	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	1 of 27

1. Purpose

This document defines the internal process followed by the Certification Body (CB) for conformity assessment to determine whether a product with digital elements and the manufacturer's processes meet the essential cybersecurity requirements in Annex I, thereby supporting CE marking under the CRA.

2. Scope

This document defines the internal process followed by [Certification Body] acting as a conformity assessment body / notified body under Regulation (EU) 2024/2847 (Cyber Resilience Act) for the performance of third-party conformity assessment procedures pursuant to Article 32.

The process determines whether a product with digital elements, and where applicable the manufacturer's or any other economic operator's quality and vulnerability-handling processes, conform to the essential cybersecurity requirements set out in Annex I of the CRA, thereby supporting the manufacturer's EU Declaration of Conformity and CE marking.

This process applies where third-party conformity assessment is required under the CRA, including for important products with digital elements as defined in Article 7 and Annex III, and for critical products with digital elements as defined in Article 8 and Annex IV of Regulation (EU) 2024/2847. It may also be applied where a manufacturer voluntarily chooses an applicable third-party conformity assessment route under the CRA and requests certification by the CB.

The following reference documents apply to this procedure:


- Regulation (EU) 2024/2847 (Cyber Resilience Act) — Article 1 (subject matter), Article 2 (scope), Article 3 (definitions), Article 6 (essential cybersecurity requirements), Article 7 (important products with digital elements), Article 8 (critical products with digital elements), Article 10 (free movement), Article 13 (obligations of manufacturers), Article 14 (reporting obligations of manufacturers), Articles 24 to 29 (EU declaration of conformity, CE marking, and general principles and rules of the conformity assessment framework), Article 31 (notification of conformity assessment bodies), Article 32 (conformity assessment procedures), the CRA provisions on conformity assessment bodies, notifying authorities, notified bodies and notification, and the CRA provisions on

market surveillance and enforcement, Annex I (essential cybersecurity requirements), Annex III (important products with digital elements), and Annex IV (critical products with digital elements)

- Commission Implementing Regulation (EU) 2025/2392 — technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847
- European Commission CRA guidance and related official interpretive materials — used as supporting interpretive references for application of Regulation (EU) 2024/2847, including notified body, market surveillance, and implementation context
- ISO/IEC 17065 — Conformity assessment — Requirements for bodies certifying products, processes and services
- ISO/IEC 17021-1 — Conformity assessment — Requirements for bodies providing audit and certification of management systems — referenced as a supporting source of relevant audit principles where appropriate to structure evaluation of documented quality assurance arrangements under Module H

3. Roles and Responsibilities

Role	Responsibility
Economic operator (for example, manufacturer, importer, or distributor)	<ul style="list-style-type: none"> - Shall ensure that the product is designed, developed, and produced in line with the Annex I essential requirements and shall undertake and document a cybersecurity risk assessment, update it during the support period, and include it in the technical documentation. - Shall prepare and maintain the technical documentation required for conformity assessment and CE marking, including, but not limited to, the cybersecurity risk assessment. - Shall maintain the arrangements, processes, and records necessary to support compliance with applicable post-market obligations under the CRA, including Article 14 and Article 15 obligations where relevant.
Certification body (CB) / Notified Body	<ul style="list-style-type: none"> - Shall perform conformity assessment activities strictly within the scope of its notification under Article 32.

	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	3 of 27

Role	Responsibility
	<ul style="list-style-type: none"> - Shall verify conformity with Annex I requirements through documented evidence assessment.
Market surveillance authorities / Notifying Authority	<ul style="list-style-type: none"> - The Notifying Authority designates, notifies, and oversees the notified body, including matters affecting notification scope, competence, and continued fulfilment of notification conditions. - Market surveillance and enforcement are carried out by competent national authorities and remain distinct from the CB's certification activities.

4. Process Overview

- Application review and determination of the applicable CRA conformity assessment module under Article 32.
- Conformity assessment planning, execution, and reporting.
- Certification decision and issuance of the certification outcome.
- Maintenance, surveillance, renewal, reduction, suspension, and withdrawal of certification.

5. Detailed Process Description


5.1. Application review

The application review shall be carried out in accordance with procedure SM-01-02 and shall additionally confirm the following:

- Whether third-party conformity assessment is mandatory under Article 32, or whether the manufacturer has voluntarily selected an applicable third-party route;
- Whether the product is classified as an important product or a critical product;
- Whether the Certification Body holds a valid notification covering the relevant product category; where any restriction, uncertainty, or issue affecting notified scope is identified, the matter shall be handled in accordance with section 5.9 Notifying authority interaction and market surveillance authority cooperation

Where a product relies on remote data processing solutions, the CB shall verify and document whether such processing is:

- Developed under the responsibility of the manufacturer; and

	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	4 of 27

- Functionally indispensable for the product to perform at least one intended function.

This review determines CRA applicability and the scope of the assessment.


At the end of this stage, the product shall be registered in the system. All related documentation, including the completed application form, completed application review form, and the signed contract or, where applicable, the rejection letter, shall be formally recorded. This ensures that all necessary materials are documented as part of the application review process. The file shall be assigned to a competent and independent CB assessor in accordance with [RES-01-01](#).

5.2. Technical competence domains for CRA assessors

Technical competence for CRA conformity assessment personnel shall be defined, evaluated, and authorised in accordance with [RES-01-01](#). For CRA activities, the competence matrix shall identify the functions a person is approved to perform, such as application review, assessment, independent technical review, certification decision support, and complaints or appeals review, together with the relevant technical domains for the product category and assessment route.

At a minimum, the [RES-01-01](#) competence matrix shall define and maintain competence domains covering:

- CRA legal and procedural knowledge, including Regulation (EU) 2024/2847, Annex I, Annex III, Annex IV, Article 32 route selection, Article 14 reporting obligations, and the CB's obligations as a conformity assessment body / notified body;
- Secure product development, product architecture, and technical documentation review for products with digital elements;
- Cybersecurity risk assessment, threat analysis, vulnerability management, security update management, and coordinated vulnerability handling;
- Assessment of Annex I Part I product requirements and Annex I Part II process requirements;
- Conformity assessment route execution, including Module B + C, Module H, and evaluation of European cybersecurity certification scheme evidence where applicable;
- Assessment of manufacturer preparedness for post-market obligations, including Article 14 notification and user communication arrangements;
- Product-category-specific technical knowledge necessary for the relevant important or critical product type under the CRA, including supporting

	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	5 of 27

technologies, deployment context, interfaces, and security-relevant operational characteristics;

- Competence for independent review and certification decision support, including the ability to evaluate assessment sufficiency, traceability of findings, and appropriateness of certification recommendations; and
- Competence for handling CRA-related complaints, appeals, and authority-facing escalation where relevant to the assigned function.

The depth of competence required shall be determined according to the assessor’s role, the complexity of the product, the selected assessment route, and any reliance on external evidence such as harmonised standards, common specifications, or applicable European cybersecurity certification schemes. Where necessary, the CB may assign additional technical experts, provided their competence and authorisation are recorded under [RES-01-01](#) and the CB retains responsibility for the conformity assessment outcome.

Before assignment, the CB shall confirm that the assessor or assessment team collectively covers the required competence domains for the application. Any identified competence gap shall be resolved through reassignment, addition of an authorised technical expert, or other action permitted under [RES-01-01](#) before the assessment proceeds.


5.3. Assessment plan

During this stage, the CB selects the appropriate assessment route.

The CB selects the assessment route based on the documented product classification under Regulation (EU) 2024/2847 and the applicable provisions of Article 32. For important products with digital elements falling under Class I in Annex III, Article 32(2) requires third-party conformity assessment where harmonised standards, common specifications or an applicable European cybersecurity certification scheme at assurance level at least substantial have not been applied, have been applied only in part, or do not exist; in such cases, the manufacturer may choose either Module B + C or Module H.

For important products with digital elements falling under Class II in Annex III, Article 32(3) provides that the manufacturer may choose either Module B + C or Module H, or, where available and applicable, a European cybersecurity certification scheme at assurance level at least substantial.

For critical products with digital elements falling under Annex IV, the CB shall determine and document the applicable conformity assessment route in accordance with the CRA

	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	6 of 27


provisions governing critical products and any available and applicable European cybersecurity certification scheme, rather than presuming a single route solely from the classification. The classification decision, legal basis, and selected route must be recorded in the application review and assessment plan.

Where the CRA does not make third-party conformity assessment mandatory for the product, the manufacturer may nevertheless choose an applicable third-party route and request assessment by the CB. In such cases, the CB shall document that the route was selected voluntarily by the manufacturer and shall apply the same route-specific assessment, evidence, and decision criteria as for a mandatory third-party assessment.

Harmonised standards do not constitute a conformity assessment route in themselves, but they are relevant to whether third-party conformity assessment is triggered and to how conformity is demonstrated.

For Annex III Class I important products under Article 32(2), full application of the relevant harmonised standards may support the manufacturer's demonstration of conformity with the applicable Annex I requirements and can affect whether third-party assessment is required for the product. Where harmonised standards are not available, are applied only in part, or do not cover all applicable Annex I requirements, the remaining requirements shall be assessed through the selected third-party route and documented in the assessment plan.

Product classification	Decision criteria	Applicable route	Assessor record
Important product, Annex III Class I	Article 32(2): third-party assessment required where harmonised standards, common specifications or an applicable European cybersecurity certification scheme at assurance level at least substantial are not applied, are only partly applied, or do not exist.	Module B + C or Module H	Record classification, missing/partial standards position, legal basis, and selected route.

	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	7 of 27	

Product classification	Decision criteria	Applicable route	Assessor record
Important product, Annex III Class II	Article 32(3): manufacturer may choose third-party assessment or, where available and applicable, a European cybersecurity certification scheme at assurance level at least substantial.	Module B + C, Module H, or applicable certification scheme	Record classification, legal basis, selected route, and scheme applicability where relied on.
Critical product, Annex IV	Determine the applicable route under the CRA provisions governing critical products and any available and applicable European cybersecurity certification scheme; do not presume a single route solely from the classification.	Route determined by applicable CRA provision and, where relevant, certification scheme	Record classification, applicable legal provision, selected route, and justification for any scheme used.


Following selection of the assessment route, the CB shall prepare an assessment plan aligned with the certification scope. The assessment plan shall include:

- Review of the technical documentation, submitted evidence, and cybersecurity risk assessment associated with the product;
- Identification of any applicable harmonised standards or common specifications relied on by the manufacturer, the extent of their application, and any Annex I requirements that remain to be assessed directly through the selected third-party route;
- Assessment of the implementation of the applicable Annex I Part I and Part II requirements by the client, including the assessment method, conformity determination, and any justified “not applicable” decisions.

The output of this process shall be documented on the applicable assessment plan record and shared with the client in advance of the assessment, where required by the certification scheme.

5.4. Assessment execution and report

This section describes the execution of the selected assessment route and the recording of the assessment results.

	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	8 of 27

5.4.1. Assessment routes

The CB shall execute the assessment route selected and documented in the assessment plan, in accordance with the applicable provisions of Article 32 and the product classification recorded for the application.

Module B + C (EU-type examination + conformity to type)

1. Where selected for an Annex III Class I or Class II important product under Article 32(2) or 32(3), perform EU-type examination of the product evidence set, including review of technical documentation, cybersecurity risk assessment, and conformity with the applicable Annex I product requirements.
2. Verify the manufacturer's arrangements to ensure continued conformity of production with the approved type and the applicable CRA requirements.

Module H (Full quality assurance)


Where Module H requires evaluation of the manufacturer's documented quality assurance arrangements, the CB shall perform the assessment within its product certification framework consistent with ISO/IEC 17065. Relevant audit principles from ISO/IEC 17021-1 may be used where appropriate to structure evaluation of documented processes and their implementation, but do not constitute a separate certification basis and do not change the CRA conformity assessment route, criteria, or the CB's product certification responsibility.

1. Where selected under the applicable CRA provisions, assess the manufacturer's full quality assurance arrangements, including the processes put in place to ensure conformity with the applicable Annex I requirements and, where relevant, the vulnerability-handling and update processes.
2. Confirm that the approved quality system is capable of ensuring that products placed on the market or made available continue to meet the applicable product and process requirements covered by the selected route.

European cybersecurity certification scheme used as evidence

Where an applicable European cybersecurity certification scheme is relied on under Article 32, the CB shall validate that:

- The scheme is available for the product category, is applicable to the product under assessment, and provides the required assurance level;
- The evidence package derived from the scheme is sufficient, together with any supplementary evidence identified by the CB, to demonstrate conformity with the applicable Annex I requirements for the product and any relevant processes.

	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	9 of 27

Acceptance of scheme-derived evidence shall be based on a documented coverage mapping performed by the CB.

The mapping shall identify, for each applicable Annex I requirement, whether the scheme evidence provides full coverage, partial coverage, or no coverage; the CB shall define and obtain supplementary evidence for any partial or uncovered requirement before relying on the scheme evidence as part of the conformity assessment conclusion. The acceptance decision shall record the scheme version, scope, assurance level, product/version covered, evidence reviewed, mapping result, any limitations or assumptions, and the rationale for concluding that the evidence is sufficient in the context of the selected route.


Annex I requirement set	Scheme evidence source	Coverage result	Supplementary evidence / action	CB conclusion
Annex I Part I product requirements relevant to the assessed product	Certificate, report, scheme profile, test results, evaluator findings, or equivalent scheme outputs	Full / Partial / None	Identify additional evidence, clarification, or assessment activity needed	Accepted / Accepted with supplementary evidence / Not accepted
Annex I Part II process requirements relevant to the selected route	Scheme process evidence, quality system evidence, maintenance or surveillance outputs, or equivalent scheme outputs	Full / Partial / None	Identify additional evidence, clarification, or assessment activity needed	Accepted / Accepted with supplementary evidence / Not accepted

5.4.2. Report

The output of the assessment shall be recorded in the applicable assessment report template.

5.4.3. Nonconformities

Where the assessment identifies failure to meet an applicable CRA requirement, route requirement, certification scheme requirement, or documented certification criterion,

	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	10 of 27

the CB shall raise a nonconformity. Each nonconformity shall be recorded in the assessment report or certification status review record, classified according to its significance, supported by objective evidence, and communicated to the client together with the requirement not met.

Nonconformities shall be graded as major or minor. A major nonconformity is one that calls into question the product's conformity with applicable Annex I requirements, the effective implementation of required manufacturer processes, the validity of scheme-derived evidence relied on by the CB, or the integrity of the conformity assessment conclusion. A minor nonconformity is one that does not by itself invalidate the conformity assessment conclusion but requires correction and, where appropriate, corrective action to prevent recurrence.

The client shall provide correction and, where required, corrective action addressing the cause of the nonconformity within the timeframe set by the CB. The CB shall review the response, determine whether additional evidence or follow-up assessment is required, and record the closure decision. Nonconformities remain open until the CB has verified that the proposed actions are adequate and, where necessary, effectively implemented.


5.5. Assessment report review and certification decision

The report and associated records shall be independently reviewed by the CB/notified body before the certification decision is made.

The possible outcomes of the certification decision process are as follows. Decisions to refuse certification or to grant certification with conditions are subject to the complaints and appeals process in section 5.8 Complaints and appeals.

- Grant certification
- Grant certification with conditions
- Reduction of scope
- Refuse certification based on documented justification

The outputs and results of this process shall be formally documented on the applicable certification decision record. Where the decision or underlying findings trigger communication with the notifying authority or a competent Market Surveillance Authority, the matter shall also be handled in accordance with section 5.9 Notifying authority interaction and market surveillance authority cooperation.

	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	11 of 27

Where certification is granted, the certificate issued to the client shall clearly specify the certified product and version and shall be managed in accordance with the applicable certification scheme requirements.

CE marking remains the sole responsibility of the manufacturer, based on completion of applicable conformity assessment procedures and issuance of the EU Declaration of Conformity.

Certification shall not be granted while a major nonconformity remains open. Minor nonconformities may be accepted for certification decision only where the CB has accepted a documented correction plan, determined that the remaining issue does not invalidate the conformity assessment conclusion, and defined any necessary conditions or follow-up.


Prior to granting certification, the CB verifies that the manufacturer has established and documented procedures enabling compliance with Article 14 reporting obligations for actively exploited vulnerabilities and severe incidents, including the applicable notification timelines and user communication requirements.

- A documented workflow for identification, triage, and internal escalation of suspected actively exploited vulnerabilities and severe incidents, including defined decision owners, evidence capture, and the capability to issue the Article 14 early warning notification within 24 hours of becoming aware of the event.
- Documented reporting procedures, templates, and responsible contacts for notification through the CRA reporting channel, demonstrating the capability to submit the Article 14 notification and available update information within 72 hours, maintain traceable records of submissions, and preserve supporting evidence for review.
- Criteria and communication mechanisms for informing users, where required, about severe incidents and risk mitigation measures, supported by tested playbooks, role assignments, draft notice content, and evidence that personnel and tools are prepared to execute the process within the CRA-required timeframe.

The CB does not itself perform incident reporting.

5.6. Maintenance of certification and CRA-based surveillance activities

Where the CRA and the applicable conformity assessment procedure require post-certification or periodic oversight by the notified body, the CB shall perform surveillance activities, including periodic audits of vulnerability-handling processes as required by the CRA, to confirm that the basis on which certification was granted remains valid. These

	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	12 of 27


activities are not limited to Module H and do not transfer operational security responsibilities to the CB.

Where relevant to the certified product and the selected conformity assessment route, the CB shall also consider whether the manufacturer maintains the arrangements and records necessary to support compliance with applicable Article 15 obligations insofar as they affect continued conformity and certification validity.

The CB is responsible for evaluating the impact of vulnerability disclosures, product changes, and updates that occur during the certification period. All reviews related to these activities shall be documented using the applicable certification status review record.

Where the CRA and the applicable conformity assessment procedure require surveillance or ongoing oversight by the notified body/CB, the CB shall perform CRA-based surveillance activities to confirm that the basis on which certification was granted remains valid. Such activities include the CRA-required periodic audits of the manufacturer's vulnerability-handling processes against Annex I Part II and are not limited to a single assessment route. They shall be proportionate to the product risk profile, the manufacturer's processes, and any information indicating potential impact on continued conformity with the applicable Annex I requirements. These activities do not replace market surveillance by competent authorities.

- Review of relevant product changes, updates, and version changes to determine whether the certified scope, technical documentation, cybersecurity risk assessment, or conformity conclusions remain valid;
- Review of the manufacturer's vulnerability-handling, security update, and related post-market processes against the requirements applicable to the selected route and Annex I Part II;
- Periodic audits of the manufacturer's vulnerability-handling process to verify adequate implementation of the processes required under Annex I Part II, including governance, intake, triage, remediation planning, security update handling, communication, and recordkeeping;
- Review of available records relating to vulnerabilities, incidents, security advisories, corrective actions, and user communications, insofar as they are relevant to continued conformity and certification status;
- Verification that corrective actions and updates relevant to certified products are assessed, documented, and implemented in a manner consistent with the basis of certification;

	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	13 of 27

- Where certification scheme evidence is relied on, review of continued validity, scope, and applicability of that evidence, including any changes, limitations, or withdrawals that could affect the CB's conformity assessment conclusion.


Extraordinary surveillance may be initiated where the CB becomes aware of significant product changes, relevant vulnerability disclosures, severe incidents, failures in vulnerability-handling or update processes, concerns affecting scheme evidence relied on for certification, or other information that could materially affect the validity, scope, or conditions of certification. The outcome of surveillance shall be recorded on the applicable certification status review record and, where warranted, shall trigger certification status action under section 5.7 Suspension or withdrawal of certification and cooperation with the notifying authority or a competent Market Surveillance Authority under section 5.9 Notifying authority interaction and market surveillance authority cooperation. Where surveillance findings raise issues affecting the CB's notified scope, competence, or the reliability of conformity assessment outcomes, the matter shall also be escalated through the CB's regulatory notification process for interaction with the Notifying Authority.

The surveillance plan, frequency, and depth of review shall be determined by the selected route, the characteristics of the certified product, the support period, previous findings, and any identified risk indicators. The CB shall define the evidence to be reviewed, the competence required for the surveillance activity, and the decision criteria for maintaining, conditioning, reducing, suspending, or withdrawing certification.

Where surveillance identifies a nonconformity, the CB shall require correction and, where appropriate, corrective action within a defined timeframe and verify closure based on evidence or follow-up assessment. Minor nonconformities may result in continued certification, continued certification with conditions, or increased surveillance where the CB determines that the issue does not invalidate continued conformity and that adequate correction controls are in place. Major, unresolved, or recurring nonconformities shall trigger evaluation for reduction of scope, suspension, or withdrawal under section 5.7 Suspension or withdrawal of certification.

The possible outcomes of the certification status decision process are as follows. Continued certification with conditions, reduction of certification scope, suspension, withdrawal, or non-renewal are subject to the complaints and appeals process in section 5.8 Complaints and appeals, where applicable.

- Continued certification
- Continued certification with conditions

	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	14 of 27

- Reduction of certification scope
- Suspension of certification until significant issues are resolved
- Non-renewal of certification
- Withdrawal of certification

The results and outputs of this process shall be recorded on the applicable certification status decision record.

Where certification remains valid following maintenance or renewal activities, the CB shall maintain or reissue certification documentation as required by the applicable certification scheme.

This surveillance activity is distinct from market surveillance as described in the CRA. Where information arising from maintenance, surveillance, product changes, or vulnerability disclosures requires cooperation with the notifying authority or a competent Market Surveillance Authority, section 5.9 Notifying authority interaction and market surveillance authority cooperation applies.


Renewal of certification shall be treated as a documented certification decision based on continued conformity of the product and applicable manufacturer processes, closure of relevant nonconformities, review of product changes and vulnerability-handling performance during the preceding certification period, and completion of any required surveillance or reassessment activities. Where these conditions are not met, the CB shall decide non-renewal or another appropriate certification status action.

5.7. Suspension or withdrawal of certification

This section applies in particular where surveillance identifies a major nonconformity, or where a nonconformity remains unresolved or recurs after correction or corrective action.

The CB shall decide the appropriate course of action where nonconformity with certification scheme requirements results from surveillance activities or from changes affecting certification, for example changes relating to vulnerability handling. These actions include the following and, where applicable, the affected party shall be informed of the complaints and appeals process in section 5.8.

- Conditional continued certification, for example with increased surveillance, evaluation, or review of certification status;
- Reduction of certification scope to exclude nonconforming product variants;
- Suspension of certification pending remediation by the client;

	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	15 of 27

- Withdrawal of certification.

Certification may also be terminated at the client's request.

If certification is withdrawn or terminated, the CB shall update certification documents, public information, and any authorisations for use of marks or logos, as applicable, to ensure that the change in certification status is clearly reflected and that no representation remains that the affected product is certified. Where withdrawal or termination is relevant to the notifying authority or a competent Market Surveillance Authority, communication shall be handled in accordance with section 5.9 Notifying authority interaction and market surveillance authority cooperation.

Reduction of scope shall be used where nonconformity, product change, withdrawal of supporting evidence, or another relevant limitation affects only part of the certified scope, and the CB can clearly define the remaining conforming scope. The CB shall verify that the remaining certified scope continues to meet the applicable requirements, that certification documents and public information are updated accordingly, and that any excluded product variants, versions, or functions are no longer represented as certified.


If the scope of certification is reduced, the certification body shall make the necessary modifications to formal certification documents, public information, authorisations for use of marks, and related materials to ensure that the reduced scope is clearly communicated to the client and accurately reflected in certification documentation and public information. Where the reduction of scope is relevant to the notifying authority or a competent Market Surveillance Authority, communication shall be handled in accordance with section 5.9 Notifying authority interaction and market surveillance authority cooperation.

If certification is suspended, the CB shall formulate and communicate the following to the client:

- Actions needed to end suspension and restore certification for the product(s) in accordance with the certification scheme;
- Any other actions required by the certification scheme.

If certification is reinstated after suspension, the CB shall make all necessary modifications to certification documents, public information, and any authorisations for use of marks or logos, as applicable, to ensure that the product's certified status is correctly reflected.

If a decision to reduce the scope of certification is made as a condition of reinstatement, the certification body shall make all necessary modifications to formal certification documents, public information, authorisations for use of marks, and related materials to

	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	16 of 27

ensure that the reduced scope of certification is clearly communicated to the client and clearly specified in certification documentation and public information.

5.8. Complaints and appeals

The process for handling complaints and appeals is governed by SM-01-01. This procedure applies that process to CRA conformity assessment activities and shall be read together with SM-01-01. This section supports the impartial, traceable, and reviewable handling of issues arising from conformity assessment activities performed under Article 32 of Regulation (EU) 2024/2847 and ensures appropriate separation between certification activities and market surveillance responsibilities under the CRA.


A complaint is an expression of dissatisfaction relating to the CB's certification activities, including conduct, communication, timeliness, process execution, or other actions of the CB or its personnel in connection with CRA conformity assessment. An appeal is a formal request by an applicant or certificate holder for reconsideration of a certification decision, including refusal to certify, certification with conditions, reduction of scope, suspension, withdrawal, or non-renewal.

The CB shall ensure that complaints and appeals handling is impartial, documented, traceable, and carried out by competent personnel independent of the activities or decision being challenged. Submission of a complaint or appeal shall not result in retaliation, discrimination, or any adverse treatment of the complainant or appellant.

On receipt of a complaint or appeal, the CB shall acknowledge the submission and conduct an initial triage to determine whether the matter falls within the scope of the CB's certification activities. Where the matter primarily concerns suspected product non-compliance on the market, incident handling by the manufacturer, or regulatory enforcement under the CRA, the CB shall inform the submitter that such matters fall within the remit of the competent Market Surveillance Authority or other competent authority. Where appropriate, the CB shall preserve relevant records and escalate or communicate the matter internally in accordance with its legal and notification obligations.

For matters that fall within scope, the CB shall investigate the complaint or appeal in accordance with [SM-01-01](#) and maintain records of the submission, review, evidence considered, decision, and communication of the outcome. Appeals relating to certification decisions shall be reviewed by personnel independent of the original assessment, review, and certification decision.

Where a complaint or appeal reveals information that may affect the validity, scope, suspension, or withdrawal of certification, the CB shall initiate the relevant certification

	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	17 of 27

status review and decision-making process under this procedure and [SM-01-01](#). Where the outcome identifies a matter relevant to the CB's obligations as a notified body under the CRA, including a matter requiring communication with the notifying authority or other competent authority, the CB shall handle such communication through its established regulatory notification process. The CB complaints and appeals process does not replace or limit any separate obligations of the manufacturer under the CRA, including incident and exploited vulnerability reporting.


5.9. Notifying authority interaction and market surveillance authority cooperation

The CB shall cooperate with the notifying authority and competent Market Surveillance Authorities in accordance with the CRA and the conditions of its notification. This cooperation shall be handled through the CB's established regulatory notification process and shall preserve the distinction between the CB's certification activities and authority decisions on monitoring, enforcement, or corrective action.

Upon request from the notifying authority or a competent Market Surveillance Authority, the CB shall provide relevant information and records relating to its conformity assessment activities within the limits of applicable confidentiality and legal requirements. Such records may include application review records, assessment plans, assessment reports, certification decisions, certification status review records, and evidence supporting the scope and basis of certification. The CB shall ensure that the origin, review history, and status of such records remain traceable.


The CB shall promptly escalate and, where required, communicate matters that may affect its notification status, the validity or scope of certification, or the reliability of conformity assessment outcomes. This includes, where relevant, significant nonconformities identified during assessment or surveillance, restrictions affecting the CB's ability to operate within its notified scope, suspension or withdrawal decisions that may be relevant to authorities, and issues indicating that authority action may be required under the CRA.

Where the CB becomes aware of information suggesting suspected product non-compliance on the market, failure of the manufacturer to fulfil obligations under the CRA, or other matters falling within the remit of competent authorities, the CB shall preserve relevant records, route the matter internally in accordance with its regulatory notification process, and cooperate with the relevant authority as required. The CB does not assume the role of the Market Surveillance Authority and does not itself exercise enforcement powers.

	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	18 of 27

All interactions with the notifying authority and Market Surveillance Authorities shall be documented in the certification file or the applicable regulatory communication record, including the trigger for communication, the information provided, the date of transmission, and any resulting actions or decisions. Confidentiality shall be maintained to the extent permitted by law and shall not prevent the CB from meeting its mandatory cooperation and information-sharing obligations under the CRA.




	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	19 of 27

Annex A – CRA Conformity Assessment Process Flow

Activity	Applicant / manufacturer	CB / notified body	Notifying Authority	Market Surveillance Authority	Output / record
Application submission and intake	Submits the application, product and version details, requested certification scope, technical documentation, and cybersecurity risk assessment.	Receives and logs the application package for review.	No routine action.	No routine action.	Application received and logged.
Application review and scope confirmation	Provides any additional information requested during the review.	Reviews CRA applicability, product classification, whether third-party assessment is mandatory or voluntary, notified scope coverage, and any remote data processing relevance; records the outcome and assigns a competent assessor.	Acts only where matters affecting the CB's notification status or scope are escalated.	No routine action.	Application review outcome, scope confirmation, and file registration.



	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	20 of 27


Activity	Applicant / manufacturer	CB / notified body	Notifying Authority	Market Surveillance Authority	Output / record
Route selection and assessment planning	Confirms the chosen route where a voluntary third-party route is used and provides supporting evidence relevant to the selected route.	Determines classification, legal basis, route conditions, and any reliance on harmonised standards, common specifications, or certification scheme evidence; prepares the assessment plan and communicates it where required.	No routine action.	No routine action.	Documented classification and route basis; assessment plan issued.
Assessment execution	Makes the product, records, personnel, and supporting evidence available and responds to clarification requests.	Executes the selected assessment route, reviews technical documentation and risk assessment, evaluates Annex I requirements, and assesses manufacturer processes as applicable.	No routine action.	No routine action.	Assessment findings and identified nonconformities.



CB Logo	CRA Assessment process	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	21 of 27


Activity	Applicant / manufacturer	CB / notified body	Notifying Authority	Market Surveillance Authority	Output / record
Scheme evidence mapping (where applicable)	Provides scheme-derived evidence, clarifications, and any supplementary evidence requested.	Maps scheme evidence against Annex I requirements, identifies full, partial, or no coverage, and determines whether supplementary evidence is needed.	No routine action.	No routine action.	Coverage mapping and evidence acceptance decision.
Nonconformity management	Provides correction and, where required, corrective action within the timeframe set by the CB.	Raises, classifies, communicates, tracks, and reviews nonconformities and records closure decisions.	No routine action unless a matter affecting notification or scope is escalated.	No routine action unless the matter falls within authority remit.	Nonconformity status and closure decision.
Assessment report and certification decision	Receives the assessment outcome and, where certification is granted, remains responsible for EU Declaration of Conformity and CE marking.	Issues the assessment report, conducts independent review, verifies Article 14 preparedness, and makes and communicates the certification decision.	Receives communication where the decision triggers authority interaction relevant to notification status or scope.	Receives communication where the decision triggers cooperation under the CRA.	Assessment report completed; certification decision record; certificate issued or decision communicated.



	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	22 of 27


Activity	Applicant / manufacturer	CB / notified body	Notifying Authority	Market Surveillance Authority	Output / record
Maintenance, surveillance, and renewal	Provides records, access, and evidence relating to changes, vulnerabilities, incidents, updates, and continued conformity.	Performs surveillance, including periodic audits of vulnerability-handling processes, reviews changes and incidents, and makes documented certification status decisions.	Receives communication where surveillance findings affect the CB's notified scope, competence, or notification conditions.	May receive cooperation where surveillance findings indicate matters within authority remit.	Surveillance record; certification status review record; renewal or other status decision.
Reduction, suspension, withdrawal, or termination	Implements required corrective actions or may request termination; stops representing excluded or withdrawn scope as certified.	Decides and communicates the status action and updates certification documents, public information, and authorisations as applicable.	Receives communication where the status action is relevant to notification or scope.	May receive communication where the status action is relevant to authority action.	Certification status decision record; updated certification documentation and public information.



	<h1>CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	23 of 27

Activity	Applicant / manufacturer	CB / notified body	Notifying Authority	Market Surveillance Authority	Output / record
Complaints and appeals	Submits a complaint or appeal and provides supporting information where relevant.	Acknowledges, triages, investigates, and resolves complaints or appeals using competent and independent personnel; initiates certification status review where required.	Receives communication only where the outcome identifies a matter relevant to notification obligations.	May be the competent authority where the matter falls outside the CB's remit and concerns market non-compliance or enforcement.	Complaint or appeal record, decision, and any resulting status review.
Authority cooperation and regulatory communication	No routine action unless requested to provide information through the CB or as required by law.	Cooperates with the Notifying Authority and competent Market Surveillance Authorities, preserves records, and provides information where required.	Requests or receives relevant information, oversees matters affecting notification, and takes action within its remit.	Requests or receives relevant information and acts within its remit on market surveillance or enforcement matters.	Regulatory communication record and related authority interaction.




	<h1 style="text-align: center;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	24 of 27

Annex B – Alignment between the CRA and the Sections of this Procedure

This annex provides a high-level alignment between key CRA requirements relevant to third-party conformity assessment and the sections of this procedure in which those requirements are addressed. It is intended as a navigational aid and does not replace direct reference to Regulation (EU) 2024/2847 or the full text of the procedure.


CRA topic / provision	Alignment in this procedure	Relevant section(s)
Article 1 – Subject matter	The procedure is framed as an internal process for CRA third-party conformity assessment supporting conformity determination, certification outcome, and CE-marking-related conformity assessment activities.	1, 2, 4
Article 2 – Scope	The procedure defines when it applies, including important and critical products with digital elements and cases where third-party assessment is mandatory or voluntarily selected.	2, 5.1, 5.2
Article 3 – Definitions	The procedure uses CRA-defined concepts such as product with digital elements, manufacturer, important product, critical product, notified body, and market surveillance authority as the basis for role allocation and route determination.	2, 3, 5.1, Annex A
Article 6 and Annex I – Essential cybersecurity requirements	The procedure defines conformity assessment against Annex I requirements, including assessment of applicable product and process requirements and treatment of supporting evidence.	1, 2, 5.2, 5.3.1
Annex I Part I – Product cybersecurity requirements	The procedure requires assessment of Annex I Part I product requirements through technical documentation review, route execution, and evidence evaluation, including where scheme-derived evidence is used.	5.2, 5.3.1
Annex I Part II – Vulnerability handling and related processes	The procedure addresses assessment of vulnerability-handling, update, and related post-market processes during route execution and surveillance, including periodic audits where required.	5.2, 5.4, 5.6



	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	25 of 27


CRA topic / provision	Alignment in this procedure	Relevant section(s)
Articles 7 and 8; Annex III and Annex IV – Important and critical products with digital elements	The procedure defines the applicability of the process to important and critical products and requires documented classification and route selection based on the CRA.	2, 5.1, 5.2
Article 10 – Free movement	The procedure supports conformity assessment outcomes that underpin the manufacturer’s placement of compliant products on the Union market, without assigning market access or enforcement functions to the CB.	1, 2, 5.4, 5.8
Article 13 – Obligations of manufacturers	The procedure requires the manufacturer to provide and maintain technical documentation, risk assessment, and evidence relevant to conformity assessment and certification.	3, 5.1, 5.2, 5.3.1, Annex A
Article 14 – Reporting obligations of manufacturers	The procedure requires the CB to verify manufacturer preparedness for Article 14 reporting and user communication obligations before grant and during relevant surveillance activities, while clarifying that the CB does not perform the reporting itself.	5.5, 5.6
Article 15 – Relevant post-market or manufacturer obligations affecting continued conformity	The procedure requires the CB, where relevant to the certified product and selected conformity assessment route, to consider whether the manufacturer maintains the arrangements and records necessary to support compliance with applicable Article 15 obligations insofar as these affect continued conformity and certification validity.	5.6
Articles 24 to 29 – EU declaration of conformity, CE marking, and conformity assessment framework	The procedure supports conformity assessment outcomes feeding the manufacturer’s EU Declaration of Conformity and CE marking responsibilities and defines certification outputs and related records.	1, 2, 5.4, Annex A



	<h1 style="margin: 0;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	26 of 27

CRA topic / provision	Alignment in this procedure	Relevant section(s)
Article 31 – Notification of conformity assessment bodies	The procedure addresses the role of the notified body, the need to operate within the valid scope of notification, and escalation where notification scope or competence issues arise.	2, 3, 5.1, 5.6, 5.8, Annex A
Article 32 – Conformity assessment procedures	The procedure defines application review, route selection, assessment planning, execution, evidence treatment, reporting, and certification decision-making for third-party conformity assessment under Article 32.	2, 4, 5.1, 5.2, 5.3, 5.4, Annex A
CRA provisions on conformity assessment bodies, notifying authorities, notified bodies, and notification	The procedure defines authority interaction, notification-related escalation, record traceability, competence assignment, and the distinction between certification activities and authority oversight.	3, 5.1, 5.6, 5.9, Annex A
CRA provisions on market surveillance and enforcement	The procedure distinguishes CB surveillance from market surveillance, defines cooperation with competent authorities, and addresses escalation where suspected non-compliance or authority-relevant issues arise.	3, 5.6, 5.7, 5.9, Annex A
Complaints, appeals, and reviewability of decisions	The procedure provides for impartial handling of complaints and appeals, independence from the original assessment and decision, and initiation of status review where needed.	5.4, 5.5, 5.6, 5.7, Annex A



	<h1 style="text-align: center;">CRA Assessment process</h1>	Document:	TB-SM-01-03b
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	27 of 27

Version History

Version	Date	Author	Summary of changes	Status
1	23-04-2026	Khalimatou Samirah (NSAI)	Initial draft created.	Draft
2	29-05-2026	Khalimatou Samirah (NSAI)	Updated sections as per review comments,	Approved

