EUROPEAN
COMMISSION

Brussels, 31.1.2024
C(2024) 560 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 31.1.2024

laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

(Text with EEA relevance)

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 31.1.2024

laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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) 526/2013 (Cybersecurity Act)[1], and in particular Article 49(7) thereof,

Whereas:

(1) This Regulation specifies the roles, rules and obligations, as well as the structure of the European Common Criteria-based cybersecurity certification scheme (EUCC) in accordance with the European cybersecurity certification framework set out in Regulation (EU) 2019/881. The EUCC builds on the Mutual Recognition Agreement ('MRA') of Information Technology Security Certificates of the Senior Officials Group Information Systems Security[2] ('SOG-IS') using the Common Criteria, including the group's procedures and documents.

(2) The scheme should be based on established international standards. Common Criteria is an international standard for information security evaluation published, for instance, as ISO/IEC 15408 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. It is based on third party evaluation and envisages seven Evaluation Assurance Levels ('EAL'). The Common Criteria is accompanied by the Common Evaluation Methodology, published, for instance, as ISO/IEC 18045 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation. Specifications and documents that apply the provisions of this Regulation may relate to a publicly available standard that mirrors the standard used in certification under this Regulation, such as Common Criteria for Information Technology Security Evaluation and Common Methodology for Information Technology Security Evaluation.

(3) The EUCC uses the Common Criteria's vulnerability assessment family (AVA_VAN), components 1 to 5. The five components provide all the main determinants and

[1] OJ L 151, 7.6.2019, p. 15.

[2] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0 of January 2010, available on sogis.eu, approved by Senior Officials Group Information Systems Security of the European Commission in response to point 3 of Council Recommendation 95/144/EC of 7 April 1995 on common information technology security evaluation criteria (OJ L 93, 26.4.1995, p. 27–28).

dependencies for analysing vulnerabilities of ICT products. As the components correspond to the assurance levels in this Regulation, they allow for a well-informed choice of assurance, based on the evaluations carried out of the security requirements and the risk associated with the intended use of the ICT product. The applicant for an EUCC certificate should provide the documentation related to the intended use of the ICT product and the analysis of the levels of risks associated with such usage in order to enable the conformity assessment body to evaluate the suitability of the assurance level selected. Where the evaluation and certification activities are performed by the same conformity assessment body, the applicant should submit the requested information only once.

(4) A technical domain is a reference framework that covers a group of ICT products that have specific and similar security functionality that mitigates attacks where the characteristics are common to a given assurance level. A technical domain describes in state-of-the-art documents the specific security requirements as well as additional evaluation methods, techniques and tools that apply to the certification of ICT products that are covered by this technical domain. A technical domain therefore also fosters harmonisation of the evaluation of covered ICT products. Two technical domains are currently widely used for certification at levels AVA_VAN.4 and AVA_VAN.5. The first technical domain is the 'Smart cards and similar devices' technical domain, where significant portions of the required security functionality depend on specific, tailored and often separable hardware elements (e.g. smart card hardware, integrated circuits, smart card composite products, Trusted Platform Modules as used in Trusted Computing, or digital tachograph cards). The second technical domain is 'Hardware devices with security boxes', where significant portions of the required security functionality depend upon a hardware physical envelope (referred to as a 'Security Box') that is designed to resist direct attacks, e.g. payment terminals, tachograph vehicle units, smart meters, access control terminals and Hardware Security Modules).

(5) When applying for certification, the applicant should relate its reasoning for selecting an assurance level to the objectives laid down in Article 51 of Regulation (EU) 2019/881, and to the selection of components from the catalogue of security functional requirements and security assurance requirements contained in Common Criteria. Certification bodies should assess the appropriateness of the chosen assurance level and ensure that the chosen level is commensurate with the level of risk associated with the intended use of the ICT product.

(6) Under the Common Criteria, certification is carried out against a security target which encompasses a definition of the ICT product's security problem as well as the security objectives that address the security problem. The security problem provides details on the intended use of the ICT product and the risks associated with such use. A select set of security requirements responds to both the security problem and security objectives of an ICT product.

(7) Protection profiles are an effective means to predetermine the common criteria that are applicable to a given category of ICT products and therefore also an essential element in the certification process of ICT products covered by the protection profile. A protection profile is used to assess future security targets that fall under the given ICT product category addressed by that protection profile. They further streamline and enhance the efficiency of the ICT product certification process and help users to specify an ICT product's functionality correctly and effectively. Protection profiles

should thus be considered as integral part of the ICT process leading to the certification of ICT products.

(8) In order to enable their role in the ICT process supporting the development and delivery of a certified ICT product, protection profiles themselves should be able to be certified independently from a certification of the specific ICT product that falls under the respective protection profile. It is therefore essential to apply at least the same level of scrutiny to protection profiles as to security targets in order to ensure a high level of cybersecurity. Protection profiles should be evaluated and certified separately from the related ICT product and solely by applying the Common Criteria's and Common Evaluation Methodology's assurance class for protection profiles (APE) and, where applicable, for configurations of protection profiles (ACE). Due to their important and sensitive role as a benchmark in the certification of ICT products, they should be certified only by public bodies or by a certification body that has received prior approval for the specific protection profile by the national cybersecurity certification authority. Due to their fundamental role for certification at assurance level 'high', in particular outside of technical domains, protection profiles should be developed as state-of-the-art documents which should be endorsed by the European Cybersecurity Certification Group.

(9) Certified protection profiles should be included in the EUCC conformity and compliance monitoring by the national cybersecurity certification authorities. Where methodology, tools and skills applied to approaches for the evaluation of ICT products are available for specific certified protection profiles, technical domains may be based on those specific protection profiles.

(10) To achieve a high level of trust and assurance in certified ICT products, self-assessment should not be permitted under this Regulation. Only third-party conformity assessment by ITSEF and certification bodies should be allowed.

(11) The SOG-IS community provided joint interpretations and approaches for the application of the Common Criteria and the Common Evaluation Methodology in certification, in particular for the assurance level 'high' pursued by the technical domains "Smart cards and similar devices' and "Hardware devices with security boxes". The reuse of such supporting documents in the EUCC scheme ensures a smooth transition from the nationally implemented SOG-IS schemes to the harmonised EUCC scheme. Therefore, harmonised evaluation methodologies of general relevance for all certification activities should be included in this Regulation. In addition, the Commission should be able to request the European Cybersecurity Certification Group to adopt an opinion endorsing and recommending the application of evaluation methodologies specified in state-of-the-art documents for the certification of the ICT product or protection profile under the EUCC scheme. This Regulation therefore lists in Annex I the state-of-the-art documents for the evaluation activities carried out by conformity assessment bodies. The European Cybersecurity Certification Group should endorse and maintain state-of-the-art documents. State-of-the-art documents should be used in certification. Only in exceptional and duly justified cases, a conformity assessment body may not use them subject to specific conditions, in particular the approval by the national cybersecurity certification authority.

(12) Certification of ICT products at AVA_VAN level 4 or 5 should only be possible under specific conditions and where a specific evaluation methodology is available. The specific evaluation methodology may be enshrined in state-of-the-art documents

relevant for the technical domain, or in specific protection profiles adopted as state-of-the-art document that are relevant for the product category concerned. Only in exceptional and duly justified cases, certification at these assurance levels should be possible, subject to specific conditions, in particular approval by the national cybersecurity certification authority, including of the applicable evaluation methodology. Such exceptional and duly justified cases may exist where Union or national legislation require certification of an ICT product at AVA_VAN level 4 or 5. Similarly, in exceptional and duly justified cases, protection profiles may be certified without applying the relevant state-of-the-art documents, subject to specific conditions, in particular the approval by the national cybersecurity certification authority, including of the applicable evaluation methodology.

(13) The marks and labels used under EUCC aim at visibly demonstrating the trustworthiness of the certified ICT product to users and enable them to make an informed choice when purchasing ICT products. The use of marks and labels should also be subject to the rules and conditions set out in ISO/IEC 17065 and, where applicable, ISO/IEC 17030 with the applicable guidance.

(14) Certification bodies should decide on the duration of the validity of certificates taking into account the life cycle of the ICT product concerned. The duration of the validity should not exceed 5 years. National cybersecurity certification authorities should work on harmonising duration validity in the Union.

(15) Where the scope of an existing EUCC certificate is reduced, the certificate shall be withdrawn and a new certificate with the new scope should be issued to ensure that users are clearly informed about the current scope and assurance level of the certificate of a given ICT product.

(16) The certification of protection profiles differs from that of ICT products as it concerns an ICT process. As a protection profile covers a category of ICT products, its evaluation and certification cannot be done on the basis of a single ICT product. As a protection profile unifies the general security requirements regarding a category of ICT products and independent of the ICT product's manifestation by its vendor, the period of validity of an EUCC certificate for a protection profile should, in principle, cover 5 years as a minimum and may be extended to the lifetime of the protection profile.

(17) A conformity assessment body is defined as a body that performs conformity assessment activities including calibration, testing, certification and inspection. In order to ensure a high quality of services, this Regulation specifies that testing activities on the one hand, and certification and inspection activities on the other hand, should be carried out by entities operating independently from each other, namely Information Technology Security Evaluation Facilities ('ITSEF'), and certification bodies, respectively. Both types of conformity assessment bodies should be accredited and, in certain situations, authorised.

(18) A certification body should be accredited in accordance with standard ISO/IEC 17065 by the national accreditation body for assurance level 'substantial' and 'high'. In addition to the accreditation in accordance with Regulation (EU) 2019/881 in conjunction with Regulation (EC) No 765/2008, conformity assessment bodies should meet specific requirements in order to guarantee their technical competence for the evaluation of cybersecurity requirements under assurance level 'high' of the EUCC, which is confirmed by an 'authorisation'. To support the authorisation process,

relevant state-of-the-art documents should be developed, and be published by ENISA after endorsement by the European Cybersecurity Certification Group.

(19) The technical competence of an ITSEF should be assessed through the accreditation of the testing laboratory in accordance with ISO/IEC 17025 and complemented by ISO/IEC 23532-1 for the full set of evaluation activities that are relevant to the assurance level and specified in ISO/IEC 18045 in conjunction with ISO/IEC 15408. Both the certification body and the ITSEF should establish and maintain an appropriate competence management system for personnel that draws from ISO/IEC 19896-1 for the elements and levels of competence and for the appraisal of competence. For the level of knowledge, skills, experience and education, the applicable requirements for the evaluators should be drawn from ISO/IEC 19896-3. Equivalent provisions and measures dealing with deviations from such competence management systems should be demonstrated, in line with the system's objectives.

(20) In order to be authorised, the ITSEF should demonstrate its capability to determine the absence of known vulnerabilities, the correct and consistent implementation of state-of-the art security functionalities for the specific technology concerned and the targeted ICT product's resistance to skilled attackers. Additionally, for authorisations in the technical domain of 'Smart cards and similar devices', the ITSEF should also demonstrate the technical capabilities necessary for the evaluation activities and related tasks as defined in the 'Minimum ITSEF requirements for security evaluations of smart cards and similar devices'[3] supporting document under the Common Criteria. For authorisation in the technical domain 'Hardware devices with security boxes', the ITSEF should, in addition, demonstrate the minimum technical requirements necessary for carrying out evaluation activities and related tasks on hardware devices with security boxes' as recommended by the ECCG. In the context of the minimum requirements, the ITSEF should be capable of conducting the different types of attacks set out in 'Application of Attack Potential to Hardware Devices with Security Boxes' supporting document under the Common Criteria. Those capabilities encompass the evaluator's knowledge and skills and the equipment and evaluation methods needed to determine and assess the different types of attacks.

(21) The national cybersecurity certification authority should monitor the compliance of certification bodies, ITSEF and the holders of certificates with their obligations stemming from this Regulation and the Regulation (EU) 2019/881. National cybersecurity certification authority should use any appropriate sources of information to this end, including information received from certification process participants and own investigations.

(22) Certification bodies should cooperate with relevant market surveillance authorities and take into account any vulnerability information that could be relevant to ICT products for which they have issued certificates. Certification bodies should monitor the protection profiles they have certified to identify whether the security requirements set out for a category of ICT products continue to reflect the latest developments in the threat landscape.

(23) In support of the compliance monitoring, the national cybersecurity certification authorities should cooperate with the relevant market surveillance authorities in accordance with Article 58 of Regulation (EU) 2019/881 and Regulation

[3] Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices, version 2.1 of February 2020, available at sogis.eu.

(EU) 2019/1020 of the European Parliament and of the Council[4]. Economic operators in the Union are obliged to share information and cooperate with market surveillance authorities, pursuant to Article 4(3) of the Regulation 2019/1020.

(24) The certification bodies should monitor the compliance of the holders of a certificate and the conformity of all certificates issued under the EUCC. The monitoring should ensure that all evaluation reports provided by an ITSEF, and the conclusions taken therein as well as the evaluation criteria and methods are consistently and correctly applied across all certification activities.

(25) Where potential non-compliance issues are detected which affect a certified ICT product, it is important to ensure a proportional response. Certificates may therefore be suspended. Suspension should entail certain limitations regarding the promotion and use of the ICT product in question, but not affect the validity of the certificate. Suspension should be notified to the purchasers of the affected ICT products by the holder of the EU certificate, whilst the relevant market surveillance authorities should be notified by the relevant national cybersecurity certification authority. To inform the public, ENISA should publish information about a suspension on a dedicated website.

(26) The holder of an EUCC certificate should implement necessary vulnerability management procedures and ensure that those procedures are embedded in their organisation. When becoming aware of a potential vulnerability, the holder of the EUCC certificate should perform a vulnerability impact analysis. Where the vulnerability impact analysis confirms that the vulnerability can be exploited, the certificate holder should send a report of the assessment to the certification body which should in turn inform the national cybersecurity certification authority. The report should inform about the impact of the vulnerability, the necessary changes or remedial solutions that are required including possible broader implications of the vulnerability as well as remedial solutions for other products. Where necessary, the standard EN ISO/IEC 29147 should supplement the procedure for the vulnerability disclosure.

(27) For the purpose of certification, conformity assessment bodies and national cybersecurity certification authorities obtain confidential and sensitive data and business secrets, also relating to intellectual property or compliance monitoring that require adequate protection. They should therefore have the necessary technical competencies and knowledge and should establish systems in place for the protection of information. The requirements and conditions for the protection of information should be met for both accreditation and authorisation.

(28) ENISA should provide the list of certified protection profiles on its cybersecurity certification website and indicate their status, in accordance with Regulation (EU) 2019/881.

(29) This Regulation sets out conditions for mutual recognition agreements with third countries. Such mutual recognition agreements may be bi- or multilateral and should replace similar agreements currently in place. In view of facilitating a smooth transition to such mutual recognition agreements, Member States may continue existing cooperation arrangements with third countries for a limited period.

---

[4] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

(30) Certification bodies issuing EUCC certificates at assurance level 'high', as well as the relevant associated ITSEFs, should undergo peer assessments. The objective of peer assessments should be to determine the continued compliance of a peer-assessed certification body's constitution and procedures with the requirements of the EUCC scheme. Peer assessments are different from peer reviews among national cybersecurity certification authorities, as provided for in Article 59 of Regulation (EU) 2019/881. Peer assessments should ascertain that certification bodies work in a harmonised way and produce the same quality of certificates and they should identify any potential strength or weakness in the performance of certification bodies, also in view of sharing best practices. As there are different types of certification bodies, different types of peer assessment should be allowed. In more complex cases, such as certification bodies issuing certificates on different AVA_VAN levels, different types of peer assessment can be used, provided that all the requirements are met.

(31) The European Cybersecurity Certification Group should play an important role in the maintenance of the scheme. It should, inter alia, be carried out through cooperation with the private sector, the creation of specialised subgroups and relevant preparatory work and assistance requested by the Commission. The European Cybersecurity Certification Group plays an important role in the endorsement of state-of-the-art documents. In the endorsement and adoption of state-of-the-art documents, due account should be taken of the elements referred to in Article 54(1) letter c) of Regulation (EU) 2019/881. Technical domains and state-of-the art documents should be published in Annex I of this Regulation. Protection profiles that have been adopted as state-of-the-art documents should be published in Annex II. In order to ensure that these Annexes are dynamic, the Commission may amend them, in accordance with the procedure set out in Article 66(2) of Regulation (EU) 2019/881, and taking into account the opinion of the European Cybersecurity Certification Group. Annex III contains recommended protection profiles, which at the time of entry into force of this Regulation are not state-of-the-art documents. They should be made public on the ENISA website referred to in Article 50(1) of Regulation (EU) 2019/881.

(33) This Regulation should start to apply 12 months after its entry into force. The requirements of Chapter IV and Annex V do not require a transition period and should therefore apply as from the entry into force of this Regulation.

(34) The measures provided for in this Regulation are consistent with the opinion of the European Cybersecurity Certification Committee established by Article 66 of Regulation (EU) 2019/881,

HAS ADOPTED THIS REGULATION:

Chapter I

General provisions

Article 1

Subject matter and scope

This Regulation sets out the European Common Criteria-based cybersecurity certification scheme (EUCC).

This Regulation applies to all information and communication technologies ('ICT') products, including their documentation, which are submitted for certification under the EUCC, and to

all protection profiles which are submitted for certification as part of the ICT process leading to the certification of ICT products.

Article 2

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) 'Common Criteria' mean the Common Criteria for Information Technology Security Evaluation, as set out in ISO standard ISO/IEC 15408;

(2) 'Common Evaluation Methodology' means the Common Methodology for Information Technology Security Evaluation, as set out in ISO/IEC standard ISO/IEC 18045;

(3) 'target of evaluation' means an ICT product or part thereof, or a protection profile as part of an ICT process, which is subjected to cybersecurity evaluation to receive EUCC certification;

(4) 'security target' means a claim of implementation-dependent security requirements for a specific ICT product;

(5) 'protection profile' means an ICT process that lays down the security requirements for a specific category of ICT products, addressing implementation-independent security needs, and that may be used to assess ICT products falling into that specific category for the purpose of their certification;

(6) 'evaluation technical report' means a document produced by an ITSEF to present the findings, verdicts and justifications obtained during the evaluation of an ICT product or a protection profile in accordance with the rules and obligations set out in this Regulation;

(7) 'ITSEF' means an Information Technology Security Evaluation Facility, which is a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008 that performs evaluation tasks;

(8) 'AVA_VAN level' means an assurance vulnerability analysis level that indicates the degree of cybersecurity evaluation activities carried out to determine the level of resistance against potential exploitability of flaws or weaknesses in the target of evaluation in its operational environment as set out in the Common Criteria;

(9) 'EUCC certificate' means a cybersecurity certificate issued under the EUCC for ICT products, or for protection profiles that can be used exclusively in the ICT process of certification of ICT products;

(10) 'composite product' means an ICT product that is evaluated together with another underlying ICT product that has already received an EUCC certificate and on whose security functionality the composite ICT product depends;

(11) 'national cybersecurity certification authority' means an authority designated by a Member State pursuant to Article 58(1) of Regulation (EU) 2019/881;

(12) 'certification body' means a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008, which performs certification activities;

(13) 'technical domain' means a common technical framework related to a particular technology for the harmonised certification with a set of characteristic security requirements;

(14) ‘state-of-the-art document’ means a document which specifies evaluation methods, techniques and tools that apply to the certification of ICT products, or security requirements of a generic ICT product category, or any other requirements necessary for certification, in order to harmonise evaluation, in particular of technical domains or protection profiles;

(15) ‘market surveillance authority’ means an authority defined in Article 3(4) of Regulation (EU) 2019/1020.

Article 3

Evaluation standards

The following standards shall apply to evaluations performed under the EUCC scheme:

(a) the Common Criteria;

(b) the Common Evaluation Methodology.

Article 4

Assurance levels

1. Certification bodies shall issue EUCC certificates at assurance level ‘substantial’ or ‘high’.

2. EUCC certificates at assurance level ‘substantial’ shall correspond to certificates that cover AVA_VAN level 1 or 2.

3. EUCC certificates at assurance level ‘high’ shall correspond to certificates that cover AVA_VAN level 3, 4 or 5.

4. The assurance level confirmed in a EUCC certificate shall distinguish between the conformant and augmented use of the assurance components as specified in the Common Criteria in accordance with Annex VIII.

5. Conformity assessment bodies shall apply those assurance components on which the selected AVA_VAN level depends in accordance with the standards referred to in Article 3.

Article 5

Methods for certifying ICT products

1. Certification of an ICT product shall be carried out against its security target:

(a) as defined by the applicant; or

(b) incorporating a certified protection profile as part of the ICT process, where the ICT product falls in the ICT product category covered by that protection profile.

2. Protection profiles shall be certified for the sole purpose of the certification of ICT products falling in the specific category of ICT products covered by the protection profile.

Article 6

Conformity self-assessment

A conformity self-assessment within the meaning of Article 53 of Regulation (EU) 2019/881 shall not be permitted.

Chapter II

Certification of ICT products

SECTION I

SPECIFIC STANDARDS AND REQUIREMENTS FOR EVALUATION

Article 7

Evaluation criteria and methods for ICT products

1. An ICT product submitted for certification shall, as a minimum, be evaluated in accordance with the following:

   (a) the applicable elements of the standards referred to in Article 3;

   (b) the security assurance requirements classes for vulnerability assessment and independent functional testing, as set out in the evaluation standards referred to in Article 3;

   (c) the level of risk associated with the intended use of the ICT products concerned pursuant to Article 52 of Regulation (EU) 2019/881 and their security functions that support the security objectives set out in Article 51 of Regulation (EU) 2019/881;

   (d) the applicable state-of-the-art documents listed in Annex I; and

   (e) the applicable certified protection profiles listed in Annex II.

2. In exceptional and duly justified cases, a conformity assessment body may request to refrain from applying the relevant state-of-the-art document. In such cases the conformity assessment body shall inform the national cybersecurity certification authority with a duly reasoned justification for its request. The national cybersecurity certification authority shall assess the justification for an exception and, where justified, approve it. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate. The national cybersecurity certification authority shall notify the approved exception, without undue delay, to the European Cybersecurity Certification Group, which may issue an opinion. The national cybersecurity certification authority shall take utmost account of the opinion of the European Cybersecurity Certification Group.

3. Certification of ICT products at AVA_VAN level 4 or 5 shall only be possible in the following scenarios:

   (a) where the ICT product is covered by any technical domain listed in Annex I, it shall be evaluated in accordance with the applicable state-of-the-art documents of those technical domains,

   (b) where the ICT product falls into a category of ICT products covered by a certified protection profile that includes AVA_VAN levels 4 or 5 and that has been listed as a state-of-the-art protection profile in Annex II, it shall be

evaluated in accordance with the evaluation methodology specified for that protection profile,

(c) where points a) and b) of this paragraph are not applicable and where the inclusion of a technical domain in Annex I or of a certified protection profile in Annex II is unlikely in the foreseeable future, and only in exceptional and duly justified cases, subject to the conditions set out in paragraph 4.

4. Where a conformity assessment body considers to be in an exceptional and duly justified case referred to in point c) of paragraph 3, it shall notify the intended certification to the national cybersecurity certification authority with a justification and a proposed evaluation methodology. The national cybersecurity certification authority shall assess the justification for an exception and, where justified, approve or amend the evaluation methodology to be applied by the conformity assessment body. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate. The national cybersecurity certification authority shall report, without undue delay, the intended certification to the European Cybersecurity Certification Group, which may issue an opinion. The national cybersecurity certification authority shall take utmost account of the opinion of the European Cybersecurity Certification Group.

5. In the case of an ICT product undergoing a composite product evaluation in accordance with the relevant state-of-the-art documents, the ITSEF that carried out the evaluation of the underlying ICT product shall share the relevant information with the ITSEF performing the evaluation of the composite ICT product.

SECTION II

ISSUANCE, RENEWAL AND WITHDRAWAL OF EUCC CERTIFICATES

Article 8

Information necessary for certification

1. An applicant for certification under EUCC shall provide or otherwise make available to the certification body and the ITSEF all information necessary for the certification activities.

2. The information referred to in paragraph 1 shall include all relevant evidence in accordance with the sections on ‘Developer action elements’ in the appropriate format as set out in the sections on ‘Content and presentation of evidence element’ of the Common Criteria and Common Evaluation Methodology for the selected assurance level and associated security assurance requirements. The evidence shall include, where necessary, details on the ICT product and its source code in accordance with this Regulation, subject to safeguards against unauthorised disclosure.

3. Applicants for certification may provide to the certification body and ITSEF appropriate evaluation results from prior certification pursuant to:

(a) this Regulation;

(b) another European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881;

(c) a national scheme referred to in Article 49 of this Regulation.

4. Where the evaluation results are pertinent to its tasks, the ITSEF may reuse the evaluation results provided that such results conform to the applicable requirements and its authenticity is confirmed.

5. Where the certification body allows the product to undergo a composite product certification, the applicant for certification shall make available to the certification body and the ITSEF all necessary elements, where applicable, in accordance with the state-of-the-art document.

6. Applicants for certification shall also provide the certification body and the ITSEF with the following information:

   (a) the link to their website containing the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881;

   (b) a description of the applicant's vulnerability management and vulnerability disclosure procedures.

7. All relevant documentation referred to in this Article shall be retained by the certification body, the ITSEF and the applicant for a period of 5 years after the expiry of the certificate.

Article 9

Conditions for issuance of an EUCC certificate

1. The certification bodies shall issue an EUCC certificate where all of the following conditions are met:

   (a) the category of ICT product falls within the scope of the accreditation, and where applicable of the authorisation, of the certification body and the ITSEF involved in the certification;

   (b) the applicant for certification has signed a statement undertaking all commitments listed in paragraph 2;

   (c) the ITSEF has concluded the evaluation without objection in accordance with the evaluation standards, criteria and methods referred to in Articles 3 and 7;

   (d) the certification body has concluded the review of the evaluation results without objection;

   (e) the certification body has verified that the evaluation technical reports provided by the ITSEF are consistent with the provided evidence and that the evaluation standards, criteria and methods referred to in Articles 3 and 7 have been correctly applied.

2. The applicant for certification shall undertake the following commitments:

   (a) to provide the certification body and the ITSEF with all the necessary complete and correct information, and to provide additional necessary information if requested;

   (b) not to promote the ICT product as being certified under the EUCC before the EUCC certificate has been issued;

   (c) to promote the ICT product as being certified only with respect to the scope set out in the EUCC certificate;

(d) to cease immediately the promotion of the ICT product as being certified in the event of the suspension, withdrawal or expiry of the EUCC certificate;

(e) to ensure that the ICT products sold with reference to the EUCC certificate are strictly identical to the ICT product subject to the certification;

(f) to respect the rules of use of the mark and label established for the EUCC certificate in accordance with Article 11.

3. In the case of an ICT product undergoing a composite product certification, in accordance with the relevant state-of-the-art documents, the certification body that carried out the certification of the underlying ICT product shall share the relevant information with the certification body performing the certification of the composite ICT product.

Article 10

Content and format of an EUCC certificate

1. An EUCC certificate shall include at least the information set out in Annex VII.

2. The scope and boundaries of the certified ICT product shall be unambiguously specified in the EUCC certificate or the certification report, indicating whether the entire ICT product has been certified or only parts thereof.

3. The certification body shall provide the applicant with the EUCC certificate at least in electronic form.

4. The certification body shall produce a certification report in accordance with Annex V for each EUCC certificate it issues. The certification report shall be based on the evaluation technical report issued by the ITSEF. The evaluation technical report and the certification report shall indicate the specific evaluation criteria and methods referred to in Article 7 used for the evaluation.

5. The certification body shall provide the national cybersecurity certification authority and ENISA with every EUCC certificate and every certification report in electronic form.

Article 11

Mark and label

1. The holder of a certificate may affix a mark and label to a certified ICT product. Mark and label demonstrate that the ICT product has been certified in accordance with this Regulation. Mark and label shall be affixed in accordance with this Article and with Annex IX.

2. The mark and label shall be affixed visibly, legibly and indelibly to the certified ICT product or its data plate. Where that is not possible or not warranted on account of the nature of the product, it shall be affixed to the packaging and to the accompanying documents. Where the certified ICT product is delivered in the form of software, the mark and label shall visibly, legibly and indelibly appear in its accompanying documentation or this documentation shall be made easily and directly accessible to users by means of a website.

3. The mark and label shall be set out as in Annex IX and contain:

(a) the assurance level and the AVA_VAN level of the certified ICT product;

(b) the unique identification of the certificate, consisting of:

(1) the name of the scheme;

(2) the name and the reference number of the accreditation of the certification body that has issued the certificate;

(3) year and month of issuance;

(4) identification number assigned by the certification body that has issued the certificate.

4. The mark and label shall be accompanied by a QR code with a link to a website containing at least:

(a) the information on the validity of the certificate;

(b) the necessary certification information as set out in Annexes V and VII;

(c) the information to be made publicly available by the holder of the certificate in accordance with Article 55 of Regulation (EU) 2019/881; and

(d) where applicable, the historic information related to the specific certification or certifications of the ICT product to enable traceability.

Article 12

Period of validity of an EUCC certificate

1. The certification body shall set a period of validity for each EUCC certificate issued taking into account the characteristics of the certified ICT product.

2. The period of validity of the EUCC certificate shall not exceed 5 years.

3. By derogation from paragraph 2 that period may exceed 5 years, subject to the prior approval of the national cybersecurity certification authority. The national cybersecurity certification authority shall notify the European Cybersecurity Certification Group of the granted approval without undue delay.

Article 13

Review of an EUCC certificate

1. Upon request of the holder of the certificate or for other justified reasons, the certification body may decide to review the EUCC certificate for an ICT product. The review shall be carried out in accordance with Annex IV. The certification body shall determine the extent of the review. Where necessary for the review, the certification body shall request the ITSEF to perform a re-evaluation of the certified ICT product.

2. Following the results of the review, and where applicable of the re-evaluation, the certification body shall:

(a) confirm the EUCC certificate;

(b) withdraw the EUCC certificate in accordance with Article 14;

(c) withdraw the EUCC certificate in accordance with Article 14 and issue a new EUCC certificate with an identical scope and an extended validity period; or

(d) withdraw the EUCC certificate in accordance with Article 14 and issue a new EUCC certificate with a different scope.

3. The certification body may decide to suspend, without undue delay, the EUCC certificate in accordance with Article 30, pending remedial action by the holder of the EUCC certificate.

Article 14

Withdrawal of an EUCC certificate

1. Without prejudice to Article 58(8), point (e), of Regulation (EU) 2019/881, an EUCC certificate shall be withdrawn by the certification body that issued that certificate.

2. The certification body referred to in paragraph 1 shall notify the national cybersecurity certification authority of the withdrawal of the certificate. It shall also notify ENISA of such withdrawal in view of facilitating the performance of its task under Article 50 of Regulation (EU) 2019/881. The national cybersecurity certification authority shall notify other relevant market surveillance authorities.

3. The holder of an EUCC certificate may request the withdrawal of the certificate.

Chapter III

Certification of protection profiles

SECTION I

SPECIFIC STANDARDS AND REQUIREMENTS FOR EVALUATION

Article 15

Evaluation criteria and methods

1. A protection profile shall be evaluated, as a minimum, in accordance with the following:

(a) the applicable elements of the standards referred to in Article 3;

(b) the level of risk associated with the intended use of the ICT products concerned pursuant to Article 52 of Regulation (EU) 2019/881 and their security functions that support the security objectives set out in Article 51 of that; and

(c) the applicable state-of-the-art documents listed in Annex I. A protection profile covered by a technical domain shall be certified against the requirements set out in that technical domain.

2. In exceptional and duly justified cases, a conformity assessment body may certify a protection profile without applying the relevant state-of-the-art documents. In such cases, it shall inform the competent national cybersecurity certification authority and provide a justification for the intended certification without application of the relevant state-of-the-art documents as well as the proposed evaluation methodology. The national cybersecurity certification authority shall assess the justification and, where justified, approve the non-application of the relevant state-of-the-art documents, and approve or amend, where appropriate, the evaluation methodology to

be applied by the conformity assessment body. Pending the decision of the national cybersecurity certification authority, the conformity assessment body shall not issue any certificate for the protection profile. The national cybersecurity certification authority shall notify, without undue delay, the authorised non-application of the relevant state-of-the-art documents to the European Cybersecurity Certification Group, which may issue an opinion. The national cybersecurity certification authority shall take utmost account of the opinion of the European Cybersecurity Certification Group.

SECTION II

ISSUING, RENEWING AND WITHDRAWING EUCC CERTIFICATES FOR PROTECTION PROFILES

Article 16

Information necessary for certification of protection profiles

An applicant for certification of a protection profile shall provide or otherwise make available to the certification body and the ITSEF all information necessary for the certification activities. Article 8(2), (3), (4) and (7) shall apply mutatis mutandis.

Article 17

Issuance of EUCC certificates for protection profiles

1. The applicant for certification shall provide the certification body and the ITSEF with all the necessary complete and correct information.
2. Articles 9 and 10 shall apply mutatis mutandis.
3. The ITSEF shall evaluate whether a protection profile is complete, consistent, technically sound and effective for the intended use and the security objectives of the ICT product's category covered by that protection profile.
4. A protection profile shall be certified solely by:
   (a) a national cybersecurity certification authority or another public body accredited as certification body; or
   (b) a certification body, upon prior approval by the national cybersecurity certification authority for each individual protection profile.

Article 18

Period of validity of an EUCC certificate for protection profiles

1. The certification body shall set a period of validity for each EUCC certificate.
2. The period of validity may be up to the lifetime of the protection profile concerned.

Article 19

Review of an EUCC certificate for protection profiles

1. Upon request of the holder of the certificate or for other justified reasons, the certification body may decide to review an EUCC certificate for a protection profile.

The review shall be carried out by applying the conditions set out in Article 15. The certification body shall determine the extent of the review. Where necessary for the review, the certification body shall request the ITSEF to perform a re-evaluation of the certified protection profile.

2. Following the results of the review, and where applicable of the re-evaluation, the certification body shall do one of the following:

(a) confirm the EUCC certificate;

(b) withdraw the EUCC certificate in accordance with Article 20;

(c) withdraw the EUCC certificate in accordance with Article 20 and issue a new EUCC certificate with an identical scope and an extended validity period;

(d) withdraw the EUCC certificate in accordance with Article 20 and issue a new EUCC certificate with a different scope.

Article 20

Withdrawal of an EUCC certificate for a protection profile

1. Without prejudice to Article 58(8), point (e) of Regulation (EU) 2019/881, an EUCC certificate for a protection profile shall be withdrawn by the certification body that issued that certificate. Article 14 shall apply mutatis mutandis.

2. A certificate for a protection profile issued in accordance with Article 17(4), point (b) shall be withdrawn by the national cybersecurity certification authority that approved that certificate.

Chapter IV

Conformity assessment bodies

Article 21

Additional or specific requirements for a certification body

1. A certification body shall be authorised by the national cybersecurity certification authority to issue EUCC certificates at assurance level 'high' where that body demonstrates that, in addition to meeting the requirements laid down in Article 60(1) and the Annex to Regulation (EU) 2019/881 regarding accreditation of conformity assessment bodies, the following:

(a) it has the expertise and competences required for the certification decision at assurance level 'high';

(b) it conducts its certification activities in cooperation with an ITSEF authorised in accordance with Article 22; and

(c) it has the requisite competences and put in place appropriate technical and operational measures to effectively protect confidential and sensitive information for assurance level 'high', in addition to the requirements set out in Article 43.

2. The national cybersecurity certification authority shall assess whether a certification body fulfils all the requirements set out in paragraph 1. That assessment shall include

at least structured interviews and a review of at least one pilot certification performed by the certification body in accordance with this Regulation.

In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities granted pursuant to:

(a) this Regulation;

(b) another European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881;

(c) a national scheme referred to in Article 49 of this Regulation.

3. The national cybersecurity certification authority shall produce an authorisation report which is subject to peer review in accordance with Article 59(3), point (d), of Regulation (EU) 2019/881.

4. The national cybersecurity certification authority shall specify the ICT product categories and protection profiles to which the authorisation extends. The authorisation shall be valid for a period no longer than the validity of the accreditation. It may be renewed upon request provided that the certification body still meets the requirements set out in this Article. For the renewal of the authorisation, no pilot evaluations are required.

5. The national cybersecurity certification authority shall withdraw the authorisation of the certification body where it no longer meets the conditions set out in this Article. Upon withdrawal of the authorisation, the certification body shall cease immediately promoting itself as an authorised certification body.

Article 22

Additional or specific requirements for an ITSEF

1. An ITSEF shall be authorised by the national cybersecurity certification authority to carry out the evaluation of ICT products which are subject to certification under the assurance level ‘high’, where the ITSEF demonstrates that, in addition to meeting the requirements laid down in Article 60(1) and the Annex to Regulation (EU) 2019/881 regarding accreditation of conformity assessment bodies, it complies with all of the following conditions:

(a) it has the necessary expertise for performing the evaluation activities to determine the resistance to state-of-the-art cyberattacks carried out by actors with significant skills and resources;

(b) for the technical domains and protection profiles, which are part of the ICT process for those ICT products, it has:

(1) the expertise to perform the specific evaluation activities necessary to methodically determine a target of evaluation’s resistance against skilled attackers in its operational environment assuming an attack potential of ‘moderate’ or ‘high’ as set out in the standards referred to in Article 3;

(2) the technical competences as specified in the state-of-the-art documents listed in Annex I;

(c) it has the requisite competences and put in place appropriate technical and operational measures to effectively protect confidential and sensitive

information for assurance level 'high' in addition to the requirements set out in Article 43.

2. The national cybersecurity certification authority shall assess whether an ITSEF fulfils all the requirements set out in paragraph 1. That assessment shall include at least structured interviews and a review of at least one pilot evaluation performed by the ITSEF in accordance with this Regulation.

3. In its assessment, the national cybersecurity certification authority may reuse any appropriate evidence from prior authorisation or similar activities granted pursuant to:

   (a) this Regulation;

   (b) another European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881;

   (c) a national scheme referred to in Article 49 of this Regulation.

4. The national cybersecurity certification authority shall produce an authorisation report which is subject to peer review in accordance with Article 59(3), point (d) of Regulation (EU) 2019/881.

5. The national cybersecurity certification authority shall specify the ICT product categories and protection profiles to which the authorisation extends. The authorisation shall be valid for period no longer than the validity of the accreditation. It may be renewed upon request provided that the ITSEF still meets the requirements set out in this Article. For the renewal of the authorisation, no pilot evaluations should be required.

6. The national cybersecurity certification authority shall withdraw the authorisation of the ITSEF where it no longer meets the conditions set out in this Article. Upon withdrawal of the authorisation, the ITSEF shall stop promoting itself as being an authorised ITSEF.

Article 23

Notification of certification bodies

1. The national cybersecurity certification authority shall notify the Commission of the certification bodies in its territory that are competent to certify at assurance level 'substantial' based on their accreditation.

2. The national cybersecurity certification authority shall notify the Commission of the certification bodies in their territory that are competent to certify at assurance level 'high' based on their accreditation and the authorisation decision.

3. The national cybersecurity certification authority shall provide at least the following information when notifying the Commission of the certification bodies:

   (a) the assurance level or levels for which the certification body is competent to issue EUCC certificates;

   (b) the following information related to accreditation:

      (1) date of the accreditation;

      (2) name and address of the certification body;

      (3) country of registration of the certification body;

(4) reference number of the accreditation;

(5) scope and duration of validity of the accreditation;

(6) the address, location and link to the relevant website of the national accreditation body; and

(c) the following information related to authorisation for level 'high':

(1) date of the authorisation;

(2) reference number of the authorisation;

(3) duration of validity of the authorisation;

(4) scope of the authorisation including the highest AVA_VAN level and, where applicable, the covered technical domain.

4. The national cybersecurity certification authority shall send a copy of the notification referred to in paragraphs 1 and 2 to ENISA for the publication of accurate information on the cybersecurity certification website regarding the eligibility of certification bodies.

5. The national cybersecurity certification authority shall examine without undue delay any information regarding a change in the status of the accreditation provided by the national accreditation body. Where the accreditation or authorisation have been withdrawn, the national cybersecurity certification authority shall inform the Commission thereof, and may submit to the Commission a request in accordance with Article 61(4) of Regulation (EU) 2019/881.

Article 24

Notification of ITSEF

The notification obligations of the national cybersecurity certification authorities set out in Article 23 shall also apply to ITSEF. The notification shall include the address of the ITSEF, the valid accreditation and, where applicable, the valid authorisation of that ITSEF.

Chapter V

Monitoring, non-conformity and non-compliance

SECTION I

COMPLIANCE MONITORING

Article 25

Monitoring activities by the national cybersecurity certification authority

1. Without prejudice to Article 58(7) of Regulation (EU) 2019/881, the national cybersecurity certification authority shall monitor the compliance of:

(a) the certification body and the ITSEF with their obligations pursuant to this Regulation and Regulation (EU) 2019/881;

(b) the holders of an EUCC certificate with their obligations pursuant to this Regulation and Regulation (EU) 2019/881;

(c) the certified ICT products with the requirements set out in the EUCC;

(d) the assurance expressed in the EUCC certificate addressing the evolving threat landscape.

2. The national cybersecurity certification authority shall perform its monitoring activities in particular on the basis of:

(a) information coming from certification bodies, national accreditation bodies and relevant market surveillance authorities;

(b) information resulting from its own or another authority's audits and investigations;

(c) sampling, carried out in accordance with paragraph 3;

(d) complaints received.

3. The national cybersecurity certification authority shall, in cooperation with other market surveillance authorities, sample annually at least 4% of the EUCC certificates as determined by a risk assessment. Upon request and acting on behalf of the competent national cybersecurity certification authority, certification bodies and, if necessary, ITSEF shall assist that authority in monitoring compliance.

4. The national cybersecurity certification authority shall select the sample of certified ICT products to be checked using objective criteria, including:

(a) product category;

(b) assurance levels of products;

(c) holder of a certificate;

(d) certification body and, where applicable, the subcontracted ITSEF;

(e) any other information brought to the authority's attention.

5. The national cybersecurity certification authority shall inform the holders of the EUCC certificate about the selected ICT products and the selection criteria.

6. The certification body that certified the sampled ICT product shall, upon request of the national cybersecurity certification authority, with the assistance of the respective ITSEF, conduct additional review in accordance with the procedure laid down in Section IV.2 of Annex IV and inform the national cybersecurity certification authority of the results.

7. Where the national cybersecurity certification authority has sufficient reason to believe that a certified ICT product is no longer in compliance with this Regulation or Regulation (EU) 2019/881, it may carry out investigations or make use of any other monitoring powers set out in Article 58(8) of Regulation (EU) 2019/881.

8. The national cybersecurity certification authority shall inform the certification body and ITSEF concerned about ongoing investigations regarding selected ICT products.

9. Where the national cybersecurity certification authority identifies that an ongoing investigation concerns ICT products that are certified by certification bodies established in other Member States, it shall inform thereof the national cybersecurity certification authorities of the relevant Member States in order to collaborate in the

investigations, where relevant. Such national cybersecurity certification authority shall also notify the European Cybersecurity Certification Group of the cross-border investigations and the subsequent results.

Article 26

Monitoring activities by the certification body

1. The certification body shall monitor:
   (a) the compliance of the holders of a certificate with their obligations under this Regulation and Regulation (EU) 2019/881 towards the EUCC certificate that was issued by the certification body;
   (b) the compliance of the ICT products it has certified with their respective security requirements;
   (c) the assurance expressed in the certified protection profiles.
2. The certification body shall undertake its monitoring activities on the basis of:
   (a) the information provided on the basis of the commitments of the applicant for certification referred to in Article 9(2);
   (b) information resulting from activities of other relevant market surveillance authorities;
   (c) complaints received;
   (d) vulnerability information that could impact the ICT products it has certified.
3. The national cybersecurity certification authority may draw up rules for a periodical dialogue between certification bodies and holders of EUCC certificates to verify and report on compliance with the commitments made pursuant to Article 9(2), without prejudice to activities related to other relevant market surveillance authorities.

Article 27

Monitoring activities by the holder of the certificate

1. The holder of an EUCC certificate shall perform the following tasks to monitor the conformity of the certified ICT product with its security requirements:
   (a) monitor vulnerability information regarding the certified ICT product, including known dependencies by its own means but also in consideration of:
      (1) a publication or a submission regarding vulnerability information by a user or security researcher referred to in Article 55(1), point (c) of Regulation (EU) 2019/881;
      (2) a submission by any other source;
   (b) monitor the assurance expressed in the EUCC certificate.
2. The holder of an EUCC certificate shall work in cooperation with the certification body, the ITSEF, and, where applicable, the national cybersecurity certification authority to support their monitoring activities.

SECTION II

CONFORMITY AND COMPLIANCE

Article 28

Consequences of non-conformity of a certified ICT product or protection profile

1. Where a certified ICT product or protection profile does not conform with the requirements laid down in this Regulation and in Regulation (EU) 2019/881, the certification body shall inform the holder of the EUCC certificate about the identified non-conformity and request remedial actions.
2. Where an instance of non-conformity with the provisions of this Regulation might affect compliance with other relevant Union legislation, which provides for the possibility to demonstrate the presumption of conformity with the requirements of that legal act by using the EUCC certificate, the certification body shall inform the national cybersecurity certification authority without delay. The national cybersecurity certification authority shall immediately notify the market surveillance authority responsible for such other relevant Union legislation regulation about the instance of non-conformity identified.
3. Upon receipt of the information referred to in paragraph 1, the holder of the EUCC certificate shall within the time period set by the certification body, which shall not exceed 30 days, propose to the certification body the remedial action necessary to address the non-conformity.
4. The certification body may suspend, without undue delay, the EUCC certificate in accordance with Article 30 in case of emergency, or where the holder of the EUCC certificate does not duly cooperate with the certification body.
5. The certification body shall carry out a review in accordance with Articles 13 and 19, assessing whether the remedial action addresses the non-conformity.
6. Where the holder of the EUCC certificate does not propose appropriate remedial action during the period referred to in paragraph 3, the certificate shall be suspended in accordance with Article 30 or withdrawn in accordance with Articles 14 or 20.
7. This Article shall not apply to cases of vulnerabilities affecting a certified ICT product, which shall be handled in accordance with Chapter VI.

Article 29

Consequences of non-compliance by the holder of the certificate

1. Where the certification body finds that:
   (a) the holder of the EUCC certificate or the applicant for certification is not compliant with its commitments and obligations as set out in Articles 9(2), 17(2), 27 and 41; or
   (b) the holder of the EUCC certificate does not comply with Article 56(8) of Regulation (EU) 2019/881 or Chapter VI of this Regulation;

it shall set a time period of not more than 30 days within which the holder of the EUCC certificate shall take remedial action.

2. Where the holder of the EUCC certificate does not propose appropriate remedial action during the time period referred to in paragraph 1, the certificate shall be suspended in accordance with Article 30 or withdrawn in accordance with Article 14 and Article 20.

3. Continued or recurring infringement by the holder of the EUCC certificate of the obligations referred to in paragraph 1 shall trigger the withdrawal of the EUCC certificate in accordance with Articles 14 or Article 20.

4. The certification body shall inform the national cybersecurity certification authority of the findings referred to in paragraph 1. Where the instance of non-compliance affects compliance with other relevant Union legislation, the national cybersecurity certification authority shall immediately notify the market surveillance authority responsible for such other relevant Union legislation about the instance of non-compliance identified.

Article 30

Suspension of the EUCC certificate

1. Where this Regulation refers to suspension of an EUCC certificate, the certification body shall suspend an EUCC certificate concerned for a period appropriate to the circumstances triggering suspension, that does not exceed 42 days. The suspension period shall begin on the day following the day of the decision of the certification body. The suspension shall not affect the validity of the certificate.

2. The certification body shall notify the holder of the certificate and the national cybersecurity certification authority of the suspension without undue delay and shall provide the reasons for the suspension, the requested actions to be taken and the suspension period.

3. Certification holders shall notify the purchasers of the ICT products concerned about the suspension and the reasons provided by the certification body for the suspension, except those parts of the reasons the sharing of which would constitute a security risk or which contain sensitive information. This information shall also be made publicly available by the holder of the certificate.

4. Where other relevant Union legislation provides for a presumption of conformity based on certificates issued under the provisions of this Regulation, the national cybersecurity certification authority shall inform the market surveillance authority responsible for such other relevant Union legislation about the suspension.

5. The suspension of a certificate shall be notified to ENISA in accordance with Article 42(3).

6. In duly justified cases, the national cybersecurity certification authority may authorise an extension of the period of suspension of an EUCC certificate. The total period of suspension may not exceed 1 year.

Article 31

Consequences of non-compliance by the conformity assessment body

1. In case of non-compliance by a certification body with its obligations, or by the relevant certification body in case of identifying non-compliance by an ITSEF, the national cybersecurity certification authority shall, without undue delay:

(a) identify, with the support of the concerned ITSEF, the potentially affected EUCC certificates;

(b) where necessary, request evaluation activities to be performed on one or more ICT products or protection profiles by either the ITSEF which performed the evaluation, or any other accredited and, where applicable, authorised ITSEF that may be in a better technical position to support that identification;

(c) analyse the impacts of non-compliance;

(d) notify the holder of the EUCC certificate affected by non-compliance.

2. On the basis of the measures referred to in paragraph 1, the certification body shall adopt either of the following decisions with respect to each affected EUCC certificate:

(a) maintain the EUCC certificate unaltered;

(b) withdraw the EUCC certificate in accordance with Article 14 or Article 20, and, where appropriate, issue a new EUCC certificate.

3. On the basis of the measures referred to in paragraph 1, the national cybersecurity certification authority shall:

(a) where necessary, report the non-compliance of the certification body or related ITSEF to the national accreditation body;

(b) where applicable, assess the potential impact on the authorisation.

Chapter VI

Vulnerability management and disclosure

Article 32

Scope of vulnerability management

This Chapter applies to ICT products for which an EUCC certificate was issued.

SECTION I

VULNERABILITY MANAGEMENT

Article 33

Vulnerability management procedures

1. The holder of an EUCC certificate shall establish and maintain all necessary vulnerability management procedures in accordance with the rules laid down in this Section and, where necessary, supplemented by the procedures set out in EN ISO/IEC 30111.

2. The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers.

3. Where a holder of an EUCC certificate detects or receives information about a potential vulnerability affecting a certified ICT product, it shall record it and carry out a vulnerability impact analysis.

4. When a potential vulnerability impacts a composite product, the holder of the EUCC certificate shall inform the holder of dependent EUCC certificates about potential vulnerability.

5. In response to a reasonable request by the certification body that issued the certificate, the holder of an EUCC certificate shall transmit all relevant information about potential vulnerabilities to that certification body.

Article 34

Vulnerability impact analysis

1. Vulnerability impact analysis shall refer to the target of evaluation and the assurance statements contained in the certificate. Vulnerability impact analysis shall be carried out in a timeframe appropriate for the exploitability and criticality of the potential vulnerability of the certified ICT product.

2. Where applicable, an attack potential calculation shall be performed in accordance with the relevant methodology included in the standards referred to in Article 3 and the relevant state-of-the-art documents listed in Annex I, in order to determine the exploitability of the vulnerability. The AVA_VAN level of the EUCC certificate shall be taken into account.

Article 35

Vulnerability impact analysis report

1. The holder shall produce a vulnerability impact analysis report where the impact analysis shows that the vulnerability has a likely impact on the conformity of the ICT product with its certificate.

2. The vulnerability impact analysis report shall contain an assessment of the following elements:

   (a) the impact of the vulnerability on the certified ICT product;

   (b) possible risks associated with the proximity or availability of an attack;

   (c) whether the vulnerability may be remedied;

   (d) where the vulnerability may be remedied, possible resolutions of the vulnerability.

3. The vulnerability impact analysis report shall, where applicable, contain details about the possible means of exploitation of the vulnerability. Information pertaining to possible means of exploitation of the vulnerability shall be handled in accordance with appropriate security measures to protect its confidentiality and ensure, where necessary, its limited distribution.

4. The holder of an EUCC certificate shall transmit a vulnerability impact analysis report to the certification body or the national cybersecurity certification authority in accordance with Article 56(8) of Regulation (EU) 2019/881, without undue delay.

5. Where the vulnerability impact analysis report determines that the vulnerability is not residual within the meaning of standards referred to in Article 3, and that it can be remedied, Article 36 shall apply.

6. Where the vulnerability impact analysis report determines that the vulnerability is not residual and that it cannot be remedied, the EUCC certificate shall be withdrawn in accordance with Article 14.

7. The holder of the EUCC certificate shall monitor any residual vulnerabilities to ensure that it cannot be exploited in case of the changes in the operational environment.

Article 36

Vulnerability remediation

The holder of an EUCC certificate shall submit a proposal for an appropriate remedial action to the certification body. Certification body shall review the certificate in accordance with Article 13. The scope of the review shall be determined by the proposed remediation of the vulnerability.

SECTION II

VULNERABILITY DISCLOSURE

Article 37

Information shared with the national cybersecurity certification authority

1. The information provided by the certification body to the national cybersecurity certification authority shall include all elements necessary for the national cybersecurity certification authority to understand the impact of the vulnerability, the changes to be made to the ICT product and, where available, any information from the certification body on the broader implications of the vulnerability for other certified ICT products.

2. The information provided in accordance with paragraph 1 shall not contain details of the means of exploitation of the vulnerability. This provision is without prejudice to the investigative powers of the national cybersecurity certification authority.

Article 38

Cooperation with other national cybersecurity certification authorities

1. The national cybersecurity certification authority shall share the relevant information received in accordance with Article 37 with other national cybersecurity certification authorities and ENISA.

2. Other national cybersecurity certification authorities may decide to further analyse the vulnerability or, after informing the holder of the EUCC certificate, request the relevant certification bodies to assess whether the vulnerability may affect other certified ICT products.

Article 39

Publication of the vulnerability

Upon withdrawal of a certificate, the holder of the EUCC certificate shall disclose and register any publicly known and remediated vulnerability in the ICT product on the European vulnerability database, established in accordance with Article 12 of Directive (EU) 2022/2555 of the European Parliament and of the Council[5] or other online repositories referred to in Article 55(1), point (d) of Regulation (EU) 2019/881.

Chapter VII

Retention, disclosure and protection of information

Article 40

Retention of records by certification bodies and the ITSEF

1. The ITSEF and certification bodies shall maintain a record system, which shall contain all documents produced in connection with each evaluation and certification they perform.

2. Certification bodies and the ITSEF shall store the records in a secure manner and shall keep those records for the period necessary for the purposes of this Regulation and for at least 5 years after the withdrawal of the relevant EUCC certificate. When the certification body has issued a new EUCC certificate in accordance with Article 13(2), point (c), it shall retain the documentation of the withdrawn EUCC certificate together with and as long as for the new EUCC certificate.

Article 41

Information made available by the holder of a certificate

1. The information referred to in Article 55 of Regulation (EU) 2019/881 shall be available in a language that can be easily accessible to users.

2. The holder of an EUCC certificate shall store the following securely for the period necessary for the purposes of this Regulation and for at least 5 years after the withdrawal of the relevant EUCC certificate:

   (a) records of the information provided to the certification body and to the ITSEF during the certification process;

   (b) specimen of the certified ICT product.

3. When the certification body has issued a new EUCC certificate in accordance with Article 13(2), point (c), the holder shall retain the documentation of the withdrawn EUCC certificate together with and as long as for the new EUCC certificate.

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

4. Upon request by the certification body or the national cybersecurity certification authority, the holder of an EUCC certificate shall make available the records and copies referred to in paragraph 2.

Article 42

Information to be made available by ENISA

1. ENISA shall publish the following information on the website referred to in Article 50(1) of Regulation (EU) 2019/881:
   (a) all EUCC certificates;
   (b) the information on the status of an EUCC certificate, notably whether it is in force, suspended, withdrawn, or expired;
   (c) certification reports corresponding to each EUCC certificate;
   (d) a list of accredited conformity assessment bodies;
   (e) a list of authorised conformity assessment bodies;
   (f) the state-of-the-art documents listed in Annex I
   (g) the opinions of the European Cybersecurity Certification Group referred to in Article 62(4), point (c), of Regulation (EU) 2019/881;
   (h) peer assessment reports issued in accordance with Article 47.
2. The information referred to in paragraph 1 shall be made available at least in English.
3. Certification bodies and, where applicable, national cybersecurity certification authorities shall inform ENISA without delay about their decisions which affect the content or the status of an EUCC certificate referred to in paragraph 1, point (b).
4. ENISA shall ensure that the information published in accordance with paragraph 1 points (a), (b) and (c), clearly identifies the versions of a certified ICT product which are covered by an EUCC certificate.

Article 43

Protection of information

Conformity assessment bodies, national cybersecurity certification authorities, ECCG, ENISA, the Commission and all other parties shall ensure the security and protection of business secrets and other confidential information, including trade secrets, as well as the preserving intellectual property rights, and take the necessary and appropriate technical and organisational measures.

Chapter VIII

Mutual recognition agreements with third countries

Article 44

Conditions

1. Third countries willing to certify their products in accordance with this Regulation, and who wish to have such certification recognised within the Union, shall conclude a mutual recognition agreement with the Union.

2. The mutual recognition agreement shall cover the applicable assurance levels for certified ICT products and, where applicable, protection profiles.

3. Mutual recognition agreements referred to in paragraph 1, may only be concluded with third countries that meet the following conditions:

   (a) have an authority that:

      (1) is a public body, independent of the entities it supervises and monitors in terms of organisational and legal structure, financial funding and decision making;

      (2) has appropriate monitoring and supervising powers to carry out investigations and is empowered to take appropriate corrective measures to ensure compliance;

      (3) has an effective, proportionate and dissuasive penalty system to ensure compliance;

      (4) agrees to collaborate with the European Cybersecurity Certification Group and ENISA to exchange best practice and relevant developments in the field of cybersecurity certification and to work towards a uniform interpretation of the currently applicable evaluation criteria and methods, amongst others, by applying harmonised documentation that is equivalent to the state-of-the-art documents listed in Annex I

   (b) have an independent accreditation body performing accreditations using equivalent standards to those referred to in Regulation (EC) No 765/2008;

   (c) commit that the evaluation and certification processes and procedures will be carried out in a duly professional manner, taking into account compliance with the international standards referred to in this Regulation, in particular in Article 3;

   (d) have the capacity to report previously undetected vulnerabilities and an established, adequate vulnerability management and disclosure procedure in place;

   (e) have established procedures that enable it to effectively lodge and handle complaints and provide effective legal remedy for the complainant;

   (f) establishing a mechanism for cooperation with other Union and Member States' bodies relevant to the cybersecurity certification under this Regulation including the sharing of information about the possible non-compliance of certificates, monitoring relevant developments in the field of certification and ensuring a joint approach on certification maintenance and review.

4. In addition to the conditions set out in paragraph 3, a mutual recognition agreement referred to in paragraph 1 covering assurance level "high" may only be concluded with third countries where also the following conditions are met:

   (a) the third country has an independent and public cybersecurity certification authority performing or delegating evaluation activities necessary to allow certification under assurance level 'high' that are equivalent to the

requirements and procedures laid down for national cybersecurity authorities in this Regulation and in Regulation (EU) 2019/881;

(b) the mutual recognition agreement establishes a joint mechanism equivalent to the peer assessment for EUCC certification to enhance the exchange of practices and jointly solve issues in the area of evaluation and certification.

Chapter IX

Peer assessment of certification bodies

Article 45

Peer assessment procedure

1. A certification body issuing EUCC certificates at assurance level 'high' shall undergo a peer assessment on a regular basis and at least every 5 years. The different types of peer assessment are listed in Annex VI.

2. The European Cybersecurity Certification Group shall draw up and maintain a schedule of peer assessments ensuring that such periodicity is respected. Except in duly justified cases, peer assessments shall be performed on-site.

3. The peer assessment may rely on evidence gathered in the course of previous peer assessments or equivalent procedures of the peer-assessed certification body or national cybersecurity certification authority, provided that:

   (a) the results are not older than 5 years;

   (b) the results are accompanied by a description of the peer assessment procedures established for that scheme where they relate to a peer assessment conducted under a different certification scheme;

   (c) the peer assessment report referred to in Article 47 specifies which results were reused with or without further assessment.

4. Where a peer assessment covers a technical domain, the concerned ITSEF shall also be assessed.

5. The peer-assessed certification body and, where necessary, the national cybersecurity certification authority shall ensure that all relevant information is made available to the peer assessment team.

6. The peer assessment shall be carried out by a peer assessment team set up in accordance with Annex VI.

Article 46

Peer assessment phases

1. During the preparatory phase, the members of the peer assessment team shall review the certification body's documentation, covering its policies and procedures, including the use of state-of-the-art documents.

2. During site visit phase, the peer assessment team assesses the body's technical competence and, where applicable, the competence of an ITSEF that performed at least one ICT product evaluation covered by peer assessment.

3. The duration of the site visit phase may be extended or reduced depending on such factors as the possibility of reusing existing peer assessment evidence and results or the number of ITSEF and technical domains for which the certification body issues certificates.

4. If applicable, the peer assessment team shall determine the technical competence of each ITSEF by visiting its technical laboratory or laboratories and interviewing its evaluators as regards the technical domain and related specific attack methods.

5. In the reporting phase, the assessment team shall document their findings in a peer assessment report including a verdict and, where applicable, a list of observed non-conformities, each graded by a criticality level.

6. The peer assessment report must be first discussed with the peer-assessed certification body. Following those discussions, the peer-assessed certification body establishes a schedule of the measures to be taken to address the findings.

Article 47

Peer assessment report

1. The peer assessment team shall provide the peer-assessed certification body with a draft of the peer assessment report.

2. The peer-assessed certification body shall submit to the peer assessment team comments regarding the findings and a list of commitments to address the shortcomings identified in the draft peer assessment report.

3. The peer assessment team shall submit to the European Cybersecurity Certification Group a final peer assessment report, which shall also include the comments and the commitments made by the peer-assessed certification body. The peer assessment team shall also include their position on the comments and on whether those commitments are sufficient to address the shortcomings identified.

4. Where non-conformities are identified in the peer-assessment report, the European Cybersecurity Certification Group may set an appropriate time limit for the peer-assessed certification body to address the non-conformities.

5. The European Cybersecurity Certification Group shall adopt an opinion on the peer assessment report:

   (a) where the peer-assessment report does not identify non-conformities or where non-conformities have been appropriately addressed by the peer-assessed certification body, the European Cybersecurity Certification Group may issue a positive opinion and all relevant documents shall be published on ENISA's certification website;

   (b) where the peer-assessed certification body does not address the non-conformities appropriately within the set time limit, the European Cybersecurity Certification Group may issue a negative opinion that shall be published on ENISA's certification website, including the peer assessment report and all relevant documents.

6. Prior to the publication of the opinion, all sensitive, personal or proprietary information shall be removed from the published documents.

Chapter X

Maintenance of the scheme

Article 48

Maintenance of the EUCC

1. The Commission may request the European Cybersecurity Certification Group to adopt an opinion in view of maintaining the EUCC and to undertake the necessary preparatory works.
2. The European Cybersecurity Certification Group may adopt an opinion to endorse state-of-the-art documents.
3. State-of-the-art documents which have been endorsed by the European Cybersecurity Certification Group shall be published by ENISA.

Chapter XI

Final provisions

Article 49

National schemes covered by the EUCC

1. In accordance with Article 57(1) of Regulation (EU) 2019/881 and without prejudice to Article 57(3) of that Regulation, all national cybersecurity certification schemes and the related procedures for ICT products and ICT processes that are covered by the EUCC shall cease to produce effects from 12 months after the entry into force of this Regulation.
2. By derogation from Article 50, a certification process may be initiated under a national cybersecurity certification scheme within 12 months from the entry into force of this Regulation provided that the certification process is finalised not later than 24 months after entry into force of this Regulation.
3. Certificates issued under national cybersecurity certification schemes may be subject to review. New certificates replacing the reviewed certificates shall be issued in accordance with this Regulation.

Article 50

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from [Publications Office: insert the date 12 months after the date of entry into force].

Chapter IV and Annex V shall apply from the date of entry into force of this Regulation.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 31.1.2024

For the Commission
The President
Ursula VON DER LEYEN