Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-10

Peer assessments

March 2026
Version 1

MINISTERIO DE DEFENSA

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained therein, expressly rejecting any type of implied warranty that may be found related. In no event can the National Cryptologic Center be held liable for direct, indirect, incidental or extraordinary damages arising from the use of the information and software indicated even when it is warned of such possibility.

LEGAL NOTICE

It is strictly prohibited, without the written authorization of the National Cryptologic Center, under the sanctions established by law, the partial or total reproduction of this document by any means or procedure, including reprography and computer processing, and the distribution of copies thereof by public rent or loan.

COURTESY TRANSLATION NOTICE

This document is provided solely as a courtesy translation. This translation has been generated using automated tools with minimal human supervision. In the event of any discrepancy, ambiguity, or conflict between this translation and the original Spanish version, the original Spanish version text shall prevail and shall be deemed the only official, authoritative, and legally binding version.

VERSION CONTROL

Version	Comments
1.0	Initial version

INDEX

1. INTRODUCTION

1. This document lays down the policy and rules for peer assessments applicable to certification bodies issuing **EUCC** certificates at the 'high' assurance level, as well as to associated assessment laboratories (**ITSEFs**), in accordance with the requirements of **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on the certification of cybersecurity of information and communication technologies** (hereinafter **CSA**) and **Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down detailed rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European cybersecurity certification scheme based on the Common Criteria (EUCC)**.

2. Certification Bodies (**CBs)** authorised to issue **EUCC** certificates at the high assurance level, as well as associated ITSEFs participating in the relevant assessment activities, shall regularly undergo peer assessments in accordance with [**CSA**] and the **EUCC** scheme. Successful completion of these assessments is a prerequisite for maintaining authorization to operate at the high level. The objective of these assessments is to verify that the evaluated **CAB** complies with the applicable requirements of the scheme, ensuring that all authorized bodies work in a harmonized manner, apply consistent criteria and produce certificates of the same quality level.

2. POLITICS

4. The National Cybersecurity Certification Authority (**NCCA**) is committed to facilitating peer assessments under the **EUCC** scheme for Certification Bodies (**CBs**) issuing **EUCC** certificates at the high assurance level and, where appropriate, for associated **ITSEFs**, in accordance with Articles 45 to 47 of [**EUCC**] and the peer assessments mechanism established within the European Cybersecurity Certification Group (**ECCG**).

5. This commitment is reflected in:

   a) **Resource Planning: NCCA** Unit Head **(JAN)** ensures that there are a sufficient number of **NCCA** technical staff **(TA)** trained and available to support the planning, coordination and implementation of peer assessments, including timely provision of information and on-site support to peer assessment teams.

   b) **Collaboration:** The **JAN** maintains close cooperation with the evaluated Certification Bodies (**CBs**) and their associated **ITSEFs**, as well as with the **ECCG** and **ENISA**, to ensure that assessments are conducted in an effective, harmonised and impartial manner.

   c) **Independence and separation of functions:** When the National Cryptologic Center (**CCN**) also acts as a Certification Body (**CB**) and as the National Cybersecurity Certification Authority (**NCCA**), it shall ensure a strict separation between its supervisory and coordinating role in peer assessments and any operational role in certification activities, thereby ensuring impartiality.

   d) **Information security and confidentiality:** the **JAN** will impose security, confidentiality and personal data protection measures for all information relating to peer assessments, using the National Cybersecurity Certification Authority information system **(SGA)** and secure exchange channels agreed with the peer assessment team.

   e) **Transparency and procedural guarantees:** The **JAN** shall ensure that assessed Certification Bodies (**CBs**) are informed of the expectations, timeframes and acceptance criteria, while complying with the schedule and procedures of the **ECCG**. The relevant decisions shall be formalized by the signature of the Secretary of State–Director of the CCN (**SED**).

6. Assignment of responsibilities:

   a) The Deputy Director General of the **CCN** (**SGCCN**) signs formal letters, confidentiality commitments and final communications addressed to evaluated Certification Bodies (**CBs**) and the **ECCG**."

   b) The **JAN** is informed of the timetable of peer assessments, major milestones and results.

c) The **JAN** oversees the allocation of resources, the acceptance of files submitted for evaluation, and the responses to findings, and coordinates all actions related to peer assessments.

d) The **TA**, designated by the **JAN**, leads the specific coordination of the peer assessment team, acts as the point of contact with the **ECCG** and Certification Bodies (**CBs**), validates the technical scope and suitability of the files, and organises on-site logistics.

e) The **TA** is responsible for the collection of evidence, document control, the secure transfer of information, the organisation of meetings, and the maintenance of records in the information system of the National Cybersecurity Certification Authority (**SGA**).

3. PEER ASSESSMENTS STANDARDS

7. Peer assessments shall be carried out exclusively in accordance with the procedures adopted within the **ECCG**, which may define the composition of the team, the phases, the re-use of evidence and the preparation of reports, as set out in Articles 45 to 47 and Annex VI to [**EUCC**]. The **TA** shall ensure alignment with the latest decisions of the **ECCG** and shall inform the evaluated Certification Body (**CB**) of any instructions defining the scope that may affect the assessment.

8. Once the timetable for peer assessments has been defined by the **ECCG** in coordination with the **NCCA**, the evaluated Certification Body (**CB**) shall submit an assessment plan to the **NCCA** for approval. The plan shall include at least:

    a) The scope and objectives of the assessment as communicated by the (including technical areas and, where appropriate, **ITSEF** partners).

    b) A proposal for candidate certification decisions and the underlying evaluation dossiers (certification or evaluation dossiers) representative of the scope to be sampled by the peer assessment team, together with a justification for such representativeness.

    c) The classification and confidentiality marking of each element of the file, data minimisation measures (e.g. deletions or exclusive on-site access) and secure handling measures.

    d) Proposed deadlines, access restrictions (e.g. laboratory standards) and designated contact points.

    e) Declarations of conflicts of interest of staff who will interact with the peer assessment team.

9. The **TA** will review the peer assessment plan to verify its integrity, technical suitability and compliance with security and confidentiality requirements. The **JAN** shall approve it or request any amendments as appropriate. The **NCCA** is committed to facilitating peer assessment and will collaborate with the **CB** evaluated to agree on a plan that enables an effective assessment while protecting sensitive, confidential information and personal data. Where particularly sensitive content is involved, the **TA** may authorise on-site access only, the removal of non-essential details, or limited sampling, provided that such measures do not undermine the objectives of the assessment.

3.1 PREPARATION AND COORDINATION WITH THE ECCG

10. Upon receipt of the timetable established by the **ECCG**, the **NCCA** shall:

    a) record the plan in the **SGA** and notify the evaluated Certification Body (**CB**) and, where appropriate, the affected **ITSEFs**;

    b) designate a coordination team composed of **TAs** and appoint a person responsible for the assessment;

c) confirm with the peer assessment team the safe channels and information exchange procedures;

d) align the internal timetable with the **ECCG** milestones and communicate any restrictions or rules applicable to visits;

e) It shall provide the **ECCG** with the assessment plan proposed by the **CB**, in coordination with the **ITSEFs.**

3.2 IMPLEMENTATION SUPPORT AND PROVISION OF INFORMATION

11. During the preparatory and on-site visit phases, the **TA**:

a) organize interviews with **CB** staff evaluated and, where appropriate, with the **ITSEFs**;

b) facilitate laboratory visits and demonstrations where technical areas fall within the scope of the assessment;

c) it shall ensure that all information is treated in accordance with the agreed confidentiality measures and is recorded in the **SGA**.

12. The **TA** will ensure that the peer assessment team is promptly informed of any substantial changes (e.g. in personnel, processes or scope) occurring in the **CB** evaluated or at related **ITSEFs** during the assessment period.

3.3 RESULTS, REPORT MANAGEMENT AND FOLLOW-UP

13. Upon receipt of the draft peer assessment report, the **TA** shall coordinate the preparation of the response by the evaluated Certification Body (**CB**), including the handling of deviations and, where appropriate, the corrective action plan, ensuring its submission within the deadlines set by the peer assessment team. The **JAN** shall approve the response before it is sent. The **SGCCN** shall sign, where appropriate, formal letters addressed to the **ECCG**.

14. When the **ECCG** delivers its final opinion, the **TA** shall record the result (positive or negative, list of non-conformities, deadlines) in the **SGA** and , where appropriate, shall activate:

a) the follow-up of corrective actions by the **CB** evaluated and, where appropriate, **ITSEF**;

b) coordination with **ENAC** where the results may affect the accreditation;

c) review of the status of the authorization pursuant to '*ANCC-PO-03, Authorisation of Conformity Assessment Bodies*';

d) any monitoring or control activity in accordance with the *'ANCC-PO-07, Compliance Monitoring'*.

15. Aspects relating to publication by **ENISA** shall be supported by providing, where necessary, refined versions of the documentation, ensuring that sensitive, personal or proprietary information is deleted in accordance with Article 47(6) of [**EUCC**].

3.4 CONFIDENTIALITY, SECURITY AND RECORDS

16. **JAN** shall ensure that all information relating to peer assessments is treated under appropriate confidentiality commitments. The **TA** shall define the processing instructions (classification, access control, retention and destruction periods) and require that the exchanges of records be carried out by mutually agreed secure means. The **TA** will maintain complete records of communications, referrals, attendance and access to ensure traceability and enable subsequent audits.

3.5 REUSE OF EVIDENCE

17. The **TA** may propose to the peer assessment team the reuse of recent evidence from peer assessments (not earlier than five years) or equivalent procedures, accurately identifying their origin, scope and procedures used, so that the peer assessment report can specify the results reused with or without additional evaluation.

4. REFERENCES

ACCCB	Accreditation of certification bodies for EUCC (https://certification.enisa.europa.eu/publications/accreditation-cbs-eucc_en)
ACCITSEF	Accreditation of ITSEF for EUCC (https://certification.enisa.europa.eu/publications/accreditation-itsefs-eucc_en)
AUTH	Authorisation of certification bodies and ITSEF for the EUCC scheme (https://certification.enisa.europa.eu/publications/eucc-guidelines-authorisation-cabs_en)
CSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies, and repealing Regulation (EU) No 526/2013 (http://data.europa.eu/eli/reg/2019/881/oj)
CSA-E1	Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services (http://data.europa.eu/eli/reg/2025/37/oj)
EUCC	Implementing Regulation (EU) 2024/482 of the 31 January 2024 Commission laying down detailed rules for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European criteria-based cybersecurity certification scheme common (http://data.europa.eu/eli/reg_impl/2024/482/oj)
LPAC	Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (https://www.boe.es/eli/es/l/2015/10/01/39/con)
NOTIF	Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 laying down the circumstances, formats and procedures for notification in accordance with Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies (http://data.europa.eu/eli/reg_impl/2024/3143/oj)
VULMD	Guidelines on Vulnerability Management and Disclosure (https://certification.enisa.europa.eu/publications/eucc-guidelines-vulnerability-management-and-disclosure-and-eccg-opinion_en)

5. ACRONYMS

NCCA	National Cybersecurity Certification Authority
CCN	National Cryptologic Center
EC	European Commission
CSIRT	Computer Security Incident Response Teams
ENAC	National Accreditation Body
ENISA	European Union Agency for Cybersecurity
EUCC	European cybersecurity certification scheme based on common criteria
ECCG	European Cybersecurity Certification Group
ITSEF	Information Technology Security Evaluation Facility
JAN	Head of the NCCA unit
CB	Certification Body
CAB	Conformity assessment body
CSA	Cybersecurity Regulations
SED	Secretary of State Director of the CCN
SGA	Information System of the National Cybersecurity Certification Authority
TA	Technical staff attached to the NCCA
ICT	Information and Communication Technologies
EU	European Union
VPA	Voluntary periodic audits
WNCCA	Website of the National Cybersecurity Certification Authority