EUROPEAN
COMMISSION

Brussels, XXX
[…](2024) XXX draft

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation

(Text with EEA relevance)

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation

(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) No 526/2013 (Cybersecurity Act)[1], and in particular Article 49(7) thereof,

Whereas:

(1) Commission Implementing Regulation (EU) 2024/482[2] 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.

(2) Implementing Regulation (EU) 2024/482 is based on established international standards that are the Common Criteria and the Common Evaluation Methodology maintained by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Implementing Regulation (EU) 2024/482 makes reference to ISO/IEC standards, but it does not specify the applicable version of those standards. It should therefore be specified which version of the standards applies for certificates issued under the EUCC. The governmental organisations that contributed to the development of the above-mentioned standards through the Common Criteria Recognition Arrangement (CCRA) are joint holders, together with ISO/IEC of the copyrights to them. These governmental organisations retain the right to use their version of the standard. Seeing the importance of these documents originating from CCRA, they should also be a basis for certification under this scheme during a transition period.

(3) International standards related to the Common Criteria might be subject to updates. To ensure an orderly and timely transition, it is appropriate to define transition rules to give vendors, Information Technologies Security Evaluation Facilities (ITSEFs) and certification bodies, and other relevant actors enough time for the necessary adjustments. Such transition rules should align to the appropriate extent with global practices, such as those defined by the CCRA. Furthermore, the Common Criteria and

[1] OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

[2] Commission Implementing Regulation (EU) 2024/482 of 31 January 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) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

the Common Evaluation Methodology standards, together with the accompanying errata, are subject to interpretations done by CCRA that facilitate their implementation and that may be considered by ITSEFs and certification bodies.

(4) Implementing Regulation (EU) 2024/482 does not specify until when an ICT product certification might be based on the previous versions of the Common Criteria and the Common Evaluation Methodology standards. Technical domains and protection profiles listed in Annexes I-III to that Implementing Regulation are based on former versions of ISO/IEC 15408 and 18045. This implementing Regulation therefore specifies under what circumstances the former version of the Common Criteria and the Common Evaluation Methodology still applies and how the transition to the latest version of the international standards will operate. During the transition period, it should be a priority for relevant stakeholders to update the relevant technical domains and protection profiles.

(5) For the purpose of calculating the deadlines referred to in article 1(5) of this Implementing Regulation, the date of issuance of the initial certificate should be understood as the date of issuance of the last certificate for a ICT product or protection profile.

(6) Annex I to Implementing Regulation (EU) 2024/482 lists applicable state-of-the-art documents for the evaluation of ICT products and protection profiles. It should be amended to include updated and new state-of-the-art documents following their endorsement by the European Cybersecurity Certification Group (ECCG), thus ensuring a uniform accreditation of conformity assessment bodies under the EUCC. The accreditation requirements related to the accreditation of ITSEFs should be updated to clarify the application of the criteria of independence and impartiality, and a new state-of-the-art document should be established for the accreditation of certification bodies (CBs).

(7) For new or updated state-of-the-art documents related to the accreditation of ITSEFs, it is appropriate to lay down a transition period for vendors, ITSEFs and certification bodies or accreditation bodies to make the necessary adjustments.

(8) Further corrections to Articles 8, 16, 29 and 44 of Implementing Regulation (EU) 2024/482 contribute to ensuring a uniform wording and clear legal interpretation.

(9) The rules for notifications of the conformity assessment bodies should be established horizontally for all schemes under the cybersecurity certification framework. [Commission Implementing Regulation …/… establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification] covers such notification rules. Therefore, Articles 23 and 24 of Implementing Regulation (EU) 2024/482 should be deleted from the date [Implementing Regulation …/…. establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification] becomes applicable.

(10) Implementing Regulation (EU) 2024/482 should therefore be amended and corrected accordingly.

(11) The measures provided for in this Regulation are in accordance with the opinion of the Committee established by Article 66 of Regulation (EU) 2019/881,

HAS ADOPTED THIS REGULATION:

Article 1

Implementing Regulation (EU) 2024/482 is amended as follows:

(1) In Article 2, points (1) and (2) are replaced by the following:

'(1) 'Common Criteria' means the Common Criteria for Information Technology Security Evaluation, as set out in the ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022, ISO/IEC 15408-5:2022;

(2) 'Common Evaluation Methodology' means the Common Methodology for Information Technology Security Evaluation, as set out in the ISO/IEC 18045:2022;';

(2) Article 3 is replaced by the following:

'Article 3

Evaluation standards

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

   (a) the Common Criteria;

   (b) the Common Evaluation Methodology.

2. Until 31 December 2027 a certificate may be issued under this scheme by applying the standards listed in Article 49(4), points (a) to (d).

3. Until 31 December 2027 an ICT product may be certified against its security target incorporating a protection profile that has been issued under national cybersecurity certification schemes that has applied the standards listed in Article 49(4), points (a) to (d).'

(3) in Chapter IV the following Article is inserted:

'Article 20a

Specification of requirements for accreditation of a conformity assessment body

The accreditation of conformity assessment bodies shall take into account the specification of requirements for accreditation laid down in the state-of-the-art documents listed in point 2(a) of Annex I.'

(4) Articles 23 and 24 are deleted;

(5) In Article 48, the following paragraphs 4 and 5 are added:

'4. State-of-the-art documents shall apply from the date of application of the amending act by which they have been incorporated in Annex I or II to this Regulation.

5. By way of derogation from paragraph 4, accreditation issued according to the state-of-the-art document referred to in point 2(a) of Annex I shall remain valid until *[Publications Office, please insert the date of entry into force of this amending act + 12 months]*.

(6) In Article 49, the following paragraph is added:

'4. When conducting the review referred to in paragraph 3 within two years of the issuance of initial certificate, the following standards may be applied:

(a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2009, ISO/IEC 15408-3:2009, ISO/IEC 15408-4:2009 and ISO/IEC 15408-5:2009;

(b) Common Criteria for Information Technology Security Evaluation, version 3.1, releases 1 through 5, published by the participants of the Agreement on the Recognition of Common Criteria Certificates in the field of IT Security;

(c) ISO/IEC 18045:2008;

(d) Common Methodology for Information Technology Security Evaluation, version 3.1, published by the participants of the Agreement on the Recognition of Common Criteria Certificates in the field of IT Security.

(7) Annex I is replaced by the text in the Annex I to this Regulation.

Article 2

Implementing Regulation (EU) 2024/482 is corrected as follows:

(1) In Article 8:

(a) the title is replaced by the following:

'Information necessary for certification and evaluation';

(b) paragraph 1 is replaced by the following:

'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 and evaluation activities.';

(2) Article 16 is replaced by the following:

'Article 16

Information necessary for certification and evaluation 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 and evaluation activities in a complete and correct form. Article 8(2), (3), (4) and (7) shall apply mutatis mutandis.';

(3) in Article 17, paragraph 1 is deleted;

(4) In Article 29, paragraph 2 is replaced by the following:

'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 or Article 20.';

Article 3

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

(2) Article 1(4) shall apply from [Please insert the date of application of Commission Implementing Regulation …/…. establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council].

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

Done at Brussels,

For the Commission
The President
Ursula von der Leyen