	<h1 style="text-align: center;">CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	1 of 14

1. Purpose

This document defines the process applied by [Certification Body] (the **Certification Body (CB)**), acting as a conformity assessment body, including where designated as a notified body, under Regulation (EU) 2024/2847 (Cyber Resilience Act), for the assessment of a certificate holder’s vulnerability handling capabilities.

The purpose of this process is to verify that certificate holders have established and implemented vulnerability handling processes that support compliance with Annex I and Articles 13 and 14 of the Cyber Resilience Act, without the CB assuming operational responsibility for vulnerability management or incident response.

2. Scope

This process applies to all CRA conformity assessment activities where third-party assessment is required under Article 32 of Regulation (EU) 2024/2847, including:


- EU-type examination (Module B)
- Conformity to type in conjunction with Module B (Module C)
- Full quality assurance (Module H), where applicable

This process covers products with digital elements (hardware, software, and remote data solutions) within the CRA scope and shall align with the requirements of SM-01-03b. For critical products, EUCC shall also be taken into account where applicable.

3. Roles and Responsibilities

Role	Responsibility
Certificate holder	<ul style="list-style-type: none"> - Vulnerability identification, remediation, and disclosure; - Incident and vulnerability reporting to ENISA and users; - Operational cybersecurity activities throughout the product lifecycle.




	<h1 style="text-align: center;">CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	2 of 14

Role	Responsibility
CB acting as Notified Body	<ul style="list-style-type: none"> - Assesses the existence, adequacy, and documented implementation of vulnerability handling processes required under the CRA; - Verifies certificate holder preparedness to comply with Article 14 reporting obligations; - Limits its activities to conformity assessment and does not perform vulnerability management or incident response.
National competent authority / market surveillance authority, as applicable	<ul style="list-style-type: none"> - Performs the market surveillance and regulatory oversight functions assigned under the CRA, where applicable; - Receives notifications and information as required under the applicable legal and regulatory framework; - Acts independently from the CB's conformity assessment activities and does not replace the certificate holder's operational responsibilities.
Coordinator CSIRT	<ul style="list-style-type: none"> - May receive voluntary reports and other relevant notifications under Article 15 of the CRA, where applicable; - May transmit information to the certificate holder, including notifications concerning reported vulnerabilities or incidents affecting the product; - Acts as a relevant coordination and communication point in the handling of reported vulnerabilities or incidents, without replacing the certificate holder's responsibility for vulnerability handling and reporting.

4. Process Overview

1. **Assessment initiation and planning** – The CB confirms the applicable conformity assessment route, defines the scope of the assessment, and identifies the vulnerability handling evidence to be reviewed as part of the CRA certification and assessment plan.
2. **Document and evidence review** – The CB reviews the certificate holder's documented vulnerability handling arrangements, including policies, procedures, roles, reporting channels, disclosure contact points, templates, selected records, and other objective evidence showing that the process is defined and operational.
3. **Verification of process coverage** – The CB verifies that the certificate holder's process covers intake of vulnerability information, analysis and classification, remediation and mitigation, communication with users and stakeholders where appropriate, and handling throughout the declared support period.



	<h1 style="text-align: center;">CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	3 of 14

4. **Assessment of linkage to the cybersecurity risk assessment** – The CB confirms that vulnerability handling is connected to the certificate holder’s cybersecurity risk assessment so that identified vulnerabilities can be prioritised, reassessed, and reflected in the supporting technical documentation where required.
5. **Verification of Article 14 notification preparedness** – The CB verifies, as assessment criteria, that the certificate holder has established procedures to support notification to ENISA within 24 hours of becoming aware of an actively exploited vulnerability or severe incident in accordance with Article 14(1), procedures to notify users where required under Article 14(3), and capability to use the ENISA Single Reporting Platform established pursuant to Article 16 for the required notifications.
6. **Recording of findings and non-conformities** – Any gaps, inconsistencies, or insufficient evidence are recorded within the conformity assessment process, including failures to demonstrate preparedness against Article 14(1) and Article 14(3) verification criteria, and the certificate holder may be required to provide clarification or corrective action before the assessment is finalised.
7. **Conclusion and input to the conformity assessment decision** – The outcome of the vulnerability handling assessment is incorporated into the overall CRA conformity assessment record and supports the final certification review and decision-making process.

This section summarises the main stages followed by the CB when assessing a certificate holder’s vulnerability handling capability as part of CRA conformity assessment, including verification of preparedness to meet Article 14(1) ENISA notification and Article 14(3) user notification obligations.


5. Detailed Process Description

5.1. General assessment approach

As part of the assessment process set out in SM-01-03b, vulnerability handling is subject to a comprehensive review. This review ensures that the necessary procedures and requirements have been addressed by the certificate holder.

In assessing these arrangements, the CB may use ISO/IEC 29147:2018 (vulnerability disclosure) and ISO/IEC 30111:2019 (vulnerability handling processes) as recognised references to support evaluation of whether the certificate holder’s processes are consistent with the applicable CRA obligations.



	<h1 style="text-align: center;">CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	4 of 14

- The assessment includes a detailed examination of the Annex I requirements. This step verifies that the certificate holder’s vulnerability handling processes align with the relevant regulatory and scheme-specific obligations.
- Additionally, a review of the cybersecurity risk assessment is conducted. This ensures that the certificate holder has properly evaluated and documented the risks associated with the ICT product, and that effective measures are in place to address identified vulnerabilities.

Evidence reviewed by the CB may include:

- Vulnerability handling policies and procedures;
- Vulnerability disclosure policy and public contact information for external reporting;
- Case tracking records, templates, and selected historical examples covering intake, analysis, remediation, and disclosure;
- Training and role descriptions.

The CB will not require unnecessary disclosure of sensitive technical vulnerability details beyond what is needed to demonstrate process capability.

5.2. Verification of vulnerability handling processes

During the assessment, the CB verifies that the certificate holder has documented vulnerability handling and disclosure processes that are consistent with the CRA and aligned, where appropriate, with ISO/IEC 30111:2019 for internal vulnerability handling processes and ISO/IEC 29147:2018 for external vulnerability disclosure arrangements.

For the purposes of this assessment, an **exploited vulnerability** should be understood as a vulnerability for which there is evidence that it has been used to compromise, misuse, or adversely affect a product with digital elements or a related environment. An **actively exploited vulnerability** is a narrower notion and refers to a vulnerability for which exploitation is ongoing, has recently occurred, or is otherwise credibly reported as taking place in the wild. The distinction is relevant because not every exploitable or theoretically exploitable vulnerability is an actively exploited vulnerability, and the certificate holder should have criteria for recognising when available information indicates actual exploitation rather than only potential exploitability.

1. Intake of vulnerability information

- Internal detection mechanisms;



- External reporting channels and designated public contact points for vulnerability disclosure;
- Handling of information from third parties, researchers, and other coordinated vulnerability disclosure participants.

2. Vulnerability analysis and classification

- Verification, triage, and severity assessment;
- Evaluation of exploitability and impact;
- Prioritisation based on risk and product context.

3. Remediation and mitigation

- Development, testing, release, and deployment of security updates or mitigations;
- Tracking of remediation actions, dependencies, and status through to resolution or justified closure.

4. Communication

- Procedures for coordinated vulnerability disclosure and communication with reporters and other relevant stakeholders;
- Procedures for informing users and publishing remediation information where appropriate.

5. Vulnerability handling during the support period


The CB verifies that, during the support period, the vulnerability handling processes:

- Remain applicable throughout the declared support period;
- Align the declared support period with the certificate holder's demonstrated capability to provide security updates;
- Are reflected consistently in technical documentation and user information.

5.3. Link to cybersecurity risk assessment

The CB verifies that vulnerability handling activities are logically and demonstrably linked to the certificate holder's cybersecurity risk assessment, including:

- Use of risk assessment outputs to prioritise vulnerability remediation;
- Reassessment of cybersecurity risks following significant vulnerabilities;

	<h1 style="text-align: center;">CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	6 of 14

- Documentation of residual risks and risk acceptance decisions where applicable.

5.4. Preparedness assessment


As part of the conformity assessment, the CB verifies, as assessment criteria, that the certificate holder has established procedures enabling compliance with Article 14 of the Cyber Resilience Act, including Article 14(1) notification to ENISA within 24 hours of becoming aware of an actively exploited vulnerability or severe incident, and Article 14(3) notification to users where required. In making this assessment, the CB may consider whether the certificate holder's disclosure and handling arrangements are aligned, where appropriate, with ISO/IEC 29147:2018 and ISO/IEC 30111:2019.

The CB may also verify whether the certificate holder has arrangements to address the **voluntary reporting** provisions of Article 15 of the CRA, under which certificate holders and other natural or legal persons may notify vulnerabilities, cyber threats affecting the risk profile of a product with digital elements, incidents having an impact on the security of the product, and relevant near misses to the coordinator CSIRT or ENISA on a voluntary basis.

The assessment may also consider whether the certificate holder has defined how it will interact with the relevant coordinator CSIRT, including receipt and handling of notifications, cooperation where appropriate in relation to reported vulnerabilities or incidents, preservation of confidentiality, and escalation of relevant information within the certificate holder's organisation. In this context, the assessment may consider whether the certificate holder can recognise when voluntary reporting may be appropriate and handle notifications received from the coordinator CSIRT where a third party has reported an actively exploited vulnerability or a severe incident affecting the certificate holder's product.

- Internal processes to identify actively exploited vulnerabilities and severe incidents;
- Defined criteria and internal decision-making processes for determining reportability;
- Procedures and capability to notify ENISA within 24 hours in accordance with Article 14(1);
- Procedures to notify users where required under Article 14(3);
- Capability to use the ENISA Single Reporting Platform established pursuant to Article 16 for required notifications;
- Procedures for submitting follow-up and final reports where applicable.



	<h1 style="text-align: center;">CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	7 of 14

The CB verifies preparedness and capability only and does not validate the correctness of actual incident reports.

5.5. Distinction between Module H surveillance and the type-examination approach under Modules B+C

Where the conformity assessment is performed under Modules B and C, the CB assesses the product type through EU-type examination and determines whether the technical design and supporting evidence demonstrate compliance for the type examined. Under Module C, conformity to type is then maintained by the certificate holder through internal production control, and the CB does not perform ongoing surveillance of the quality system under that route.

By contrast, under Module H, the CB assesses and approves the certificate holder's full quality assurance system covering design, development, final inspection and testing, and vulnerability handling arrangements within the approved scope. The CB then performs periodic surveillance of that approved system to verify that it continues to be properly implemented and remains capable of supporting compliance with the applicable CRA requirements.

- **Modules B+C:** assessment is centred on the examined product type and the associated technical documentation, with the certificate holder responsible for maintaining conformity to the approved type under Module C.
- **Module H:** assessment is centred on the certificate holder's approved quality system, including vulnerability handling processes, with continuing CB surveillance after approval.
- **Practical implication:** for vulnerability handling, Modules B+C focus on whether the relevant arrangements for the assessed product type are adequate at the point of examination, whereas Module H additionally requires confidence that the certificate holder's quality system can sustain those arrangements on an ongoing basis across the approved scope.

6. Impact on Conformity Assessment Decisions

For the purposes of CRA conformity assessment, the CB shall classify findings related to vulnerability handling as major or minor non-conformities according to their effect on the certificate holder's ability to meet the applicable Annex I requirements and Article 14 preparedness obligations. The classification shall also determine the urgency of corrective action and whether escalation to certification suspension is warranted.



- **Major non-conformity:** a complete absence of a required vulnerability handling or disclosure process, or a breakdown that materially affects the certificate holder's capability to meet applicable CRA requirements.
 - A finding shall normally be classified as major where it indicates systemic failure, repeated breakdown, or lack of effective implementation, including failure to establish procedures for Article 14(1) ENISA notification, Article 14(3) user notification, or use of the ENISA Single Reporting Platform where required.
 - A finding may also be classified as major where the certificate holder cannot demonstrate control of vulnerability intake, triage, remediation, disclosure, or support-period activities for the product scope under assessment, or where multiple related minor non-conformities together indicate loss of process effectiveness.
- **Minor non-conformity:** an isolated lapse, limited documentation gap, or implementation weakness that does not by itself materially affect the overall capability of the certificate holder's vulnerability handling process to achieve its intended outcome.
 - A finding shall normally be classified as minor where the required process exists and is generally implemented, but evidence of completeness, consistency, timeliness, or record-keeping is insufficient for one aspect of the assessed scope.
 - Repeated failure to correct a minor non-conformity, or the identification of several related minor non-conformities in the same process area, may justify reclassification as a major non-conformity.

For a major non-conformity, the certificate holder shall submit a root-cause analysis and a corrective action plan within 14 calendar days and provide objective evidence of implementation within 60 calendar days, unless a shorter period is justified by the risk.


For a minor non-conformity, the certificate holder shall submit a corrective action plan within 30 calendar days and implement the action within 90 calendar days or before the next certification decision or surveillance activity, whichever comes first. If the certificate holder fails to provide an acceptable response within these periods, or if the non-conformity remains unresolved and materially affects continued confidence in conformity, the CB may escalate the matter to limitation or suspension of certification in accordance with the applicable module and certification decision process.

Deficiencies in vulnerability handling processes that result in non-conformity with Annex I or inadequate preparedness for Article 14 obligations shall be treated as non-conformities and may result in:

CRA Vulnerability Handling process

Document:	TB-VH-01-01b
Revision:	2.0
Date issued:	DD-MM-YYYY
Owner:	To be determined
Page:	9 of 14

- Refusal to grant certification;
- Certification with conditions;
- Limitation, suspension, or withdrawal of certification, depending on severity and module applied.

	<h1>CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	10 of 14

Annex A – Application Process flow

The table below summarises the main activities and actions of the key stakeholders involved in the application and conformity assessment process.


Step	Certificate holder	CB	National authority	Coordinator CSIRT	ENISA
1. Application and submission	Prepares and submits the application, technical documentation, and supporting evidence.	Receives the application, confirms the applicable route, and plans the assessment.	No routine action at this step unless required by the legal framework.	No routine action.	No routine action.
2. Document and evidence review	Provides clarifications, records, and additional evidence on request.	Reviews the documented vulnerability handling arrangements and supporting evidence.	No routine action unless information is requested under the applicable framework.	No routine action.	No routine action.
3. Vulnerability handling assessment	Demonstrates process implementation, support-period arrangements, and decision criteria.	Assesses process coverage, linkage to risk assessment, and preparedness for Article 14 obligations.	No direct role in the assessment decision.	May become relevant if coordination arrangements are reviewed.	May be referenced where reporting platform capability is assessed.
4. Findings and corrective action	Responds to findings, submits corrective action plans, and provides evidence of implementation.	Records non-conformities, evaluates responses, and determines whether issues are resolved.	May become involved if regulatory escalation is required.	No routine role unless a reported issue triggers coordination.	No routine role unless reporting obligations are triggered.



CB Logo	<h1>CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	11 of 14

Step	Certificate holder	CB	National authority	Coordinator CSIRT	ENISA
5. Certification decision and follow-up	Maintains conformity, supports surveillance where applicable, and fulfils ongoing obligations.	Uses the assessment outcome to support certification decision-making and later surveillance, where applicable.	May receive notifications or take action under the applicable framework after certification.	May receive voluntary reports or communicate relevant information where incidents or vulnerabilities arise.	Receives Article 14 notifications and supports the reporting framework where required.




	<h1>CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	12 of 14

Annex B – Coverage of this procedure against relevant CRA provisions

The table below provides a high-level mapping between this procedure and the relevant provisions of Regulation (EU) 2024/2847 (Cyber Resilience Act) that are addressed through the conformity assessment activities described in this document.


CRA provision	Subject	Coverage in this procedure	Relevant sections
Annex I, Part I	Essential cybersecurity requirements for product design, development, and production	Covered indirectly through the review of technical documentation, product-related risk assessment, and the linkage between vulnerability handling and the assessed product scope.	1, 4, 5.1, 5.3, 6.1
Annex I, Part II	Vulnerability handling requirements	Covered directly through the assessment of intake, analysis, classification, remediation, disclosure, support-period handling, and preparedness for reporting obligations.	1, 4, 5.1, 5.2, 5.4, 6.1
Article 13	Obligations of manufacturers / certificate holders in relation to vulnerability handling and cybersecurity risk assessment	Covered through the review of vulnerability handling arrangements, cybersecurity risk assessment, support-period considerations, and evidence that the process is established and implemented.	1, 4, 5.1, 5.2, 5.3
Article 14	Reporting obligations for actively exploited vulnerabilities and severe incidents	Covered directly through preparedness assessment of identification, internal escalation, reportability criteria, ENISA notification capability, user notification procedures, and follow-up reporting arrangements.	3, 4, 5.4, 6.1, Annex A



	<h1>CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	13 of 14

CRA provision	Subject	Coverage in this procedure	Relevant sections
Article 15	Voluntary reporting	Covered through assessment of whether the certificate holder has arrangements for voluntary reporting and interaction with the coordinator CSIRT, including confidentiality and handling of notifications.	3, 5.4, Annex A
Article 16	Single reporting platform	Covered through verification that the certificate holder has the capability to use the ENISA Single Reporting Platform for required notifications.	4, 5.4, Annex A
Article 31	Technical documentation	Covered through document and evidence review, including technical documentation and the cybersecurity risk assessment used to support the conformity assessment.	4, 5.1, 5.3
Article 32	Conformity assessment procedures	Covered through the scope of this procedure for Modules B, C, and H, including the distinction between type examination and quality-system surveillance.	2, 4, 5.5, Annex A



	<h1>CRA Vulnerability Handling process</h1>	Document:	TB-VH-01-01b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	14 of 14

Version History

Version	Date	Author	Summary of changes	Status
1	21-04-2026	Khalimatou Samirah (NSAI)	Initial draft created.	Draft
2	29-05-2026	Khalimatou Samirah (NSAI)	Updated sections as per review comments,	Approved

