	<h1>EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	1 of 21

1. Purpose

This operational procedure defines how the IT Security Evaluation Facility (ITSEF) shall plan, perform, document and report cybersecurity evaluations of ICT products under the European Common Criteria-based cybersecurity certification scheme (EUCC). It establishes a consistent approach for selecting evaluation methods, preparing evaluation work, executing assessment activities, handling deviations, and producing evaluation outputs suitable for review by the certification body.


2. Scope

This procedure applies to all EUCC evaluation engagements performed by the ITSEF within its accredited and authorised scope for ICT products, protection profiles, and related assurance activities. It covers the ITSEF's role from application review, after a positive CB pre-application outcome, through evaluation planning, technical evaluation, vulnerability analysis and testing, evidence management, reporting, interaction with the certification body, the National Cybersecurity Certification Authority (NCCA), and the National Accreditation Body (NAB), and retention of records. The engagement begins only after the client has accepted the CB and ITSEF terms and conditions and the applicable agreement under [CA-01-01](#) has been signed by the client, the CB, and the ITSEF. Where national scheme instructions or certification body requirements impose stricter controls, those controls shall also apply.

3. Normative and Supporting References

- Regulation (EU) 2019/881 (Cybersecurity Act).
- Commission Implementing Regulation (EU) 2024/482 establishing the EUCC scheme, as amended.
- Applicable Common Criteria standards (ISO/IEC 15408 / CC) and Common Evaluation Methodology (ISO/IEC 18045 / CEM), in the version applicable to the engagement.
- Applicable EUCC state-of-the-art documents, including documents on ITSEF accreditation and technical competence.
- EUCC guidance on vulnerability management and disclosure, where relevant to the scope of evaluation and assurance continuity.
- ISO/IEC 17025:2017 and the ITSEF quality management system.




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

- Certification body procedures, interpretation notes, and national authority instructions applicable to the engagement.

4. Roles and Responsibilities

Role	Responsibilities
ITSEF Manager	Ensures resources, competence, independence, and assignment of qualified personnel; approves evaluation start, assurance level determination, major plan changes, and final release of deliverables.
Lead Evaluator	Participates in the application process after a positive CB pre-application outcome, performs the ITSEF application review, issues ITSEF terms and conditions, and, once the engagement is formalised under CA-01-01 , manages the evaluation. This includes maintaining the evaluation plan, performing and documenting assurance level determination, allocating tasks, coordinating technical activities, controlling evidence, managing issues and changes, and consolidating reporting.
Evaluators / Technical Experts	Perform assigned work packages, maintain working records, review evidence, conduct technical analysis, testing and vulnerability assessment, raise issues promptly, and support report drafting.
Quality Function	Verifies compliance with this procedure and the quality management system, confirms control of records and evidence handling, and performs independent review of key deliverables before release.
Customer / Developer	Submits pre-application and application information through the CB process, selects the ITSEF where applicable, accepts the CB and ITSEF terms and conditions, and signs the agreement under CA-01-01 . The customer or developer then provides the TOE, the Security Target, the protection profile basis where applicable, documentation, test environments, guidance, patches, and clarifications within agreed timelines, and supports reproducibility and issue resolution.
Certification Body (CB)	Provides certification scheme interpretations, reviews pre-application and application submissions, manages acceptance and contractual arrangements, issues the CB terms and conditions, and sends the agreement under CA-01-01 for signature once the client has accepted both sets of terms. The CB then receives evaluation outputs, reviews submissions, and makes certification decisions outside the ITSEF's remit.



	<h1 style="margin: 0;">EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	3 of 21	


Role	Responsibilities
National Cybersecurity Certification Authority (NCCA)	Performs national supervisory, authorisation, oversight, and regulatory interaction functions under the applicable scheme framework; may provide national guidance, receive notifications, and request follow-up information where required.
National Accreditation Body (NAB)	Provides accreditation, surveillance, assessment, and competence oversight relevant to the ITSEF's accredited scope; may receive information, assessment evidence, and follow-up actions related to accreditation conditions, nonconformities, and maintenance of accreditation.

5. Evaluation Methods

The ITSEF shall select and apply evaluation methods that are appropriate to the claimed Common Criteria assurance package, the target of evaluation (TOE), the technology involved, the evaluated configuration, and the applicable CC/CEM and EUCC requirements. Methods shall be justified in the evaluation plan and be traceable to the relevant assurance classes and components, work units, and applicable state-of-the-art documents. Under EUCC, the overall certification assurance level shall be determined primarily by the applicable AVA_VAN component, with the remainder of the assurance package selected in accordance with the Security Target, applicable Protection Profile, and scheme requirements.

- **Documentation review:** analysis of the security target, guidance, design, lifecycle, configuration management, test documentation, and supporting evidence for completeness, consistency, and evaluability.
- **Functional assessment:** confirmation that the TOE security functions can be tested and that developer test evidence is adequate, repeatable and relevant.
- **Independent testing:** evaluator-designed and evaluator-performed tests to confirm claimed security behaviour and investigate areas of uncertainty.
- **Vulnerability analysis:** identification and assessment of potential vulnerabilities based on public sources, design information, misuse cases, attack paths, and evaluator expertise.
- **Penetration testing:** focused technical testing to determine whether identified vulnerabilities are exploitable in the evaluated configuration.
- **Tool-assisted analysis:** use of validated or controlled tools for code review, protocol analysis, fuzzing, configuration review, binary analysis, or hardware-assisted examination where justified.



	<h1 style="margin: 0;">EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	4 of 21	

- **Sampling and depth decisions:** where the methodology permits sampling, the ITSEF shall document the rationale, sampling basis, and any limitations introduced.

For specialised technology areas such as smart cards, secure elements, cryptography, network devices, operating systems, or composite evaluations, the ITSEF shall ensure that methods, competence, facilities and equipment are consistent with the applicable EUCC scope and supporting state-of-the-art documents. Any subcontracted activity shall remain under ITSEF control and only be used where permitted by accreditation and scheme requirements.


6. Common Criteria Assurance Classes and EUCC Assurance Levels

For EUCC evaluations, the ITSEF shall define the evaluation scope using the Common Criteria assurance framework and then determine whether the resulting evaluation supports the EUCC assurance level of Substantial or High. The Common Criteria provides assurance classes and components that define the depth and rigour of evaluation work, while EUCC expresses the certification outcome at the scheme level. The procedure shall therefore distinguish between the detailed CC assurance package used for the evaluation and the EUCC assurance level claimed for certification.

6.1. Common Criteria Assurance Classes

- **ASE – Security Target Evaluation:** evaluation of the Security Target to confirm that the TOE scope, security problem definition, objectives, SFRs, SARs and claims are complete, consistent and suitable for evaluation.
- **ADV – Development:** evaluation of the TOE design and implementation representation to confirm that the security architecture, functional specification, subsystem design and interfaces support the security claims.
- **AGD – Guidance Documents:** evaluation of preparative and operational guidance to confirm that the TOE can be securely installed, configured, administered and used in the evaluated configuration.
- **ALC – Life-Cycle Support:** evaluation of configuration management, delivery, development security, problem handling, tools and related life-cycle controls relevant to assurance.



	<h1 style="margin: 0;">EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	5 of 21	

- **ATE – Tests:** evaluation of developer testing and performance of evaluator independent testing to confirm the claimed behaviour of the TOE security functionality.
- **AVA – Vulnerability Assessment:** evaluator vulnerability analysis and penetration testing to determine whether exploitable vulnerabilities exist in the evaluated configuration at the claimed attack potential.

The specific assurance components selected within these classes shall be those required by the applicable evaluation package, Protection Profile, Security Target, augmentation claims, and EUCC state-of-the-art documents. The Lead Evaluator shall ensure that the evaluation plan identifies the applicable work units for each selected component and the evidence needed to reach a conclusion.

6.2. Evaluation Assurance Level Context


Where an Evaluation Assurance Level (EAL) package is used, the ITSEF shall treat the EAL as a shorthand expression of a defined combination of assurance components across the CC assurance classes. The EAL alone does not determine the EUCC assurance level. Under EUCC, the decisive factor for scheme-level assurance is the applicable AVA_VAN component, together with the overall assurance package and any mandatory state-of-the-art technical domain requirements.

6.3. EUCC Assurance Level: Substantial

For EUCC certification at the Substantial assurance level, the evaluation shall support resistance against attackers with limited attack potential and shall typically correspond to AVA_VAN.1 or AVA_VAN.2. In practice, this usually aligns with lower to mid-range CC assurance packages, but the ITSEF shall not rely on EAL shorthand alone when determining the EUCC level. The evaluation shall include an appropriate Security Target review, design and guidance assessment, life-cycle support review, developer test assessment, independent evaluator testing, and vulnerability analysis proportionate to the claimed attack potential.

- The evaluation plan shall identify the minimum assurance components and the target AVA_VAN level supporting Substantial.
- Independent testing shall confirm security functionality and investigate publicly known or readily derivable vulnerabilities relevant to the TOE.
- Vulnerability analysis shall include public-domain sources, configuration review, misuse scenarios, and reasonable attack paths for a limited attacker.



	<h1 style="margin: 0;">EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	6 of 21	

- Reporting shall clearly state the assurance package evaluated, the achieved AVA_VAN level, and any assumptions or restrictions that condition the Substantial claim.

6.4. EUCC Assurance Level: High

For EUCC certification at the High assurance level, the evaluation shall support resistance against attackers with moderate to high attack potential and shall correspond to AVA_VAN.3, AVA_VAN.4, or AVA_VAN.5. The evaluation shall normally involve deeper design analysis, stronger evidence requirements, more rigorous independent testing, and advanced vulnerability analysis and penetration testing. Where the target level is based on AVA_VAN.4 or AVA_VAN.5, the evaluation shall, as a rule, be performed within an applicable technical domain or on the basis of a Protection Profile adopted as a state-of-the-art document under EUCC.


- The evaluation plan shall explicitly identify the target AVA_VAN level, technical domain constraints, specialist competence needs, specialised tools or facilities, and white-box or deeper design evidence required to support High.
- Independent testing and penetration testing shall be planned against more advanced attack paths and higher attack potential, including bespoke or technology-specific techniques where justified.
- The ITSEF shall ensure stronger traceability between design evidence, test hypotheses, vulnerability analysis results, and final conclusions.
- Reporting shall clearly state the assurance package evaluated, the achieved AVA_VAN level, the technical domain or state-of-the-art basis used where applicable, and any evaluation limitations affecting the High claim.

6.5. Assurance Level Determination

Before finalising the evaluation plan, the Lead Evaluator shall perform and document an assurance level determination to confirm whether the proposed evaluation scope supports the EUCC assurance level of Substantial or High. This determination shall be based on the claimed Security Target and/or applicable Protection Profile, the selected Common Criteria assurance components, the target AVA_VAN component, any applicable technical domain or state-of-the-art document, and the nature of the TOE technology and threat environment.

1. The Lead Evaluator shall identify the claimed certification path, including the customer's requested EUCC assurance level, the applicable Security Target



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

and/or Protection Profile, and any mandatory scheme or certification body constraints.

2. The Lead Evaluator shall identify the full assurance package, including all selected assurance classes and components, and confirm whether an EAL package, augmentation, or bespoke component set is being used.
3. The Lead Evaluator shall identify the target AVA_VAN component and confirm whether it supports Substantial or High under EUCC.
4. Where the target level is High and relies on AVA_VAN.4 or AVA_VAN.5, the Lead Evaluator shall confirm that the evaluation is within an applicable technical domain or supported by a Protection Profile adopted as a state-of-the-art basis under EUCC.
5. The Lead Evaluator shall assess whether the available evidence, evaluator competence, tools, facilities, and planned technical methods are sufficient to support the claimed assurance level.
6. The Lead Evaluator shall assess whether the evaluated configuration, assumptions, operational environment, and scope restrictions are compatible with the intended assurance claim and do not undermine the level sought.
7. The Lead Evaluator shall record the determination outcome as Substantial, High, or not yet justified, together with the rationale, limiting conditions, and any actions required before technical work proceeds.
8. The ITSEF Manager shall review and approve the assurance level determination before the evaluation plan is baselined.


If the assurance level cannot be justified at planning stage, the evaluation shall not be presented as supporting that EUCC level until the missing basis has been resolved. Where significant scope changes, evidence changes, or technical findings arise during execution, the assurance level determination shall be revisited and updated.

The output of this step shall be retained as a controlled record and referenced in the evaluation plan and final reporting package.

7. Evaluation Planning

Before technical work begins, the Lead Evaluator shall prepare and maintain an evaluation plan. Planning may begin only after the CB has positively completed the pre-application stage, the application has been accepted for progression, the ITSEF has completed its own application review with a positive outcome, the client has accepted the CB and ITSEF terms and conditions, and the agreement under CA-01-01 has been signed by the client, the CB, and the ITSEF. The plan shall be reviewed internally and,



	<h1 style="margin: 0;">EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	8 of 21	

where required, aligned with the certification body. Planning shall confirm that the requested evaluation is within the ITSEF's accredited scope and that the necessary personnel, facilities, independence, and confidentiality controls are in place.

- Identification of the customer, TOE, version/build, evaluated configuration, delivery form, and intended certification path.
- Identification of the claimed EUCC assurance level, the underlying assurance package and components, applicable protection profile and/or security target, and the target AVA_VAN level to be achieved.
- List of applicable standards, scheme documents, technical interpretations, and state-of-the-art documents.
- Definition of evaluation activities, work packages, milestones, dependencies, entry criteria, and completion criteria.
- Assignment of competent personnel and required specialist support.
- Definition of required test environments, tools, samples, credentials, and facilities.
- Identification of assumptions, constraints, risks, and planned mitigations.
- Communication points with the developer and certification body, including expected review cycles and reporting checkpoints.
- Rules for evidence receipt, version control, secure storage, traceability, and handling of confidential information.

If the scope, methodology, TOE configuration, or evidence baseline changes during the engagement, the Lead Evaluator shall assess the impact, update the evaluation plan, and obtain the necessary approvals before continuing affected work.


8. Evaluation Execution

The ITSEF shall perform evaluation activities in a controlled and reproducible manner. All work shall be based on the approved evaluation plan, current evidence baseline, and the applicable CC/CEM and EUCC requirements. Evaluators shall maintain sufficient working records to demonstrate what was examined, how conclusions were reached, and which versions of evidence, tools, scripts and samples were used.

8.1. Evidence Intake and Baseline Control

Upon receipt, evaluation evidence shall be checked for completeness, integrity, identification, and version status. The ITSEF shall define the evaluation baseline and ensure that subsequent changes are logged, assessed for impact, and controlled.



	<h1 style="margin: 0;">EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	9 of 21	

Unclear, incomplete or inconsistent evidence shall be raised as an issue to the customer without delay.

8.2. Technical Evaluation Activities

- Review documentation against the applicable work units and identify gaps, contradictions, or non-evaluable claims.
- Assess the TOE configuration and installation guidance to confirm that the evaluated configuration is well defined and reproducible.
- Review developer tests for coverage, repeatability, and relevance; repeat or witness tests where justified.
- Design and perform independent tests to confirm security functionality and investigate identified concerns.
- Conduct vulnerability analysis using threat-informed and design-informed techniques, public vulnerability sources, prior knowledge, and evaluator judgement.
- Perform penetration testing proportionate to the evaluation scope, attack potential and assurance claims.
- Record observations, anomalies, deviations, unresolved issues, and preliminary verdicts in controlled working papers.

8.3. Issue Handling and Escalation

All issues affecting scope, evidence quality, reproducibility, or the ability to reach a conclusion shall be logged and tracked to closure. Significant issues, including those that may affect the evaluation verdict, timelines, or certification expectations, shall be escalated to the ITSEF Manager and communicated to the certification body as required by the engagement rules.


8.4. Deviations, Changes and Retesting

When the TOE, development evidence, test environment, or claimed scope changes, the ITSEF shall assess whether previously completed work remains valid. The Lead Evaluator shall determine the need for additional review, regression testing, or re-performance of affected activities. No conclusion shall be issued on superseded evidence without documented justification.

8.5. Quality Controls During Execution

The Lead Evaluator shall perform periodic internal reviews of progress, technical consistency, evidence traceability, and adequacy of test records. Key evaluation outputs,



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

including work package conclusions and the draft final report, shall undergo independent quality review before release. Where competence gaps are identified, specialist review or reassignment shall be made before conclusions are finalised.

9. Evaluation Reporting

The ITSEF shall prepare evaluation reporting that is accurate, objective, technically supported, and aligned with the certification body's reporting templates and review expectations. Reporting shall clearly distinguish factual observations, evaluator analysis, residual limitations, and conclusions. The final report shall be traceable to the evaluation scope, evidence baseline, and activities actually performed.


- Identification of the TOE, version, configuration, customer, and evaluation scope.
- Applicable standards, scheme documents, assurance claims, and any relevant interpretations.
- Summary of evidence received and baseline versions used.
- Description of methods applied, including any sampling, tool use, or limitations.
- Results for each relevant assurance area and work package.
- Details of vulnerabilities examined, tests performed, and outcomes obtained.
- Unresolved issues, assumptions, exclusions, and conditions affecting interpretation of results.
- Overall evaluation conclusions and recommendation for certification body review.

Interim status reports may be issued where required by contract or scheme process. Any communication of preliminary results shall be clearly marked as provisional and shall not be interpreted as a certification decision.

10. Records and Retention

The ITSEF shall retain evaluation plans, evidence inventories, working papers, test records, issue logs, review records, communications relevant to conclusions, and released reports for the retention period defined by the quality management system, accreditation requirements, contractual obligations, and applicable scheme rules. Records shall be protected for confidentiality, integrity, and retrievability.




	<h1>EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	11 of 21

11. Review and Improvement

This procedure shall be reviewed periodically and updated when EUCC scheme documents, applicable standards, accreditation conditions, technical methods, or certification body expectations change. Lessons learned from completed evaluations, nonconformities, internal audits, and external assessments shall be incorporated into process improvements, templates, competence development, and tool control.



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


Annexes

Annex A – Stakeholder Process Steps and Actions

The following table summarises the main process steps in this procedure and the expected actions of each stakeholder involved in the EUCC evaluation process. It is intended as an operational reference to clarify responsibilities and interfaces during planning, execution, reporting, certification body review, and interaction with the National Cybersecurity Certification Authority (NCCA) and the National Accreditation Body (NAB).


Process Step	Customer/ Developer	Lead Evaluator	Evaluators/Technical Experts	ITSEF Manager	Quality Function	Certification Body (CB)	NCCA	NAB
1. Pre-application outcome, application review and engagement initiation	Provide pre-application and application information through the CB process, select the ITSEF where applicable after positive pre-application outcome, review and accept the terms and conditions of engagement of	Participate in the application process after a positive CB pre-application outcome, perform the ITSEF application review and record a positive or negative outcome, confirm the requested scope, identify the evaluation path, issue ITSEF terms and conditions, and confirm	Provide technical input on technology, evaluation feasibility, and likely specialist needs.	Confirm resource availability, independence, and fit with accredited scope, and approve ITSEF engagement after the contractual trigger has been met.	Confirm procedural controls and records required at engagement start.	Complete pre-application and application review, confirm acceptance for progression, issue the CB terms and conditions, and send the agreement under CA-01-01 for signature once the client has accepted both the CB and ITSEF terms. The CB	Provide national scheme guidance, authorisation expectations, or oversight conditions where applicable.	Provides accreditation scope constraints, surveillance expectations, or accreditation conditions relevant to the ITSEF's ability to undertake the engagement.



	<h1 style="margin: 0;">EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	13 of 21


Process Step	Customer/ Developer	Lead Evaluator	Evaluators/Technical Experts	ITSEF Manager	Quality Function	Certification Body (CB)	NCCA	NAB
	both the CB and the ITSEF, and sign the applicable agreement under CA-01-01.	readiness for planning once the client has accepted both sets of terms and the agreement under CA-01-01 has been signed.				also provides scheme expectations, the reporting route, and any initial certification constraints.		
2. Assurance level determination	State requested assurance objective and provide applicable Protection Profile and/or Security Target basis.	Perform and document the assurance level determination, including target AVA_VAN and rationale.	Support technical feasibility assessment for the claimed assurance level.	Review and approve the assurance level determination before baselining.	Verify that the determination record is complete and controlled.	Clarify certification interpretation where the assurance basis or certification path is uncertain.	Clarify national interpretation, authorisation conditions, or oversight expectations where relevant to the claimed level.	May assess whether the claimed methods, competence, and scope remain consistent with accreditation capabilities where this affects accredited coverage.
3. Evaluation planning	Provide evidence baseline, contacts, test access, schedules, and constraints.	Prepare the evaluation plan, assign work packages, define milestones, tools, facilities, and	Review assigned tasks and confirm technical methods, environments, and prerequisites.	Approve start of evaluation and ensure competent staffing and facilities.	Review plan compliance with the procedure and quality requirements.	Review or align with reporting, review, and oversight expectations where applicable.	Be informed where the engagement requires notification, authorisation linkage, or	May review accreditation-relevant planning interfaces during surveillance or



	<h1 style="margin: 0;">EUCC Evaluation Process</h1>	Document: TB-SM-01-03
		Revision: 2.0
		Date issued: DD-MM-YYYY
		Owner: To be determined
		Page: 14 of 21


Process Step	Customer/ Developer	Lead Evaluator	Evaluators/Technical Experts	ITSEF Manager	Quality Function	Certification Body (CB)	NCCA	NAB
		communication points.					national supervisory visibility.	assessment, especially where facilities, methods, or competence affect accredited scope.
4. Evidence intake and baseline control	Submit evidence, version identifiers, guidance, and updates in controlled form.	Define baseline, assess completeness and consistency, and raise issues where needed.	Check technical sufficiency of evidence for assigned work units.	Support escalation where evidence gaps materially affect scope or schedule.	Verify evidence handling, traceability, and record control arrangements.	Be informed of material baseline issues where they affect certification expectations or review planning.	Be informed where evidence issues raise national oversight, non-compliance, or authorisation concerns.	May examine evidence-control arrangements as part of accreditation assessment, surveillance, or follow-up on nonconformities affecting validity of results.
5. Documentation review and evaluator analysis	Respond to clarification requests and provide corrected or supplementary evidence.	Coordinate review activities and consolidate emerging findings and issues.	Review documentation, identify gaps or contradictions, and record preliminary conclusions.	Monitor progress and support resolution of significant obstacles.	Confirm that review outputs are adequately documented and controlled.	Provide interpretation support where certification-specific questions arise.	Receive escalations where national authority awareness is required by scheme rules or supervisory obligations.	May review competence and process control evidence during assessment or surveillance where evaluation



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


Process Step	Customer/ Developer	Lead Evaluator	Evaluators/Technical Experts	ITSEF Manager	Quality Function	Certification Body (CB)	NCCA	NAB
								activities relate to accredited technical capability.
6. Developer test review and independent testing	Provide test evidence, environments, credentials, and support for reproducibility.	Define independent testing scope and ensure it addresses claimed functionality and identified concerns.	Assess developer tests, repeat or witness tests as needed, and perform independent tests.	Ensure required resources, facilities, and technical support remain available.	Verify adequacy of test records and review evidence supporting conclusions.	Receive escalations if test outcomes affect certification assumptions, reporting, or scope.	Be informed where testing outcomes may trigger regulatory concern, supervisory notification, or national follow-up.	May review test capability, facilities, or method control as part of accreditation assessment or surveillance of the ITSEF.
7. Vulnerability analysis and penetration testing	Provide design details, configurations, patches, and technical clarifications relevant to vulnerability analysis.	Direct vulnerability analysis strategy and confirm testing is proportionate to the claimed assurance level.	Perform vulnerability analysis, penetration testing, and record methods, results, and limitations.	Ensure specialist capability and approvals for advanced testing where required.	Check traceability between findings, test evidence, and conclusions.	Be informed of significant findings that may affect certification path, reporting, assurance continuity, or scheme obligations.	Be informed of significant vulnerability findings where national monitoring, coordinated handling, or supervisory action may be required.	May review the ITSEF's technical capability, specialised methods, and control of facilities relevant to accredited vulnerability analysis and penetration testing activities.



	EUCC Evaluation Process	Document:	TB-SM-01-03
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	16 of 21


Process Step	Customer/ Developer	Lead Evaluator	Evaluators/Technical Experts	ITSEF Manager	Quality Function	Certification Body (CB)	NCCA	NAB
8. Issue handling, changes, and retesting	Provide responses, corrective updates, revised evidence, and revised TOE builds where applicable.	Assess impact of issues or changes, update plan, and determine need for regression or re-performance.	Reassess affected work packages and perform additional review or testing as directed.	Approve major plan changes and support escalation decisions.	Verify that changes, deviations, and retesting decisions are controlled and justified.	Review major changes where notification, certification review, or revised reporting is required.	Receive notification where major changes affect authorised scope, national oversight, or compliance expectations.	May be informed or may assess follow-up where changes or nonconformities affect accredited scope, validity of results, or maintenance of accreditation.
9. Draft reporting and internal review	Review factual accuracy when invited and clarify outstanding points.	Prepare the draft report and consolidate assurance conclusions, limitations, and recommendations.	Contribute technical sections, evidence references, and supporting rationale.	Review readiness for release and confirm managerial approval path.	Perform independent quality review of draft deliverables before issue.	May receive draft outputs or status updates according to certification process and review arrangements.	May be provided information or notified where required by supervisory process or national scheme practice.	May review documented evidence of process control, impartiality, or competence during accreditation assessment or surveillance, rather than draft certification content itself.
10. Final reporting and submission	Acknowledge final factual inputs and receive	Finalise reporting package and submit evaluation outputs for	Support closure of technical comments and archive working records.	Approve final release of deliverables.	Confirm that review comments are resolved and	Review submitted outputs and use them as	Receive information, notification, or copied outputs	May receive information relevant to accreditation



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

Process Step	Customer/ Developer	Lead Evaluator	Evaluators/Technical Experts	ITSEF Manager	Quality Function	Certification Body (CB)	NCCA	NAB
	released deliverables as agreed.	certification body review.			records are complete.	input to certification decision-making.	where required for national register, supervision, or authority action.	follow-up, surveillance, or closure of accreditation-related nonconformities where applicable.
11. Record retention and post-evaluation follow-up	Provide follow-up information if needed for residual questions or continuity activities.	Ensure records are complete, archived, and retrievable; support follow-up technical clarifications.	Ensure working papers, scripts, and test artefacts are retained in controlled form.	Oversee record retention and lessons learned actions.	Verify retention, integrity, confidentiality, and retrievability of records.	Request clarification or follow-up information where needed for certification or assurance continuity purposes.	Request clarification, follow-up, or supervisory information where required under national oversight or monitoring responsibilities.	May request records, follow-up evidence, or corrective-action updates where needed for surveillance, reassessment, or maintenance of accreditation.




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

Annex B – Coverage of the Procedure Against EUCC Articles

The following table provides a high-level coverage view showing how this procedure addresses key articles of the EUCC regulation that are relevant to ITSEF evaluation activities, assurance handling, reporting, interaction with the certification process, and accreditation-related oversight. It is intended as a traceability aid and does not replace direct consultation of the regulation, accreditation requirements, or applicable scheme guidance.


EUCC Article	Article Topic	Procedure Coverage	Coverage Notes	Accreditation / NAB Relevance
Article 3	Evaluation standards	Sections 3, 5, 5A, 6, 7, 8	The procedure references Common Criteria and Common Evaluation Methodology as normative bases and applies them in evaluation methods, assurance handling, execution, and reporting.	Highly relevant to NAB oversight because accreditation assessments examine whether the ITSEF applies recognised standards, controlled methods, and competent technical practices within accredited scope.
Article 4	Assurance levels	Sections 5A.2, 5A.3, 5A.4, 5A.5, 6	The procedure distinguishes EUCC Substantial and High, explains the role of AVA_VAN, and defines an assurance level determination step before baselining the evaluation plan.	Relevant to NAB review where assurance-level claims affect competence, methods, facilities, and the technical scope for which the ITSEF is accredited.
Article 5	Methods for certifying ICT products	Sections 5, 5A, 6, 7, 8	The procedure defines evaluation methods, planning controls, execution activities, and reporting outputs that support the certification process for ICT products.	Relevant because NAB assessments consider whether evaluation methods are controlled, validated where appropriate, and supported by the ITSEF's accredited competence and facilities.
Article 7	Evaluation criteria and methods for ICT products	Sections 5, 5A, 6, 7, 8	The procedure addresses evaluation criteria through CC assurance classes, assurance components, evaluation planning,	Relevant to NAB review of technical execution capability, specialist competence, traceability of work, and consistency of evaluation practice with accredited methods.



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


EUCC Article	Article Topic	Procedure Coverage	Coverage Notes	Accreditation / NAB Relevance
			documentation review, testing, vulnerability analysis, penetration testing, and reporting.	
Article 8	Information necessary for certification and evaluation	Sections 6, 7.1, 8, 9, Annex A	The procedure defines required planning inputs, evidence intake and baseline control, reporting content, retention of records, and stakeholder actions relating to provision and handling of evaluation information.	Highly relevant to NAB oversight of evidence control, confidentiality, integrity of records, and validity of results under the accreditation framework.
Article 9	Conditions for issuance of an EUCC certificate	Sections 5A, 7, 8, Annex A	The procedure supports certificate issuance indirectly by requiring justified assurance claims, controlled execution, traceable reporting, and submission of evaluation outputs to the certification body.	Indirectly relevant to NAB because accreditation supports confidence in the competence and controls underpinning evaluation outputs, even though certificate issuance itself is outside the NAB's remit.
Article 13	Review of an EUCC certificate	Sections 7.4, 8, 9, Annex A	The procedure addresses changes, retesting, record retention, and post-evaluation follow-up, which support later review of certification outcomes where required.	Relevant to NAB follow-up where ongoing competence, record retention, change control, or validity of results are examined during surveillance or reassessment.
Article 14	Withdrawal of an EUCC certificate	Sections 7.3, 7.4, 8, 9	The procedure supports withdrawal-related scenarios indirectly through issue escalation, change impact assessment, controlled reporting, and maintenance of records supporting traceability of findings.	Indirectly relevant where withdrawal-related issues expose weaknesses in accredited processes, competence, or control measures that may also require NAB follow-up.



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

EUCC Article	Article Topic	Procedure Coverage	Coverage Notes	Accreditation / NAB Relevance
Article 22	Additional or specific requirements for an ITSEF	Sections 2, 4, 5, 6, 7, 8, 9, 10, Annex A	The procedure addresses accredited scope, roles, competence, evaluation methods, quality review, evidence and records control, reporting, and improvement activities relevant to ITSEF operation.	Central to NAB relevance because accreditation, surveillance, competence assessment, and maintenance of accredited scope are core mechanisms supporting these ITSEF-specific requirements.
Article 24	Notification of ITSEF	Sections 2, 4, Annex A	The procedure recognises operation within authorised scope and includes interaction points with the certification body and NCCA, but notification mechanics remain primarily outside the scope of this operational procedure.	Relevant to NAB indirectly because accreditation status and accredited scope commonly underpin the basis on which the ITSEF can be notified or maintained as competent within scheme arrangements.
Article 25	Monitoring activities by the NCCA	Sections 2, 4, Annex A	The procedure recognises NCCA oversight, notification, and follow-up interaction points, especially in the roles table and stakeholder annex.	NAB relevance is indirect but complementary, as accreditation surveillance and corrective-action follow-up can support confidence in the ITSEF controls that are also subject to NCCA monitoring.



	<h1 style="text-align: center;">EUCC Evaluation Process</h1>	Document:	TB-SM-01-03
		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	28-05-2026	Khalimatou Samirah (NSAI)	Initial draft created.	Draft
2	02-06-2026	Khalimatou Samirah (NSAI)	Updated sections as per review comments,	Approved

