right, subject to accreditation assessments and/or other scheme defined processes and procedures. The CB, the NAB where necessary for the purpose of accreditation, and the NCCA where necessary for the purpose of it's monitoring and supervision tasks, shall be informed about these contract obligations.

6.2.3 Competence

EUCC, "6. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB"
ISO/IEC 17025:2017, "6.2 Personnel"

The ITSEF, their evaluators and, if applicable, the relevant staff of their subcontracted partiess shall be required to have the necessary expertise and experience in performing the specific testing activities to determine the product's resistance against specific attacks (penetration testing).

The ITSEF shall define and operate a competence management system for the evaluators where:

- The elements of competence, competency levels and the measurement of the elements of competence are drawn from ISO/IEC 19896-1:2018, and if they differ, they shall be commensurate with the objectives that are defined and at least be equivalent to the elements defined by ISO/IEC 19896-1:2018. The ITSEF needs to demonstrate this.
- The knowledge, skills, experience and education, and the applicable requirements for the evaluators are drawn from ISO/IEC 19896-3:2018, and if they differ, they shall be commensurate with the objectives and be

at least equivalent to the requirements defined by ISO/IEC 19896-3:2018. The ITSEF needs to demonstrate this.

- The knowledge required for evaluating security assurance requirement classes is specified based on Annex B of ISO/IEC 19896-3:2018.
- The knowledge required for evaluating security functional requirement classes is specified based on Annex C of ISO/IEC 19896-3:2018.
- The knowledge required for evaluating specific technologies and exercising different evaluation technique types are to be specified by the ITSEF using the classification provided in Annex.
  The ITSEF may use other classification criteria, as long as it can be mapped to the one provided in Annex. Such mapping, and the supporting rationale, shall be made available to the CB the ITSEF is subcontracted with, the NABs and NCCA.

6.2.4 Facilities

EUCC, "6. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB"
ISO/IEC 17025:2017, "6.3 Facilities and environmental conditions"

Additional requirement to ISO/IEC TS 23532-1:2021, 6.3.1.1

Network isolation must ensure the integrity of the test results and their confidentiality.

6.2.5 Subcontracting

EUCC, "7. NOTIFICATION AND AUTHORISATION OF CABS, FUNCTIONING OF CABS AND SUBCONTRACTORS"
ISO/IEC 17025:2017, "6.6 Externally provided products and services"

The ITSEF shall operate according to defined procedures ensuring that:

- The use of a subcontracted third-party facility is outlined in the evaluation plan, approved by the manufacturer or provider and by the CB and compliant with the obligations under the CSA, Annex 1 of the CSA and the EUCC while the ITSEF remains responsible for the work done. The sub-contacted third -party shall be subject to the accreditation procedure for the subcontracted tasks it is performing;
- If the ITSEF uses equipment at a third-party facility as specified in the sub-contracting, the evaluator shall be present and instruct the equipment operating personnel. To instruct the operating personnel, evaluators shall have the required knowledge of the subcontract with the third-party, the TOE, the equipment, and the purpose and scope of the evaluation.

6.2.6 Non-compliance

EUCC, "13. RULES RELATED TO NON-COMPLIANCE"
The ITSEF shall support the CB's, for which it performed evaluation activities, in their handling of non-compliances in the conditions under which the evaluation of the certification takes place, by defining and operating a process where:

- They identify within the scope of their tasks potentially impacted certified ICT products, from those TOEs evaluated by the ITSEF that contributed to the certification of the ICT product.
- They perform where deemed necessary by the CB, or at the discretion of the NCCA, a series of re-evaluation tasks on one or more certified ICT products.
- If the ITSEF that performed evaluation activities on behalf of a certified product, proves to be non-compliant, the NCCA guiding the non-compliance with the responsible CB may appoint an other supporting ITSEF to perform certain evaluation activities.

6.2.7 Retention of records

EUCC, "15. RETENTION OF RECORDS BY A CAB"
ISO/IEC 17025:2017, "7.5 Technical records", "8.4 Control of records"

The record system shall include all records and other related documents produced in connection with each evaluation; the recording shall be updated, accurate and complete to enable the course of each evaluation to be traced and reproduceable.

All records shall be securely and accessibly stored for a period of at least five (5) years after the final date of the certificate validity, with the exception of running investigations related non-compliance and complaint handling and their respective legal remedy procedures.

All records related to the handling of non-compliances and/or complaints not related to the evaluation shall be kept for a period of at least five (5) years after the non-compliance and/or complaint was handled and all related (legal) procedures are closed.

In case a different expiration date of the certificate has been attributed in accordance with the conditions of Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES of the EUCC, it shall be taken into account for the new calculation of the retention period of the records, with the same rules in this section.

New or revised information related to the activities described under Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES of the EUCC shall be added to the previous records for the evaluation.

6.2.8 Ensuring the validity of results

ISO/IEC 17025:2017, “7.7.2 Monitoring of laboratory performance”

This clause requires that a laboratory shall monitor its performance by comparison with the results of other laboratories. In particular, the ITSEF needs to demonstrate that it is having a planning and where already the benchmarking is performed a demonstrated proof of participation and result report.

Further guidance is needed how to apply this requirement on CC laboratories, also to ensure a level playing field within Europe.

6.2.9 Management System documentation

ISO/IEC 17025:2017, “8.2 Management system documentation (Option A)”

Additional requirement to ISO/IEC TS 23532-1:2021, 8.2.8

Procedures for evaluation should be written with a level of detail that would allow a technical competent evaluator to perform the evaluation without further guidance.

6.2.10 Quality process

EUCC, “11. RULES FOR MONITORING COMPLIANCE”
ISO/IEC 17025:2017, “8.8 Internal audits”

The management process of the ITSEF shall explicitly ensure conformity with all the applicable requirements and obligations of the EUCC, including the requirements associated to handle complaints.

6.2.11 Composite evaluations

EUCC, “8. SPECIFIC EVALUATION CRITERIA AND METHODS”

The ITSEF shall operate according to defined procedures that ensure that, where an ICT product undergoes a composite product evaluation, sensitive information that is reused from the initial evaluation is provided to the ITSEF performing the composite evaluation. This information sharing shall take place in the form of an evaluation technical report (ETR) for composition, based on the template provided by ENISA.

The information sharing in the case of composite evaluation must take place in full cooperation between the CBs, i.e. the CB that has certified the base component and the one handling the composite evaluation.

Besides the relevant documentation, which should be exchanged there must exist a communication channel between all involved parties to clarify technical problems. All parties/bodies, esp. the ITSEF which is responsible for the composition ETR must support this approach.

6.2.12 Monitoring compliance

EUCC, “11. RULES FOR MONITORING COMPLIANCE”

Monitoring compliance of certified ICT products with the requirements of the European cybersecurity certificates: Manufacturers, developers and any other holders of a cybersecurity certificate shall have procedures and processes in place that allow to demonstrate their continued compliance with the specified cybersecurity requirements under their certification.

The CB must carry out an assessment of the criticality of the reported irregularities with the support of the ITSEF if necessary.

To support compliance monitoring, ITSEFs shall define a set of compliance monitoring processes that ensure that, for TOEs evaluated by the ITSEF:

- They carry out an active cybersecurity oriented technology watch, and keep themselves informed and continuously updated of the main discovered vulnerabilities and attack techniques relevant to their scope of assessment,
- They systematically carry out a search for publicly known vulnerabilities in connection with the products being assessed,
- They instantly report to their their CB any vulnerability they are aware of that affects the compliance of a certified ICT product with the certification requirements,
- They support the the CB, and upon request the NCCA, in the implementation of their compliance monitoring obligations and processes.

The ITSEF of a certified ICT product shall be involved by the NCCA in monitoring activities, where the NCCA deems it necessary.

The monitoring activity may under circumstances consist, among other things, in the re-assessment of the ICT product by the ITSEF upon request of the CB, accompanied - if necessary - by an audit subject to the monitoring activities (for example compliance of the complaints procedure, events of a security incident,…).

6.2.13 Patch management

EUCC, “12. CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES”
EUCC, “41. ANNEX 15: PATCH MANAGEMENT”

ITSEFs provides evaluation services related to ICT product certification that is including patch management that is upon request of the applicant included in the scope of certification. Patch management is associated to vulnerability handling, and which may also be used for the maintenance activities of certificates

The ITSEF shall provide such services based on defined procedures and methods that ensure their conformity with the requirements laid out for ITSEFs in Annex II Article II.4 of the EUCC Regulation.

ANNEX TECHNOLOGY AND EVALUATION

This annex provides a taxonomy of technology and evaluation technique types, with examples. This taxonomy should be used both for the management of the competence of the ITSEF and for its assessment by NABs.

A.1 TECHNOLOGY TYPES

A.1.1 Hardware and software architectures, OS and applicative security

Code	Description	Notes
S1	Hardware architectures	Includes CPU architectures
S2	Personal computer and server security	Includes general purpose operating systems
S3	Embedded systems, microkernels	Includes trusted enviroments, realtime operating systems
S4	Virtualization	
S5	Applicative security	
S6	Databases	
S7	Web technologies	

A.1.2 Network & Wireless

Code	Description	Notes
N1	Network protocols	
N2	Communication protocols	
N3	Low-level interfaces	Includes serial line buses
N4	Wireless	
N5	Hardware components protocols	Includes hardware roots of trust
N6	Phone and VoIP	
N7	Mobile networks	Includes 3/4/5G
N8	Filtering	
N9	Intrusion detection	

A.1.3 Secure microcontrollers and smartcards

Code	Description	Notes
H1	Secure hardware components architectures	
H2	Hardware sensors, reactive technology	
H3	Platforms and applications security	Includes run-time systems, multiplatform interpreters/byte code execution environments

A.1.4 Cryptography

Code	Description	Notes
C1	State-of-the-art of Approved Cryptographic Mechanisms	

A.2 EVALUATION TECHNIQUE TYPES

The ITSEF is expected to indicate the reference to the definition of applied methods and the identification of tools used to exercise the evaluation techniques under assessment for accreditation.

Some references are included in the following tables, where alternative methods can be applied if proved equivalent by the ITSEF.

A.2.1 Source code review

Languages	Manual/automatic review	Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal)
Example: C/C++	Both	

A.2.2 Source code review

Object	Principle of the method	Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal)
Cryptographic algorithms and protocols	Conformity analysis and tests	ISO/IEC 18367:2016 Cryptographic algorithms and security mechanisms conformance testing
Random bit generators	Entropy analysis	ISO/IEC 20543:2019 Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
Cryptographic protocols	Security assessment	ISO/IEC 29128:2011 Verification of cryptographic protocols

A.2.3 Vulnerability analysis and penetration tests (generic)

Technologies embedded in the evaluated product	Mastered attack technique	Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal)
Fill-in using codes from Technology types. Example: S1, S2, N1	Bypass Code Injection Denial of service Direct attacks Exploit development Forensic analysis Generational fuzzing Generic vulnerability search Hooking attacks Memory dumps Meta characters, encoding & input validation Misuse Mutational fuzzing Overrun Protocol attacks Protocol fuzzing Public exploits application Race conditions Tampering	ISO/IEC 20004:2015 Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 OWASP Penetration Testing Methodologies

Technologies embedded in the evaluated product	Mastered attack technique	Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal)
	Web application security	

A.2.4 Vulnerability analysis and penetration tests (smartcards and similar devices)

Technologies embedded in the evaluated product	Mastered attack technique	Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal)
Fill-in using codes from Technology types. Example: H1, H2, H3	Non-invasive /side channel attacks (electric consumption, electromagnetic radiations, execution time) Semi-invasive simple attacks (light injection, electromagnetic injection, power/clock frequency glitch) Invasive attacks: components preparation and probing	

A.2.4 Vulnerability analysis and penetration tests (hardware devices with security boxes)

Technologies embedded in the evaluated product	Mastered attack technique	Reference to applied methods and/or tools (EUCC harmonized or ITSEF internal)
Fill-in using codes from Technology types. Example: H1, H2, H3	Identification of components on a PCB Debug interfaces manipulation (JTAG, UART) Security boxes tampering Disabling sensor networks Non-invasive /side channel attacks (electric consumption, electromagnetic radiations, execution time)	

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu