Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-07

Compliance monitoring

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 procedure defines the way in which the National Certification Authority **(NCCA)** monitors and ensures compliance by certified **ICT** products and services with its **ICT** processes, **European Cybersecurity Certification Scheme (EUCC)** and Conformity Assessment Bodies **(CABs)**, including **CBs** and **ITSEFs**, of the requirements laid down in European cybersecurity certification schemes. It covers ongoing monitoring mechanisms, audits and investigations, sampling of certificates, processing of complaints and actions taken in cases of non-compliance, as provided for in **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**) **[CSA]** and on the **EUCC** scheme**.**

2. SUPERVISION ACTIVITIES

2. The **NCCA** takes a continuous and risk-based approach to supervision compliance with all European cybersecurity certificates issued. This approach covers the supervision of certified **ICT** products and services, related **ICT** processes, **EUCC** certificate holders and the activities of authorized **CABs** (including **CBs** and associated **ITSEF**). The head of the **NCCA** unit **(JAN)** will lead the supervision activities. Previously assigned **NCCA** technical staff **(TA)** will be responsible for the supervision tasks specific to each scheme and will support the collection and analysis of information. The following main sources and activities feed into **NCCA** supervision:

   a) **Exchange of information**. Regular flows of information from relevant organizations support oversight. The **NCCA** collects inputs from **CBs (**e.g. periodic reports or notifications), from the National Certification Body (**ENAC)** (in relation to accreditation status or incidents) and from other market surveillance authorities or European bodies (such as **ENISA** or **ECCG**), to keep it informed about factors that may affect compliance.

   b) **Audits and inspections**. The **NCCA** conducts audits of **CABs** and, where necessary, inspections related to specific certificates. These audits can be scheduled periodically or initiated on the basis of risk indicators. They verify that certification activities and certified products continue to meet applicable requirements. The **TA** prepares and executes audits, both *on-site* and remotely.

   c) **Sampling.** The **NCCA** conducts proactive checks on a sample of certificates issued each year (described in the sampling program below). This risk-based sampling of certified **ICT** products helps to systematically identify possible undetected non-conformities.

   d) **Claims and Incident Reports**. The **NCCA** considers complaints, vulnerability reports or other incident information from certificate holders, users, security investigators or other stakeholders. These resources are recorded and analyzed as potential indicators of non-compliance and may lead to further investigations where appropriate (see *ANCC-PO-05, Handling of complaints*).

   e) **Threat tracking**. The **NCCA** monitors the evolution of the cybersecurity threat landscape to ensure that the level of assurance provided by existing certificates remains valid. Emerging threats, vulnerabilities and technological changes that may undermine certified security assurances are tracked. Where appropriate, the **NCCA** assesses whether certified products require reassessment or additional measures (in coordination with the issuing **CB**), in accordance with the vulnerability management procedures.

3. AUDITS AND INVESTIGATIONS

3. **NCCA** conducts audits and compliance investigations to verify, where necessary, compliance with certification requirements by **CABs**. These actions may be initiated as part of the planned monitoring program or triggered by specific concerns (e.g. indications of possible non-conformity, complaints or results of the sampling program). Audits may include documentary reviews, on-site or remote evaluations and, in certain cases, visits to the premises of certificate holders, using its authority of access to premises in accordance with applicable legal procedures. All investigations are carried out in compliance with Union law and national law, including the requirements of the administrative procedure established in **Law 39/2015, of 1 October, of the Common Administrative Procedure of Public Administrations [LPAC]**.

4. Normally, the **TA** performs routine audit and fact-finding tasks. The **JAN** approves the opening of any significant investigation or extraordinary audit, while keeping it informed of the main ongoing compliance records. Where necessary, the **NCCA** may involve external experts or cooperate with **ENAC** (e.g. through joint evaluations with accreditation evaluators) to strengthen the effectiveness of the investigation.

5. Where an investigation concerns a particular certified **ICT** product or its holder, the **NCCA** shall inform the holder of the certificate, the relevant **CB** and, where appropriate, the **ITSEF** concerned that the investigation is ongoing. This communication ensures transparency and facilitates the collaboration of these entities. If the investigation has cross-border implications (e.g. in the case of a product certified by a **CB** in another Member State), the **NCCA** will coordinate with the other national cybersecurity certification authority to cooperate in the investigation or share its results.

6. All non-conformities identified during audits, inspections or incident investigations will be systematically managed by **NCCA**. The process will include:

    a) **Registration:** The **TA** shall record each non-conformity in the **SGA**, including description, severity and date of identification.

    b) **Notification:** The **JAN** (or the **TA** on its behalf) shall formally notify the **CAB** of the non-conformity, indicating the corrective measures required and the deadline for its resolution.

    c) **Correction and Verification:** The **CAB** will implement corrective measures. The **TA** will monitor progress and verify that non-conformity has been effectively resolved (including, where appropriate, a follow-up review or inspection).

    d) **Closing and scaling:** The **JAN** will review the resolution. If you agree, you will formally close the non-conformity in the information system of the National Cybersecurity Certification Authority **(SGA)**. If it is not corrected by the deadline or is recurring, the **JAN** will escalate the matter, and may issue warnings, impose operational restrictions or recommend initiating the suspension or withdrawal of the **CAB** authorization, in accordance with the requirements of the applicable administrative procedure.

4. SAMPLING OF CERTIFICATES

7. The **NCCA** applies an annual sampling program to proactively assess the continued compliance of certified products. Each year, at least **4%** of all valid **EUCC** certificates are selected for review, as required by the scheme. The selection of this sample is coordinated by the **TA** and is based on a risk assessment carried out in cooperation with other relevant market surveillance authorities. This approach ensures that sampling focuses on certificates that are most likely to provide significant conclusions (e.g. those associated with high-risk profiles).

8. The **NCCA** can set a follow-up sampling level at two levels, based on:

   - **Monitoring:** Review limited to the documentation issued by the **CB**, to verify documentary consistency, conformity with the formal requirements of the scheme and absence of initial warning signals.

   - **Review:** Comprehensive review that includes both the certification part and the evaluation part (technical documentation, evidence, ITSEF reports, testing activities, traceability of requirements, vulnerability analysis, etc.). This type of sampling may reuse the activities provided for in the procedure '*ANCC-PO-06 Authorisation and supervision procedure for the use of the CCRA mark in the EUCC scheme*'.

9. Objective criteria are used to select the sample of certified **ICT** products to be reviewed. Factors considered include product category, assurance level, individual certificate holders, issuing **CB** and any **ITSEF** involved, as well as other information available to the **NCCA** (such as known security issues or information provided by market surveillance authorities). The **TA** records in the **SGA** the justification and risk factors for each selection.

10. Once the annual sample has been determined, the **NCCA** notifies the holders of the certificates concerned of the selection. For each selected **ICT** product, its **EUCC** certificate holder is informed of the reason for the selection.

11. For each **EUCC** certificate, the assigned **TA** shall confirm that the certificate and its certification report conform to the prescribed format and include all necessary elements marked by **[EUCC]** (e.g. Name and version of the product evaluated, assurance level, validity period, references to Protection Profiles or applied standards, certification body and, where appropriate, installation of the evaluated configuration) and that the issuing **CB** is accredited by the **ENAC** and duly authorized or notified for the **EUCC** scheme. In the case of an **EU** self-assessment of conformity under the **CSA**, **TA** shall verify that the **EU** declaration of conformity is duly signed by the responsible party and that the accompanying technical documentation is sufficient to support the declaration of conformity.

12. The **NCCA** analyzes the results of each sampling review to determine whether there is any non-conformity, procedural deficiency or security weakness. If it is considered that a sampled product may not meet the requirements, the case may be escalated to a full

investigation or other appropriate measures under this procedure (e.g. request for additional information by request to **CB** or **ITSEF**).

13. All sampling activities and their results are duly recorded in the **SGA**, which provides the register on risk assessment, selection criteria, the level of sampling applied and the results obtained associated with monitoring.

14. The conclusions drawn from the sampling program are integrated into the improvement of the overall supervision strategy and may lead to adjustments in risk criteria, sampling frequency or guidance provided to certification bodies.

5. MANAGEMENT OF COMPLAINTS RELATED TO COMPLIANCE

15. The **NCCA** maintains channels (e.g. through the authority's website (**WNCCA**) or designated contact points) for any party to submit complaints or reports concerning alleged non-compliance. Such complaints may relate to problems with certified **ICT** products, certificate holders or **CAB's** actions. Upon receipt of a complaint, the **TA** registers it in the **SGA** and conducts an initial review to assess its credibility and relevance.

16. If the complaint provides credible indications of non-compliance, **NCCA** initiates appropriate follow-up actions. These may include requesting additional information from the parties concerned (the relevant **CB**, the **ITSEF** involved or the certificate holder), as well as initiating an investigation or ad hoc audit focusing on the issues raised. In some cases, the subject matter of the complaints may be included in the next sampling cycle for more detailed review. Throughout the process, the complainant is informed, to the extent possible, of the status and outcome of his complaint. The processing of complaints is in accordance with the principles and time limits of the applicable procedure (see *ANCC-PO-05 Handling of complaints*).

6. ACTIONS IN THE EVENT OF NON-COMPLIANCE

17. Where non-conformities or infringements are identified by the supervisory activities described above, the **NCCA** takes appropriate measures to address them and enforce certification obligations. The response is tailored to the nature of the problem (whether it relates to a certified **ICT** product, a certificate holder or a **CAB**) and to the severity of its impact on cybersecurity. All enforcement actions are carried out in accordance with national legal requirements for administrative procedure (e.g. guarantees and steps provided for in **[LPAC]**), which includes providing the entities concerned with the opportunity to be heard and to correct deficiencies, where possible, before a final decision is taken.

18. If it is found that a certified **ICT** product does not comply with the requirements of its **EUCC** certificate or the scheme, the **NCCA**, in coordination with the issuing **CB**, shall ensure that corrective action is taken. The certificate holder may receive instructions (through the certification body) to remedy identified vulnerabilities or non-conformities within a specified period. The certification body shall suspend the certificate if the issue is serious or is not remedied promptly. In cases of serious non-conformity, or where remediation attempts fail, the certificate shall be withdrawn. In accordance with the **[CSA],** the **NCCA** is empowered to withdraw a European cybersecurity certificate itself, including those issued by a **CB**, in order to quickly protect the public, where necessary.

19. For certificates that are suspended as a result of identified problems, the **JAN** may authorize extensions of the suspension period (not exceeding one year in total) in duly justified circumstances, to give the holder additional time to implement corrective measures. If, after that period, the problem has not been properly resolved, the suspension will become definitive withdrawal of the certificate, unless there are compelling legal grounds for deciding otherwise.

20. Where a certificate holder fails to comply with its obligations under the scheme (e.g. failure to apply the required security updates or misuse of the certificate in its commercial communication), the **NCCA** may order the relevant **CB** to impose additional conditions, restrict the scope of the certificate or suspend or withdraw it. The **TA** shall prepare an assessment of the case, including non-fulfilled obligations, potential impact and proposed remedial measures, for consideration by **JAN**.

21. In the event of non-compliance by a **CAB**, the **NCCA** shall assess whether the identified deficiencies challenge the reliability of conformity assessment activities. Depending on the severity, the measures may include the imposition of mandatory corrective actions, the suspension or withdrawal of the **CAB** authorization to operate under the European schemes, as well as coordination with **ENAC** to review the accreditation of the body. The **NCCA** shall also assess the impact on certificates issued by the **CAB** and, where appropriate, initiate the actions provided for in this procedure (suspension, reassessment or withdrawal of certificates).

22. All significant implementing decisions – such as suspension or withdrawal of certificates, suspension or withdrawal of the authorization of a **CAB** – are formally taken by **NCCA**'s

governing bodies. The **JAN** examines the conclusions of the case proposed by the **TA** and will forward the proposed decision to the Secretary of State Director of the **CCN (SED)**, who, if appropriate, may sign the decision after evaluation. Throughout the implementation process, the **TA** supports the preparation of resolutions, the communication of decisions to affected parties and the implementation of follow-up measures (e.g. ensuring that withdrawn certificates are removed from relevant public listings).

7. COMMUNICATION AND CONSERVATION OF INFORMATION

23. The **NCCA** ensures that the results of compliance monitoring activities and enforcement actions are communicated to the relevant parties and that all stages are properly documented. Where an investigation or enforcement action has cross-border implications (e.g. where it concerns a certificate issued by a **CB** from another Member State or products available in several Member States), the **NCCA** shall inform the other national cybersecurity certification authorities concerned. In accordance with the obligations of the **EUCC** scheme, the **NCCA** shall also report to the European Cybersecurity Certification Group (**ECCG)** on these cross-border cases and the results of investigations, thus facilitating cooperation and information exchange at European level.

24. Where the non-conformity or security problem identified may be relevant for the purposes of other Union legislation (e.g. sectoral product legislation), the **NCCA** shall notify the relevant information to the competent national authorities, including market surveillance authorities, as appropriate. The **NCCA** shall cooperate with those authorities to ensure that the measures taken are coherent and properly coordinated, avoiding duplication and gaps in protection.

25. All compliance monitoring activities and their results are documented in the **SGA**. This includes audit reports, findings of investigations, decisions on the status of certificates or authorization of **CAB** and correspondence with the entities involved. Key actions (e.g. suspension or withdrawal of a certificate, or the imposition of sanctions on a **CAB**) are also reflected on the National Cybersecurity Certification Authority website where applicable, updating the public listings of certified products or publishing notices about changes in the validity of certificates. These records and results ensure traceability and accountability in each case and are integrated into the **NCCA's** periodic reporting obligations. In particular, aggregate information on compliance monitoring (such as the number of audits carried out, certificates withdrawn and other relevant statistics and observations) is included in the annual summary report submitted to **ENISA** and the **ECCG** (see *ANCC-PO-01 Annual Report*), thus contributing to the monitoring and improvement of the European cybersecurity certification framework.

8. 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)

9. 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