	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	1 of 21

1. Purpose

This document defines the internal process followed by [Certification Body] for the assessment of ICT products under the EUCC scheme.

2. Scope

This document covers the assessment process for:

- EUCC Certification of ICT products (hardware, software, or components)
- Assurance levels Substantial and High
- Interaction between the [Certification Body] and the following parties:
 - o External IT Evaluation Facilities (ITSEF)
 - o ICT product manufacturers referred to in the document as vendors
 - o National Accreditation Body (NAB)
 - o National Cybersecurity Certification Authority (NCCA)


The following normative documents were considered:

- The EU Cybersecurity Act, Regulation (EU) 2019/881
- The Implementing Regulation (EU) 2024/482 (EUCC)
- ISO/IEC 15408 series
- ISO/IEC 18045
- Applicable ENISA guidance

3. Roles and Responsibilities

Role	Responsibility
Vendor	<ul style="list-style-type: none"> - Defines the Target of Evaluation (TOE) - Provides evaluation evidence - Responds to findings and remediation requests - Maintains vulnerability handling during certificate validity
Certification Body (CB)	<ul style="list-style-type: none"> - Overall conformity with EUCC requirements - Independent technical review - Independent certification decision-making - Issuance, maintenance, suspension, and withdrawal of EUCC certificates - Oversight of evaluation activities performed by the ITSEF, including follow-up of significant findings and vulnerability-related issues where applicable.




	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	2 of 21	

<p>Evaluation facility (ITSEF)</p>	<ul style="list-style-type: none"> - The selected ITSEF shall hold the required accreditation and, where applicable, authorisation for the proposed evaluation. The CB verifies and records that status and confirms that the ITSEF meets the applicable contractual and scheme requirements. - Performs technical and documentary evaluation activities under the EUCC scheme and the applicable Common Criteria / Common Evaluation Methodology requirements. - Produces the Evaluation Technical Report (ETR) and supports the Certification Body in the resolution of technical issues and vulnerability-related follow-up where applicable.
<p>National Accreditation Body (NAB)</p>	<ul style="list-style-type: none"> - Accredits ITSEFs and, where applicable under the relevant framework, Certification Bodies against the applicable accreditation requirements. - Issues and maintains accreditation status and scope information used by the Certification Body when verifying eligibility for EUCC activities.
<p>National Cybersecurity Certification Authority (NCCA)</p>	<ul style="list-style-type: none"> - Authorises Certification Bodies and ITSEFs where required under the applicable EUCC and national framework, including for assurance level High where applicable. - Exercises oversight of EUCC certification activities, may request information and records, and may issue corrective measures within its competence. - Receives required notifications and reports concerning authorisation, certification status, serious vulnerabilities, and other reportable events under the applicable framework.

Certification decisions are taken by personnel independent from the evaluation activities. The technical reviewer shall be assigned based on competence in the relevant technology area, assurance requirements, and Common Criteria methodology, and shall remain independent from the evaluation activities, the vendor, and the final certification decision. Any conflict of interest involving the evaluation facility or personnel is identified, documented, and managed in accordance with the Certification Body's impartiality procedures.



	<h1 style="text-align: center;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	3 of 21

4. Process Overview


- Application review
- Engagement with ITSEF and evaluation scoping
- Security Target (ST) review
- Oversight of evaluation activities and review of the Evaluation Technical Report (ETR)
- EUCC certificate issuance and publication
- Maintenance of Certification
- Surveillance activities under the EUCC
- Termination, suspension or withdrawal of certification
- Complaints and appeals
- Interaction with the NCCA

5. Detailed Process Description

5.1 Application review

The application review is carried out in accordance with procedure SM-01-02 and focuses on confirming that the application package is complete, that the requested certification scope and assurance level are identified, that the necessary contractual, administrative, and procedural prerequisites are in place, and that the required input documentation for the scoped assessment exists before the evaluation is initiated. At this stage, the review is limited to the presence and apparent completeness of the documentation set required for the requested scope; substantive technical review of that content is performed in the later evaluation and review stages.

- Identification of the ICT product, Target of Evaluation (TOE), requested assurance level, certification scope, and any claimed Protection Profile conformance.
- Security Target and any related scope-defining or certification-basis documents required to initiate the assessment.
- Input documentation supporting the applicable assurance class work for the scoped assessment, including, where relevant, ADV, AGD, ALC, and ATE evidence packages or their identified source documents.
- Assurance continuity, maintenance, or change-related inputs where the application concerns re-certification, maintenance, or another continuity-related activity, including ACO-related impact information where applicable.
- Vulnerability handling, remediation, and supporting lifecycle documentation where required by the requested scope, assurance level, or product type.

	<h1 style="text-align: center;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	4 of 21

- Any additional documentation required by the applicable EUCC scheme requirements, the selected technical domain, the chosen evaluation techniques, or other scope-specific conditions of the assessment.

If required documentation is missing, too incomplete for the scoped assessment to be properly initiated or not made available within the timeframe requested by the Certification Body, the application may be placed on hold pending completion, returned for completion, or rejected as inadmissible with documented justification.

At the end of this stage, the ICT product is registered within the system. All related documentation, including the completed application form, completed application review form, and the signed contract or, if applicable, the rejection letter, is formally recorded in the system. This ensures that all necessary materials are properly documented as part of the application review process.


5.2 Engagement with ITSEF and evaluation scoping

During this stage, the CB works with the selected ITSEF to develop the evaluation plan. The plan is prepared in line with the EUCC requirements and reflects the approved certification scope, assurance level, and the product-specific evaluation parameters established during the application process.

The CB verifies that the selected ITSEF holds the required accreditation under the applicable EUCC requirements for ITSEFs, including ISO/IEC 17025 and the relevant EUCC state-of-the-art accreditation requirements, and that its accreditation scope covers the relevant technology domain, evaluation techniques, and assurance activities for the proposed evaluation. In addition, the ITSEF shall demonstrate competence in Common Criteria and the Common Evaluation Methodology, the availability of suitably qualified personnel and secure facilities, and the organisational measures necessary to ensure confidentiality, impartiality, and the validity of evaluation results.

Where the proposed evaluation falls within a technical domain or assurance context for which additional authorisation is required under the applicable EUCC and national framework, the CB verifies that such authorisation is in place before the evaluation proceeds.

Before confirming the ITSEF for an evaluation, the CB verifies the current accreditation status against the applicable EUCC state-of-the-art accreditation document for ITSEFs and any relevant domain-specific state-of-the-art documents. The verification includes review of the formal accreditation certificate or statement issued by the competent National Accreditation Body, the published or provided accreditation scope, publicly

	<h1 style="text-align: center;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	5 of 21

available accreditation status information or direct confirmation where needed, and any additional supporting evidence necessary for the proposed evaluation.


The CB confirms that the accreditation remains valid, that the scope matches the product type, technology area, evaluation techniques, and requested assurance activities, and that any limitations, conditions, or pending scope extensions are understood and acceptable for the proposed evaluation. Where additional authorisation is required, the CB also reviews the relevant authorisation evidence and records the outcome of the verification in the case file before evaluation scoping is finalised.

Where the applicable framework requires notification or authorisation in addition to accreditation, the CB treats valid accreditation status and the relevant notification or authorisation status as preconditions for confirming the selected conformity assessment body for the proposed activity. The outcome of these checks is recorded in the case file before evaluation or certification activities proceed.

5.2.1 NCCA authorisation

Where required by the applicable EUCC and national framework, the Certification Body verifies that the selected ITSEF, and where relevant the Certification Body itself, hold the necessary authorisation from the National Cybersecurity Certification Authority (NCCA) before evaluation activities or certification activities proceed. This authorisation requirement applies in addition to accreditation and shall be treated as a mandatory precondition where the applicable framework makes such authorisation necessary, including for assurance level High activities where applicable.

- **Applicability:** The CB determines, before evaluation scoping is finalised, whether NCCA authorisation is required for the proposed evaluation or certification activity under the applicable assurance level, technical domain, product type, or national implementation rules.
- **Verification:** Where authorisation is required, the CB verifies that the authorisation is current, issued by the competent NCCA, and applicable to the specific activity, assurance context, and technical scope concerned.
- **Evidence reviewed:** The CB reviews the formal authorisation statement, licence, listing, or other official evidence made available by the NCCA or other authoritative source, together with any stated scope limitations, conditions, expiry information, or linked oversight requirements.
- **Records and decision impact:** The outcome of the authorisation verification is recorded in the case file. Where required authorisation is absent, expired, restricted in a manner that prevents the proposed activity, or otherwise unclear,

	<h1 style="text-align: center;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	6 of 21

the CB shall not confirm the ITSEF or proceed with the affected evaluation or certification activity until the issue is resolved.

5.3 Security Target Review


The CB performs a dedicated review of the Security Target (ST) before substantive evaluation activities proceed. This review confirms that the ST is complete, internally consistent, aligned with the requested certification scope and assurance level, and sufficiently precise to serve as the basis for evaluation under the EUCC scheme and ISO/IEC 18045.

- **ST completeness:** The ST is reviewed to confirm that the TOE description, operational environment, assumptions, threats, organisational security policies, security objectives, SFRs, SARs, and supporting rationale are present and sufficiently defined for the selected assurance level.
- **PP conformance:** Where PP conformance is claimed, the Certification Body verifies that the referenced PP version is identified, applicable under the EUCC scheme, and correctly reflected in the ST, including any justified interpretations, refinements, or deviations.
- **Traceability review:** The review confirms clear traceability between the TOE security problem definition, security objectives, SFRs, SARs, and any applicable PP requirements, so that all claims made in the ST can be followed through the evaluation activities and conclusions.
- **Acceptance criteria:** The ST is accepted when it is complete, coherent, and evaluable against the applicable ISO/IEC 18045 work units, reflects any claimed PP conformance, is aligned with the requested certification scope and assurance level, and contains no material ambiguities or unresolved inconsistencies. Where issues are identified, the Certification Body requests clarification or revision before the evaluation proceeds.

5.4 Oversight of evaluation activities and review of Evaluation Technical Report (ETR)

During the evaluation, the CB may request evaluation status reports from the ITSEF to maintain oversight of the process and confirm continued conformity with the applicable EUCC requirements. On receipt of the ETR, the CB reviews the report to ensure the following:

- Completeness of information provided
- Traceability to security target claims
- Clear conclusions against SFR and SAR

	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	7 of 21

- No unresolved findings remain
- Any residual risks are explicitly documented

If deficiencies are identified, the CB requests clarification from the ITSEF or corrective action from the vendor through the ITSEF.


The outputs of this review and its conclusion are documented in the applicable controlled certification records. Certification decisions are made taking the following factors into account:

- Adherence to applicable processes, procedures, and contractual requirements
- Recommendation of the technical reviewer

5.4.1 Evaluation non-conformities

For the purposes of this procedure, an evaluation non-conformity is any deficiency, inconsistency, omission, unresolved issue, or departure from applicable requirements identified during evaluation oversight, review of evaluation outputs, or review of the Evaluation Technical Report (ETR), which prevents the Certification Body from concluding that the evaluation results are complete, coherent, and adequate to support certification.

- **Identification and recording:** Evaluation non-conformities may arise from deficiencies in evaluation evidence, gaps in traceability to the Security Target, unresolved findings, incomplete work-unit coverage, inconsistencies between evaluation outputs, or departures from approved scope or procedure. Each non-conformity shall be recorded with sufficient detail to support follow-up and decision-making.
- **Classification:** The Certification Body classifies evaluation non-conformities according to their significance and impact on certification. Minor non-conformities are those that can be corrected without affecting the overall validity of the evaluation conclusions. Major non-conformities are those that materially affect the completeness, correctness, traceability, or reliability of the evaluation results or indicate that applicable requirements have not been met.
- **Handling and correction:** The Certification Body requests clarification, correction, or additional evidence through the ITSEF, and where necessary through the vendor via the ITSEF. The non-conformity remains open until the requested response has been received and reviewed and the Certification Body is satisfied that the issue has been adequately addressed.
- **Closure evidence:** Closure shall be supported by revised evaluation outputs, updated evidence, corrected traceability, or other documented justification

	<h1 style="text-align: center;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	8 of 21

demonstrating that the non-conformity no longer affects the basis for certification.


- **Escalation:** Where a major non-conformity remains unresolved, where repeated deficiencies indicate a broader failure of evaluation control, or where the issue affects the reliability of the evaluation process, the Certification Body may suspend progression of the assessment, require additional evaluation work, narrow the certification scope, or refuse certification with documented justification.
- **Impact on certification decision:** No positive certification decision shall be taken while material evaluation non-conformities remain open. The status and disposition of non-conformities shall be considered as part of the technical review and the certification decision record.

5.5 EUCC Certificate Issuance and Publication

For EUCC certificates, the certificate content shall include, as a minimum, the information required by Annex VII of Implementing Regulation (EU) 2024/482, in addition to the general certificate requirements defined in SM-01-01.

- A unique identifier established by the Certification Body issuing the certificate.
- Information related to the certified ICT product or certified protection profile and the holder of the certificate, including: the name of the ICT product or protection profile and, where applicable, of the Target of Evaluation (TOE); the type of ICT product or protection profile and, where applicable, of the TOE; the version of the ICT product or protection profile; the name, address and contact information of the holder of the certificate; and the link to the website of the holder of the certificate containing the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881.
- Information related to the evaluation and certification of the ICT product or protection profile, including: the name, address and contact information of the Certification Body that issued the certificate; the applicable assurance level; the date of issuance of the certificate; and the end date of the validity period of the certificate.
- Any additional information required by the current version of Annex VII of Implementing Regulation (EU) 2024/482 shall be included in the certificate template maintained under SM-01-01.

The issued certificate shall state the period of validity of the certificate, including the date of issuance and the end date of the validity period, in accordance with the applicable EUCC requirements and the certification decision for the specific case.

	<h1>EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	9 of 21

The certification decision is taken by the CB independently from the ITSEF. The certification decision may be one of the following:

- Grant certification
- Grant certification with conditions
- Refuse certification based on documented justification

The outputs of this process are recorded in the applicable controlled certification records.

All issued certificates must be submitted for publication in accordance with the applicable EUCC publication requirements.

5.6 Maintenance of certification

To ensure continued assurance throughout the stated validity period of the certificate, the CB actively monitors compliance with vulnerability handling obligations and disclosure procedures as per VH-01-01a. The CB is responsible for evaluating the impact of any vulnerability disclosures as well as product changes or updates that occur during this period.

Product modifications are classified as:


- Non-security-relevant changes
- Security-relevant changes requiring impact analysis
- Changes requiring partial or full re-evaluation

The Certification Body determines the classification based on input from the evaluation facility and documents the decision rationale.

5.6.1 Assurance continuity (ACO)

Assurance continuity (ACO) is assessed during the validity period of the certificate where changes to a certified ICT product or its environment are notified after certificate issuance. For the purposes of this procedure, ACO is used as an internal shorthand for assurance continuity activities. The Certification Body determines, based on the nature and security relevance of the change and the supporting analysis, whether the change may be managed under maintenance, requires targeted re-evaluation, or requires full re-evaluation and a new certification decision.

- **Criteria:** ACO may be applied where the change is sufficiently bounded, its effect on the certified security functionality and assurance claims is understood, and the Certification Body can conclude, on the basis of an impact analysis and supporting evidence, that the existing certificate remains valid or can be

	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	10 of 21


maintained with defined conditions. Changes that materially affect the TOE boundary, the security problem definition, the security functions, the assumptions about the operational environment, the assurance measures, or the attack surface shall not be accepted under simplified maintenance alone and shall be considered for partial or full re-evaluation.

- Re-evaluation scope:** The scope of re-evaluation is determined case by case. Minor changes with no material impact on certified claims may be managed through maintenance activities only. Security-relevant changes shall be subject to targeted re-evaluation of the affected Security Target claims, evaluation evidence, and relevant ISO/IEC 18045 work units. Major changes, or combinations of changes whose cumulative effect is significant, shall trigger full re-evaluation and, where necessary, a new certification decision.
- Documentation requirements:** The vendor shall provide a documented description of the change, an impact analysis identifying affected assets, functions, interfaces, guidance, and evidence, and the updated evaluation evidence needed to support the proposed continuity decision. Where required, the ITSEF shall provide its technical assessment of the change and the adequacy of the updated evidence. The Certification Body shall document the change classification, the rationale for the determined scope of review or re-evaluation, the recommendation of the technical reviewer, and the resulting certification decision in the applicable maintenance and certification records.

5.6.2 Surveillance activities under the EUCC

During the validity period of an EUCC certificate, the Certification Body performs surveillance activities to confirm that the conditions supporting certification continue to be met and that the certified ICT product remains managed in accordance with the applicable EUCC obligations. These activities support certificate maintenance and assurance continuity and are distinct from market surveillance carried out by competent public authorities.

- Objectives:** to confirm continued conformity with the certified scope, verify that vulnerability handling and disclosure obligations remain effective, and ensure that references to the certificate, the EUCC scheme, and any applicable marks or claims remain accurate and not misleading.
- Inputs reviewed:** vulnerability notifications, change notifications, vendor impact analyses, updated guidance or evidence, publicly available product information, supplementary cybersecurity information made available by the certificate holder, and any information relevant to the use of the certificate in product documentation, software, packaging, websites, or marketing material.

	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	11 of 21


- **Surveillance activities:** review of notified vulnerabilities and remediation status; review of notified product changes and their classification; verification that published certificate information and supplementary cybersecurity information remain current where required; and review of how the certificate, certification status, EUCC references, and any authorised marks or labels are used by the certificate holder.
- **Escalation triggers:** material vulnerabilities affecting certified claims, unnotified or inadequately assessed changes, misleading or non-compliant use of the certificate or EUCC references, failure to maintain required supplementary cybersecurity information, or any indication that the certified scope or assurance claims may no longer be valid.
- **Outputs and records:** the Certification Body records the surveillance inputs reviewed, conclusions reached, required actions, deadlines, and any resulting maintenance, assurance continuity, suspension, withdrawal, or notification decisions in the applicable certification records. Where necessary, the Certification Body informs the certificate holder of corrective actions and notifies the NCCA in accordance with oversight requirements.

5.6.3 Post-certification non-conformities

Post-certification non-conformities are issues identified after certificate issuance that indicate that the conditions supporting certification, maintenance, surveillance, assurance continuity, or proper use of the certificate are not being met. These may arise from surveillance activities, vulnerability handling, change notifications, product lifecycle information, misuse of certification references, or failures to comply with reporting and notification obligations.

These activities are conducted during the stated validity period of the certificate and are documented in the applicable controlled maintenance, surveillance, and certification records.

- **Typical sources:** unresolved or inadequately handled vulnerabilities; unnotified or inadequately assessed product changes; inaccurate, misleading, or unauthorised use of the certificate, EUCC references, or related claims; failure to maintain required supplementary cybersecurity information; missed reporting or notification obligations; or evidence that the certified scope, assumptions, or assurance claims are no longer valid.
- **Classification and initial response:** The Certification Body classifies post-certification non-conformities according to their significance, urgency, and effect on the certified scope and claims. The CB may require immediate clarification,

	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	12 of 21

corrective action, temporary containment measures, additional monitoring, or targeted review by the ITSEF where technical reassessment is needed.

- **Corrective action and follow-up:** The certificate holder shall provide, within the timeframe set by the Certification Body, the proposed correction, remediation plan, impact analysis, and any updated evidence required to demonstrate restoration of conformity. The Certification Body records the non-conformity, tracks the required actions and deadlines, and verifies the adequacy of closure evidence before closing the issue.
- **Escalation and authority notification:** Where a post-certification non-conformity is major, repeated, systemic, or remains unresolved, the Certification Body may impose conditions, reduce scope, suspend the certificate, withdraw the certificate, or require targeted or full re-evaluation. Where required by the applicable framework, the Certification Body notifies the NCCA and any other competent authority of serious or reportable non-conformities.
- **Decision impact and records:** The status, classification, actions taken, closure evidence, and resulting maintenance or lifecycle decision for each post-certification non-conformity shall be recorded in the applicable certification records and reflected in any resulting surveillance, assurance continuity, suspension, withdrawal, or reporting decision.

5.7 Termination, Suspension or Withdrawal of Certification

The process for termination, suspension, withdrawal, or reduction of scope is managed in accordance with SM-01-01, supplemented by the EUCC-specific requirements set out in this procedure for maintenance, non-conformities, surveillance, and authority interaction.


5.8 Complaints and appeals

The process for handling complaints and appeals is documented under SM-01-01. The following additional requirements apply for the EUCC certification scheme:

The CB is the first-line handler of complaints and appeals related to its certification activities.

The NCCA retains oversight powers over CBs and may:

- Investigate systemic issues
- Act on unresolved or serious complaints
- Initiate peer-review or corrective actions

	<h1 style="text-align: center;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	13 of 21

5.9 Interaction with the NCCA


The Certification Body cooperates with the NCCA as part of the applicable authorisation, oversight, and reporting framework and provides information upon request, including certification records, monitoring activities, and corrective actions.

The CB follows mandatory instructions or corrective measures issued by the NCCA and records their implementation.

5.9.1 NCCA authorisation of the Certification Body and ongoing reporting

Where required by the applicable EUCC and national framework, the Certification Body shall maintain any NCCA authorisation necessary to perform EUCC certification activities within the authorised assurance level, technical domain, and scope of activity. The Certification Body shall also fulfil the ongoing reporting and notification obligations attached to that authorisation and to the NCCA's oversight role throughout the lifecycle of its certification activities.


- **Authorisation status:** The Certification Body shall verify and maintain its own NCCA authorisation status, where such authorisation is required, and shall ensure that no EUCC certification activity is undertaken outside the authorised scope.
- **Scope and conditions:** The Certification Body shall monitor any conditions, limitations, expiry dates, technical domain restrictions, assurance level restrictions, or corrective requirements attached to the authorisation and shall implement any necessary controls to remain within scope.
- **Periodic and event-driven reporting:** The Certification Body shall provide periodic reports, returns, or confirmations where required by the NCCA and shall also provide event-driven notifications where significant certification events, serious vulnerabilities, major non-conformities, suspension or withdrawal decisions, or other reportable matters arise. Where required by the applicable framework, corresponding notifications shall also be made to the competent accreditation or notification authorities.
- **Notification of significant changes:** The Certification Body shall notify the NCCA, in accordance with applicable requirements, of significant changes affecting its capability, impartiality, competence, ownership, governance, resourcing, procedures, or other conditions relevant to its authorisation or to the reliability of EUCC certification activities. Where relevant under the applicable framework, the Certification Body shall also notify the competent accreditation or notification authorities of such changes.

	<h1 style="text-align: center;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	14 of 21

- **Oversight cooperation:** The Certification Body shall cooperate with NCCA oversight, monitoring, peer review, audit, or information requests and shall provide access to relevant certification records, authorisation-related records, and evidence of implemented corrective actions within the timeframes specified by the NCCA.
- **Records:** The Certification Body shall retain records of authorisation status, communications with the NCCA, submitted reports, notifications, corrective actions, and decisions affecting authorised scope as part of its controlled certification records.

5.9.2 Additional requirements for assurance level High

Where the applicable EUCC and national framework imposes additional requirements for certification activities at assurance level High, the Certification Body shall verify, before accepting or continuing such activities, that it holds any required NCCA authorisation for High activities and that the activity remains within the authorised technical domain, assurance level, and scope of operation. The Certification Body shall also comply with any additional scheme-specific conditions, reporting obligations, oversight requirements, or access-to-records obligations attached to High authorisation.


	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	15 of 21

Annex A – EUCC Assessment Process Flow

This annex describes the end-to-end EUCC assessment process followed by the Certification Body from application intake through certification, post-certification activities, and interaction with the NCCA. The flow is aligned with section 5 of this procedure and is intended to provide an operational overview of the main decision points and outputs.


Stage	Vendor	ITSEF	Certification Body (CB)	NAB / NCCA
1. Application receipt and registration	Submits application, scope details, and supporting documentation.	No primary action at this stage unless pre-engaged.	Registers the case, confirms requested scope and assurance level, and checks contractual prerequisites.	No primary action.
2. Application review and admissibility	Provides clarifications or missing information where requested.	No primary action unless consulted on feasibility.	Assesses completeness and admissibility; accepts, pauses, or rejects with documented justification.	No primary action.
3. Selection and verification of the ITSEF	Identifies or agrees the proposed ITSEF and supports engagement arrangements.	Provides accreditation, scope, competence, and authorisation evidence where applicable.	Verifies accreditation, scope, and any required authorisation; records the outcome before scoping.	The NAB is the source of accreditation status and scope information. The NCCA provides authorisation or oversight information where applicable.
4. Evaluation scoping and planning	Confirms TOE scope, interfaces, assumptions, and evidence availability.	Defines evaluation activities, methods, interfaces, deliverables, and timeline.	Confirms evaluation scope and planning assumptions against the requested certification basis.	No primary action unless specific oversight is triggered.



	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	16 of 21


Stage	Vendor	ITSEF	Certification Body (CB)	NAB / NCCA
5. Security Target review	Provides the ST and any clarifications, updates, or PP conformance justifications.	May provide technical input on evaluability and traceability implications.	Reviews ST completeness, PP conformance, traceability, and acceptance criteria before substantive evaluation.	No primary action.
6. Evaluation performance and oversight	Supplies evidence, supports testing, and addresses findings through the ITSEF.	Performs evaluation activities, records results, and prepares evaluation outputs.	Maintains oversight, requests status where needed, and ensures significant issues are addressed.	No primary action unless notified of serious issues.
7. Review of outputs and technical review	Supports clarification of residual findings where required.	Provides the ETR and supporting technical evidence; answers CB queries.	Reviews ETR completeness and conclusions; obtains independent technical reviewer recommendation.	No primary action.
8. Certification decision	Receives the decision and any certification conditions or refusal rationale.	No decision-making role; may support clarification if requested.	Takes the independent certification decision based on evaluation results and technical review.	No primary action unless notification is required.
9. Certificate issuance and publication	Receives certificate and provides supplementary cybersecurity information where required.	No primary action unless referenced in certification documentation.	Issues the certificate, completes certification records, and submits for publication.	The NCCA may receive certificate information, notifications, or oversight-related submissions. The NAB has no primary role at this stage.



	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	17 of 21


Stage	Vendor	ITSEF	Certification Body (CB)	NAB / NCCA
10. Maintenance, vulnerability handling, and assurance continuity	Reports vulnerabilities and changes, provides impact analysis, and submits updated evidence.	Assesses change impact or updated evidence where required by the CB.	Classifies changes, determines maintenance or re-evaluation scope, and records the continuity decision.	May be informed of serious vulnerabilities or systemic concerns.
11. Surveillance activities	Provides supplementary cybersecurity information, responds to surveillance queries, and implements corrective action where required.	Supports targeted technical review where surveillance identifies issues requiring technical reassessment.	Performs surveillance of vulnerabilities, notified changes, public information, and certificate use; records findings and determines any required follow-up.	The NCCA may receive notifications of serious issues and may exercise oversight. The NAB has no primary role in routine surveillance.
12. Suspension, withdrawal, termination, or scope reduction	Implements required corrective action or receives lifecycle decision and restrictions.	May provide technical input on unresolved issues or affected scope.	Applies the lifecycle decision, records rationale, and updates certification status.	May be notified or may direct corrective action within oversight powers.
13. Complaints and appeals	May submit or respond to complaints and appeals relevant to certification activities.	Supports fact clarification where the complaint concerns evaluation activity.	Handles complaints and appeals as first-line authority under the applicable procedure.	May investigate serious or systemic issues and exercise oversight powers.



	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	18 of 21

Stage	Vendor	ITSEF	Certification Body (CB)	NAB / NCCA
14. Interaction with the NCCA	Cooperates where product information or corrective action is required.	Provides technical records or clarification where requested through the CB or authority process.	Provides records, implements mandatory instructions, and supports oversight activities.	The NAB maintains accreditation information within its competence. The NCCA exercises oversight, requests information, and may issue corrective measures within its competence.




	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	19 of 21

Annex B – EUCC Traceability

EUCC Article / Annex	EUCC provision title / topic	Procedure section(s)
Article 1	Subject matter	1, 2
Article 2	Scope	2
Article 3	Definitions relevant to certification activities	2, 3
Article 4	Scheme principles	2, 4
Article 5	Assurance level	2, 5.1, 5.5, 5.9.2
Article 6	Common Criteria and Common Evaluation Methodology	2, 5.2, 5.3
Article 7	Protection profiles	5.3, 5.5
Article 8	Conformity with protection profiles	5.3, 5.5
Article 9	Certification basis	5.1, 5.3, 5.5
Article 10	Protection profile-related provisions	5.3, 5.5
Article 11	Certification application	5.1
Article 12	Admissibility and initiation of the certification process	5.1, 5.2
Article 13	Security Target as evaluation basis	5.3
Article 14	Scope of evaluation	5.2, 5.3
Article 15	ITSEF selection and role	3, 5.2
Article 16	Accreditation, notification and authorisation	3, 5.2, 5.2.1, 5.9.1, 5.9.2
Article 17	Conduct of evaluation	5.2, 5.4
Article 18	Evaluation technical report	5.4, 5.4.1
Article 19	Technical review and certification decision basis	3, 5.4, 5.5
Article 20	Certification decision	5.5
Article 21	European cybersecurity certificate	5.5
Article 22	Publication of certificates and public information	5.5
Article 23	Validity period of certificate	5.5, 5.6




	<h1 style="margin: 0;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	20 of 21

EUCC Article / Annex	EUCC provision title / topic	Procedure section(s)
Article 24	Assurance continuity and maintenance	5.6, 5.6.1, 5.6.2, 5.6.3
Article 25	Vulnerability handling	5.6, 5.6.2, 5.6.3
Article 26	Suspension, withdrawal, termination, or reduction of scope	5.6.3, 5.7
Article 27	Use of the European cybersecurity certificate	5.5, 5.6.2, 5.6.3
Article 28	References to the certificate, marks and labels	5.5, 5.6.2, 5.6.3
Article 29	Transparency and public information obligations	5.5, 5.6.2
Article 30	Monitoring and oversight by the NCCA	5.6.2, 5.8, 5.9, 5.9.1, 5.9.2
Article 31	Provision of information and records to the NCCA	5.9, 5.9.1
Article 32	Corrective measures and cooperation with the NCCA	5.8, 5.9, 5.9.1
Article 33	Complaints	5.8
Article 34	Appeals	5.8
Article 35	Records and confidentiality	3, 5.1, 5.9.1
Article 36	Cooperation obligations	5.9, 5.9.1
Article 37	Scheme governance / external control	2, 5.9
Article 38	ENISA support / external control	2
Article 39	Peer review / external control	5.8, 5.9
Article 40	Final provisions	2
Annex VII	Mandatory EUCC certificate content	5.5

This matrix indicates which section of this procedure addresses each article or annex requirement of the EUCC. Where an article is primarily implemented through scheme governance, national authority processes, accreditation, notification, or other controlled documents outside this procedure, the mapped section indicates the closest related internal reference point and should be read together with the applicable external controls.



	<h1 style="text-align: center;">EUCC Assessment process</h1>	Document:	TB-SM-01-03a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	21 of 21

Version History

Version	Date	Author	Summary of changes	Status
1	21-04-2026	Khalimatou Samirah (NSAI)	Initial draft created.	Draft
2	28-05-2026	Khalimatou Samirah (NSAI)	Updated sections as per review comments	Approved

