

	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	1 of 19

1. Purpose

This document defines the processes and controls used by [Certification Body] to manage vulnerabilities affecting EUCC-certified ICT products during the certificate lifecycle, in accordance with the EUCC scheme, ENISA guidance, ISO/IEC 29147 on vulnerability disclosure, and ISO/IEC 30111 on vulnerability handling processes. This process is applied in accordance with the requirements documented under SM-01-01.

2. Scope

This process applies to:

- All EUCC certificates issued, maintained, renewed, suspended, or withdrawn by the CB.
- All vulnerability related information received:
 - From certified clients
 - From evaluation laboratories
 - From third parties (e.g. NCCAs, coordinated disclosure actors)

3. Roles and Responsibilities

Role	Responsibility
Certificate holder (product manufacturer, vendor, etc)	<ul style="list-style-type: none"> • Maintain documented vulnerability handling procedures • Notify the CB of relevant vulnerabilities affecting the certified product • Cooperate with monitoring and compliance activities
Certification body (CB)	<ul style="list-style-type: none"> • Monitor certified products for vulnerabilities and receive vulnerability-related information from certificate holders, ITSEFs, NCCAs, ENISA communications, public disclosures, and other relevant sources. • Enforce vulnerability management and disclosure obligations applicable to the certificate holder. • Assess relevance to the EUCC certificate, review the vulnerability impact analysis and supporting evidence provided by the certificate holder, and determine whether certificate review, escalation,

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	2 of 19

Role	Responsibility
	<p>coordinated handling, or disclosure oversight is required.</p> <ul style="list-style-type: none"> Notify and engage the relevant NCCA where a case is significant or otherwise requires competent authority awareness, supervisory coordination, or national follow-up. Decide on certificate status actions, including confirmation, continued validity subject to conditions, withdrawal, and, where applicable, issuance of a new certificate.
Evaluation facility (ITSEF) where applicable	<p>Supports the CB with:</p> <ul style="list-style-type: none"> Technical analysis of vulnerability impact Re-assessment against Security Target / Protection Profile
National Cybersecurity Certification Authority (NCCA)	<ul style="list-style-type: none"> Acts, where applicable, as the competent national authority for certification oversight, supervisory coordination, or national follow-up in accordance with the EUCC and applicable national procedures. Receives notifications from the CB regarding significant vulnerabilities, certificate review actions, or cases requiring authority awareness or escalation. Supports coordination with other competent actors where a case involves significant risk, cross-border relevance, or coordinated vulnerability disclosure considerations.

4. Process Overview

The CB shall manage vulnerability-related information affecting EUCC-certified ICT products through the following stages. This overview provides the end-to-end process from receipt of information to certificate status decision and associated follow-up actions, aligning internal vulnerability handling activities with ISO/IEC 30111 and external-facing disclosure and communication activities with ISO/IEC 29147.

- 1. Receipt and Logging** – Vulnerability information is received through defined intake channels from certified clients, evaluation laboratories, NCCAs, ENISA communications, public disclosures, or other relevant sources. Each case is acknowledged where appropriate, logged, assigned a unique reference, and linked to the relevant certificate, product version or configuration, and assurance level. This stage shall be completed within **5 business days** of receipt.



2. **Relevance Assessment** – The CB assesses whether the reported vulnerability applies to the certified ICT product, falls within the scope of the certified Security Target or applicable Protection Profile, and may affect the certified security claims or assurance basis of the certificate. This stage shall be completed within **10 business days** of logging the case.
3. **Impact Analysis and Technical Input** – Where the vulnerability is relevant and may affect the basis on which the certificate was issued, the certificate holder carries out a vulnerability impact analysis, validates the reported issue as necessary, and provides a vulnerability impact statement and supporting evidence to the CB.

The CB reviews that analysis, obtains technical input from the ITSEF or requests re-evaluation where necessary, and determines whether remediation, mitigation, and verification activities are required where the case may affect certificate validity. This step shall be completed within **30 calendar days** of the relevance assessment outcome, subject to timely receipt of evidence from the certificate holder and any required ITSEF input.
4. **CB Decision and Escalation** – Based on the relevance assessment and impact analysis, the CB determines the appropriate next step, including routine monitoring, coordinated handling and escalation, progression to certificate review, and NCCA notification where significance criteria are met. The CB records the rationale, actions, responsibilities, and timelines for follow-up. This step shall be completed within **5 business days** of completion of the impact analysis.
5. **Vulnerability Disclosure Oversight** – Where applicable, the CB oversees the certificate holder’s vulnerability management and coordinated disclosure activities, including verification, impact analysis reporting, remediation or mitigation planning, communication with reporters and affected parties, advisory release, post-release follow-up, and coordination with the ITSEF, NCCA, CSIRT, or other competent actors where relevant. An initial disclosure oversight plan shall be established within **10 business days** of the CB decision to escalate, and follow-up activities shall continue in accordance with the agreed remediation and disclosure timetable.
6. **Certificate Review and Status Decision** – Where the vulnerability may affect the validity of the certificate, the CB reviews the certificate and determines whether the certificate is confirmed, remains valid subject to defined conditions, or is withdrawn and, where applicable, replaced by a new certificate. The certificate status decision shall be completed within **15 business days** of conclusion of the certificate review, subject to receipt of all required evidence and any re-evaluation results.

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	4 of 19

7. **Recording, Communication and Closure** – The CB records the outcome of the review and status decision, communicates with the certificate holder and other relevant parties, updates the ENISA certificate website or portal where required, and tracks the case through closure, including any monitoring or follow-up actions. Recording of the decision and required communications shall be completed within **5 business days** of the certificate status decision, and formal case closure shall occur within **10 business days** after all required actions are completed.

5. Detailed Process Description

5.1. Sources of Vulnerability Information

The CB shall accept vulnerability information through defined intake channels from certificate holders, ITSEFs, NCCAs, ENISA communications, public disclosures, coordinated disclosure actors, and other relevant sources. For alignment with Article 33 of Commission Implementing Regulation (EU) 2024/482, the certificate holder shall maintain and publish appropriate methods for receiving information on vulnerabilities related to the certified ICT product from external sources, including users, certification bodies, and security researchers. Information received from an NCCA shall be treated as an official input to the case handling process. It shall be logged and assessed in the same manner as other vulnerability-related information, while taking into account any specific coordination, confidentiality, or follow-up requirements arising under applicable national procedures.

- Certified clients (mandatory reporting)
- NCCAs or ENISA communications
- Public disclosures assessed as potentially relevant
- Evaluation laboratories

Where appropriate, the CB shall acknowledge receipt of vulnerability reports and ensure that each report is traceable throughout assessment, handling, disclosure oversight, certificate review, and any NCCA notification or follow-up required under this procedure.

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	5 of 19

Received vulnerability information shall be managed as follows, with any authority-originated information or related coordination requirements recorded in the case file where applicable:

- Logged in the CB's certification monitoring system
- Assigned a unique reference
- Linked to:
 - Certificate ID
 - Product version/configuration
 - Assurance level (Substantial or High)

5.2. Relevance Assessment, Certificate Review Trigger, Impact Analysis and Technical Input

For alignment with Article 33(3) of Commission Implementing Regulation (EU) 2024/482, where the certificate holder detects or receives information about a potential vulnerability affecting a certified ICT product, it shall record the case and carry out a vulnerability impact analysis. For the purposes of this procedure, this includes cases where the certificate holder receives vulnerability information according to Article 55(1)(c) of the CSA, receives information on a potential vulnerability from the CB that issued the certificate, becomes aware of a new publicly disclosed vulnerability on the referenced online repositories according to Article 55(1)(d) of the CSA that is relevant to the EUCC certified product, or otherwise becomes aware of a potential related vulnerability. Such cases shall be treated as corresponding to the situations referred to in Article 33(3), requiring the certificate holder to record the case and carry out a vulnerability impact analysis.

Upon receipt of vulnerability information, the CB shall assess whether the reported vulnerability is relevant to the certified ICT product and whether it may trigger a review of the EUCC certificate.

In response to a reasonable request from the CB that issued the certificate, the certificate holder shall transmit all relevant information about potential vulnerabilities to the CB to support the relevance assessment, vulnerability impact analysis, certificate review, and any related follow-up under this procedure.



	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	6 of 19

The assessment shall determine whether the vulnerability:

1. Applies to the certified configuration of the ICT product.
2. Falls within the scope of the certified Security Target or applicable Protection Profile.
3. May affect the certified security claims, including relevant Security Functional Requirements (SFRs), or the assurance basis of the certificate.

The possible outcomes of the relevance assessment are:

- Not relevant to the certified ICT product

Where the vulnerability does not apply to the certified configuration or is outside the scope of the certified Security Target or applicable Protection Profile, the case may be closed with a recorded justification explaining why it is not relevant to the EUCC certificate.

- Relevant, but no impact on certificate confirmation

Where the vulnerability is relevant to the certified ICT product but does not affect the certified security claims or the assurance basis of the certificate, the CB may confirm the certificate and define any monitoring actions required during the certificate validity period.

- Relevant and requiring impact analysis

Where the vulnerability is relevant and may affect the certified security claims, the certified configuration, or the assurance basis of the certificate, the certificate holder shall carry out a vulnerability impact analysis and provide the resulting vulnerability impact statement and supporting evidence to the CB. The CB shall review that analysis and determine whether a formal certificate review is required.

The certificate holder shall carry out a vulnerability impact analysis where a vulnerability may:

- Undermine the certified security claims or certified configuration of the ICT product.
- Invalidate the assurance basis of the certificate, including the resistance expected at the achieved assurance level.

	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	7 of 19

Where the above applies, the certificate holder shall carry out and document the vulnerability impact analysis, and the CB shall take the following actions, as applicable:

- Request a vulnerability impact statement and supporting evidence from the certificate holder.
- Obtain technical input from the ITSEF and, where necessary, request re-evaluation of the certified ICT product against the certified Security Target or applicable Protection Profile.
- Determine whether the certificate should be confirmed, remain valid subject to conditions, or be withdrawn and, where applicable, replaced by a new certificate.

5.3. CB Decision and Escalation

Where the relevance assessment and the vulnerability impact analysis provided by the certificate holder indicate that a vulnerability may affect the EUCC certificate, the CB shall make a documented decision on the appropriate next step and determine whether escalation is required. In making that decision, the CB shall consider the significance of the vulnerability and the extent to which the certified configuration, certified security claims, Security Target, or applicable Protection Profile may be affected. The CB shall also consider whether additional evidence or technical work is required, and whether the case requires notification to or coordination with the relevant NCCA.

As part of this step, the CB shall, as applicable:

- Request further information, a vulnerability impact statement, and proposed corrective actions from the certificate holder.
- Obtain technical input from the ITSEF and, where necessary, define the scope of any re-evaluation required to support the certificate review.
- Determine whether the case can remain under routine monitoring, requires coordinated handling and escalation, or must proceed directly to certificate review and status decision.
- Determine whether the case is significant and whether the relevant NCCA shall be notified or otherwise engaged in accordance with this procedure and applicable national requirements.
- Record the rationale for the decision, the responsible parties, the required actions, and the timelines for follow-up.

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	8 of 19

Escalation shall be initiated where the vulnerability may materially affect the validity of the certificate, where the case requires coordinated vulnerability disclosure or engagement with competent authorities, or where the certificate holder does not provide sufficient evidence or corrective action within the period specified by the CB. Where the CB determines that the vulnerability is significant, or where competent authority awareness is otherwise required under the applicable national procedure, the CB shall notify and, where appropriate, engage the relevant NCCA. The output of this step shall determine whether the case proceeds to vulnerability disclosure oversight under §5.4, certificate status decision under §5.5, NCCA notification or follow-up, or a combination of these actions.

For the purposes of this process, a vulnerability shall be treated as significant where one or more of the following criteria apply:

- The vulnerability may invalidate certified security claims, materially affect the certified configuration, or undermine the assurance basis of the certificate.
- The vulnerability affects products or configurations already placed on the market under an EUCC certificate and may expose users or relying parties to material risk.
- The vulnerability requires coordinated vulnerability disclosure, engagement with competent authorities, or urgent remediation measures extending beyond routine monitoring.
- The vulnerability indicates a potential systemic issue, repeated failure of a certified security mechanism, or a material gap in the certificate holder's vulnerability handling or disclosure controls.
- The CB determines, based on technical evidence, certification oversight considerations, or applicable national procedures, that notification or follow-up by the relevant NCCA is necessary.

Where a vulnerability is assessed as significant, the CB shall notify the relevant NCCA without undue delay and, unless national procedures require a shorter period, within **5 business days** of the significance determination. The notification shall be recorded in the case file. It shall include, as applicable, the certificate identifier, product name and affected configuration or version, a summary of the vulnerability and its assessed impact, the current remediation or mitigation status, any certificate review actions initiated by the CB, any planned or ongoing coordinated disclosure actions, and the primary CB contact for follow-up.

Where additional information becomes available after the initial notification, the CB shall provide supplementary updates to the NCCA in accordance with case progression and

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	9 of 19

applicable national procedures. The NCCA may then be engaged by the CB for certification oversight, supervisory coordination, or national follow-up, as applicable. Such engagement shall not displace the CB’s responsibility for certificate review and status decision-making under this procedure.

5.4. Vulnerability Disclosure Oversight

As part of the assessment and certification process defined under SM-01-03a, the CB shall verify that the certificate holder maintains and applies a documented vulnerability management and coordinated vulnerability disclosure procedure for the certified ICT product. For vulnerabilities relevant to the EUCC certificate, the CB shall oversee, as applicable, the completeness and consistency of the process from receipt and verification through impact analysis, remediation, release, and post-release follow-up. Where a case has been assessed as significant under §5.3, or where authority coordination is otherwise required by applicable national procedures, the CB shall ensure that disclosure oversight activities are aligned with any required NCCA notification, coordination, or follow-up.

- The certificate holder shall maintain a clearly defined procedure covering preparation, receipt, acknowledgement, verification, impact analysis, remediation development, verification of corrective actions, release, post-release follow-up, and vulnerability disclosure for vulnerabilities affecting the certified ICT product.
- The procedure shall define intake channels, roles and responsibilities, record-keeping requirements, confidentiality protections, and criteria for assessing whether a reported vulnerability is relevant to the certified configuration, Security Target, or applicable Protection Profile.
- The certificate holder shall verify reported vulnerabilities, assess exploitability and impact, develop and verify remediation or mitigation measures, and provide the CB with a documented impact analysis report, supporting evidence, and proposed communication or advisory inputs where the vulnerability may affect the EUCC certificate.
- Where required by the CB, the certificate holder shall provide supporting technical evidence and cooperate with the ITSEF in relation to technical analysis or re-evaluation.

In overseeing vulnerability disclosure, the CB does not prescribe public disclosure mechanics in every case but shall verify that disclosure and coordination activities are carried out in a controlled manner consistent with the certificate holder’s documented procedure, applicable law, and the protection of users and relying parties.



	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	10 of 19

- Disclosure shall take place only after sufficient verification has been completed and, where feasible, remediation or effective mitigation measures have been prepared, unless earlier communication is required to manage significant risk.
- Where the case requires coordinated vulnerability disclosure, the certificate holder shall cooperate with the CB and, where relevant based on the significance of the case or applicable national procedures, the ITSEF, the NCCA, and the designated CSIRT or other competent coordination actor.
- The CB shall verify that affected stakeholders and competent authorities are informed in accordance with applicable legal, regulatory, and national coordinated disclosure requirements and that any required NCCA-related communications are consistent with the escalation and notification decisions made under §5.3.
- The certificate holder shall maintain records of disclosure decisions, timelines, communications, released advisories, and post-release monitoring, and shall provide them to the CB on request.
- Where remediation, mitigation, or disclosure outcomes affect the basis on which the certificate was issued, the case shall be fed back into the certificate review and status decision process.

The CB shall ensure that the timing and content of disclosure appropriately balance remediation readiness, the need to reduce exposure for users and relying parties, confidentiality obligations, and the requirements of the applicable coordinated vulnerability disclosure framework. Outcomes from this oversight step shall be reflected in the escalation record under §5.3 and, where relevant, in the certificate review and status decision under §5.5.

5.5. Certificate Status Decision

Where the relevance assessment and the vulnerability impact analysis provided by the certificate holder indicate that a vulnerability may affect the basis on which the EUCC certificate was issued, the CB shall initiate a review of the certificate and determine the extent of that review. Where necessary, the CB shall request the ITSEF to perform a re-evaluation of the certified ICT product. Following the results of the review and, where applicable, the re-evaluation, the CB shall determine the appropriate certificate status decision. Where the case has been notified to the relevant NCCA under §5.3, the CB shall ensure that the NCCA is informed of the outcome of the review and any resulting status decision in accordance with applicable national procedures.

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	11 of 19

Confirmation of the Certificate

- The vulnerability does not affect the certified configuration, the scope of the Security Target or applicable Protection Profile, or the certified security claims.
- The vulnerability does not invalidate the assurance basis of the certificate, including the achieved assurance expectations.
- The CB confirms the certificate and records any required monitoring actions.

Review Resulting in Continued Validity Subject to Conditions

- The vulnerability is relevant to the certified ICT product, but the certified claims may remain valid provided that defined corrective actions or mitigations are implemented within the period specified by the CB.
- The CB may require additional evidence from the certificate holder and, where appropriate, technical input or re-evaluation by the ITSEF to confirm that compliance with the certified Security Target or applicable Protection Profile is maintained.
- The certificate remains valid subject to compliance with the defined conditions and any enhanced monitoring measures established by the CB.

Withdrawal of the Certificate and, Where Applicable, Issuance of a New Certificate

The CB shall withdraw the certificate where the review concludes that the certificate can no longer be confirmed. This includes the following circumstances:

- The vulnerability invalidates the certified security claims, the certified configuration, or the assurance basis of the certificate.
- Required corrective actions or mitigations are not implemented within the period specified by the CB.
- The review concludes that the scope of the certified ICT product must change.
- Following withdrawal, the CB may issue a new certificate with an identical scope and extended validity period, or a new certificate with a different scope, where the EUCC review and any required re-evaluation support that outcome.

The outcome of the certificate review and status decision process shall be recorded in the Certification Status Review form or equivalent controlled record. The record shall include, as applicable:

- The vulnerability notification, supporting technical information, and the assessed applicability to the certified ICT product.

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	12 of 19	

- The review scope, the impact analysis, and any request for additional evidence or re-evaluation.
- The CB decision, including the justification for confirmation, continued validity subject to conditions, withdrawal, or withdrawal followed by issuance of a new certificate.
- Communications with the certificate holder, the ITSEF, and, where relevant, the NCCA or other competent coordination actors.

Where significant vulnerabilities affect certificate status or require coordinated handling, the CB shall ensure that the case is escalated and communicated in accordance with applicable EUCC requirements and national procedures. Where the relevant NCCA has been notified or engaged under §5.3, the CB shall provide the NCCA with the outcome of the certificate review, the resulting certificate status decision, and any further follow-up information required for certification oversight, supervisory coordination, or national follow-up.

- The case shall be reported internally and tracked through closure.
- Relevant information shall be made available to the NCCA in accordance with national procedures and the applicable certification oversight arrangements.
- Where coordinated vulnerability disclosure is required, the CB shall cooperate with the certificate holder, the ITSEF, and the competent coordination actors in accordance with the applicable procedure.

Where the certificate status changes following review, the CB shall ensure that the status of the certificate is updated on the ENISA certificate website or portal, as applicable, without undue delay.

	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	13 of 19

Annex A – Responsibility Matrix

Activity	Certificate Holder	CB	ITSEF	NCCA
Receipt and logging of vulnerability information	Reports vulnerabilities and provides relevant initial information where identified or received.	Receives, logs, acknowledges where appropriate, assigns a reference, and links the case to the certificate and product scope.	May provide vulnerability-related information to the CB where relevant.	May provide official vulnerability-related information or notifications requiring follow-up.
Relevance assessment	Provides supporting information on applicability to the certified product, configuration, and scope.	Assesses whether the vulnerability is relevant to the certified ICT product and whether certificate review may be triggered.	Provides technical clarification where requested by the CB.	May be informed where the case has authority relevance under national procedures.
Vulnerability impact analysis	Carries out and documents the vulnerability impact analysis and submits the impact statement and evidence to the CB.	Reviews the analysis and determines whether further action, review, or escalation is required.	Provides technical input and may support analysis of impact on the Security Target or Protection Profile.	Normally not directly involved unless significance or oversight considerations arise.
Technical input and re-evaluation	Provides technical evidence and cooperates with re-evaluation activities where required.	Requests technical input or defines the scope of any re-evaluation needed to support certificate review.	Performs technical analysis and, where requested, re-evaluation of the certified ICT product.	May be informed if re-evaluation outcomes have oversight significance.



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	14 of 19	

Activity	Certificate Holder	CB	ITSEF	NCCA
CB decision and escalation	Provides additional information, corrective action proposals, and supporting evidence as requested.	Determines the next step, records the rationale, and decides whether escalation, certificate review, or routine monitoring applies.	Supports the CB with technical input where needed for escalation decisions.	Is notified or engaged where significance criteria or national procedures require authority awareness or coordination.
Vulnerability disclosure oversight	Maintains and applies the vulnerability management and coordinated disclosure procedure, including remediation, communication, and record-keeping.	Oversees the completeness and consistency of disclosure-related activities and verifies alignment with certificate obligations.	Cooperates on technical aspects of coordinated handling where required.	May be coordinated with where required by significance, national procedure, or competent authority involvement.
Certificate review and status decision	Provides evidence, implements required corrective actions, and supports review activities.	Reviews certificate impact and decides whether the certificate is confirmed, remains valid subject to conditions, or is withdrawn and replaced where applicable.	Performs re-evaluation where requested and provides technical findings to support the CB decision.	Receives outcome information where notified or engaged under the escalation process.
Notification and authority coordination	Supports the CB with relevant information needed for authority-related follow-up.	Notifies the relevant NCCA where significance criteria are met and provides follow-up information as required.	May support the CB with technical inputs relevant to authority coordination.	Receives notifications, supports certification oversight, supervisory coordination, or national follow-up as applicable.



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	15 of 19

Activity	Certificate Holder	CB	ITSEF	NCCA
Recording, communication, and closure	Provides final supporting records and cooperates with closure and any monitoring actions.	Records outcomes, communicates decisions, updates certificate status where required, and tracks the case through closure.	Provides any final technical input or supporting records requested by the CB.	May receive final status or follow-up information where required by national procedures.



	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	16 of 19

Annex B – EUCC Traceability Table

Procedure Section	Topic	EUCC Reference	Traceability Note
Section 1 and Section 2	Purpose and scope of lifecycle vulnerability handling	Implementing Regulation (EU) 2024/482, Article 1; Article 2; Chapter II context	These sections position the procedure within the EUCC certification lifecycle for ICT products and support the application of scheme obligations to issued certificates.
Section 3	Roles and responsibilities of certificate holder, CB, ITSEF, and NCCA	Implementing Regulation (EU) 2024/482, Articles 7 to 14; Article 33; Article 48 context; ENISA EUCC Vulnerability Management and Disclosure Guidelines	This section operationalises the respective duties of the key actors involved in vulnerability handling, certificate review, and authority coordination under the EUCC framework.
Section 4	Process overview from receipt to closure	Implementing Regulation (EU) 2024/482, Article 13; Article 14; Article 33; ENISA EUCC Vulnerability Management and Disclosure Guidelines, Sections 3 and 4	The staged workflow reflects the expected lifecycle handling of vulnerabilities, including intake, impact analysis, disclosure oversight, certificate review, and status decision.
Section 5.1	Sources, receipt, and logging of vulnerability information	Implementing Regulation (EU) 2024/482, Article 33(1) and Article 33(3); ENISA EUCC Vulnerability Management and Disclosure Guidelines, Preparation and Receipt	This section supports the obligation to maintain and publish appropriate methods for receiving vulnerability information and to capture relevant inputs for later assessment.



	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	17 of 19

Procedure Section	Topic	EUCC Reference	Traceability Note
Section 5.2	Relevance assessment, impact analysis, and technical input	Implementing Regulation (EU) 2024/482, Article 33(3); CSA Article 55(1)(c) and Article 55(1)(d); Article 13 context; ENISA EUCC Vulnerability Management and Disclosure Guidelines, Verification and Impact Analysis Report	This section aligns with the certificate holder obligation under Article 33(3) to record potential vulnerabilities and carry out a vulnerability impact analysis, including where vulnerability information is received under Article 55(1)(c) of the CSA, from the issuing CB, through new publicly disclosed vulnerabilities on the referenced online repositories under Article 55(1)(d) of the CSA that are relevant to the EUCC certified product, or through other related sources.
Section 5.3	CB decision, escalation, and NCCA notification	Implementing Regulation (EU) 2024/482, Article 13; Article 14; Article 33; Article 48 context; ENISA EUCC Vulnerability Management and Disclosure Guidelines, coordinated handling and authority interaction	This section translates EUCC certificate review and withdrawal concepts into operational escalation and authority-coordination decisions where vulnerability significance or certificate validity is affected.
Section 5.4	Vulnerability disclosure oversight	Implementing Regulation (EU) 2024/482, Article 33(1), Article 33(3), and Article 33(4); ENISA EUCC Vulnerability Management and Disclosure Guidelines, Sections 3 to 4	This section supports the maintenance of vulnerability management and disclosure arrangements, oversight of coordinated handling, and the broader communication duties linked to vulnerabilities affecting certified products.



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	18 of 19

Procedure Section	Topic	EUCC Reference	Traceability Note
Section 5.5	Certificate review, status decision, and follow-up communications	Implementing Regulation (EU) 2024/482, Article 13; Article 14; Article 10 context; ENISA EUCC Vulnerability Management and Disclosure Guidelines, Release and Post-release	This section maps the vulnerability-handling outputs back into the formal EUCC certificate lifecycle, including review outcomes, withdrawal scenarios, and related communications.
Annex A	Responsibility matrix	Implementing Regulation (EU) 2024/482, Article 33 and related actor responsibilities; ENISA EUCC Vulnerability Management and Disclosure Guidelines	The matrix provides an operational view of how EUCC-related responsibilities are distributed across the certificate holder, CB, ITSEF, and NCCA for each major activity.

Note: References to the ENISA EUCC Vulnerability Management and Disclosure Guidelines in this annex are included to show how this procedure aligns with the recommended operational handling model that supports implementation of the EUCC scheme. These references complement, but do not replace, the regulatory requirements set out in Implementing Regulation (EU) 2024/482.



	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01a
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	19 of 19

Version History

Version	Date	Author	Summary of changes	Status
1	21-05-2026	Khalimatou Samirah (NSAI)	Initial draft created.	Draft
2	29-05-2026	Khalimatou Samirah (NSAI)	Updated sections as per review comments	Approved

