OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 12

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Project acronym	OSCRAT
Project title	Open-Source Cyber Resilience Act tools
Name	OSCRAT – Comprehensive Project Requirements Document -ANNEX 12
Number	101190180
Work package	WP2 – Requirements gathering and analysis
Due Date	30/11/2025
Submission Date	30/11/2025
Lead Partner	Lukasiewicz – AI
Author name(s)	Dariusz Rogowski
Version	2.0
Status	Draft
Type:	☒ R – Document, Report ☐ DEC – Websites, patent filings, videos, etc ☐ DEM – Demonstrator, pilot, prototype
Dissemination level:	☒ PU - Public ☐ SEN - Sensitive

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Document History			
Version	**Date**	**Modified by**	**Comments**
0.0	27/10/2025	Lukasiewicz – AI	Started working on draft n.1
1.0	14/11/2025	Lukasiewicz – AI	Finished working on draft n.1
2.0	26/11/2025	Lukasiewicz – AI	Finished working on draft n.2

Abstract
The document provides the CRA Conformity Assessment Guide.

Keywords
CRA Conformity Assessment, module A, module B, module C, module H

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

DISCLAIMER

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

CRA Conformity Assessment Guide

for manufacturers of products with digital elements

What is conformity assessment under the CRA?

Under the Cyber Resilience Act (CRA), conformity assessment is the set of procedures a manufacturer uses to demonstrate that a product with digital elements and the manufacturer's processes meet the essential cybersecurity requirements (Annex I), so the product can be CE-marked and placed on the EU market. CRA conformity assessment procedures are built on the New Legislative Framework (Decision 768/2008/EC) and are designed to verify both **product** and **process requirements** across the product lifecycle (planning, design, development/production, testing and maintenance).

The CRA's Annex VIII defines the procedures themselves (Modules A, B, C, H), what the manufacturer must do, and when/notified bodies (third-party conformity assessment bodies designated by Member States) must be involved. CE marking and the EU Declaration of Conformity follow successful assessment and must be kept at the authorities' disposal.

The Blue Guide on the implementation of EU product rules (2022/C 247/01) explains the general principles that apply across EU product laws: what conformity assessment is, the modular structure of procedures, the roles of manufacturers and notified bodies, and the risk-based rationale for selecting procedures. In short, modules range from lighter, self-assessment options to more comprehensive, third-party and quality-system-based options, and the choice must be proportionate to product risks, design complexity, and production mode.

What compliance procedures are available for products with digital elements?

CRA Article 32 and **Annex VIII** make the following procedures available:

Module A — Internal control (manufacturer self-assessment)
The manufacturer ensures and declares, on its sole responsibility, that the product and the manufacturer's processes meet the CRA's essential requirements. No notified body is involved.

Module B — EU-type examination (design/type)
A **notified body** examines the technical design and development (and, where relevant, specimens of critical parts) and issues an **EU-type examination certificate** if the type meets the essential requirements.

Module C — Conformity to type based on internal production control (production)

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

After Module B, the manufacturer controls production to ensure **all units conform to the approved type**; no notified body is involved in this phase.

Module H — Conformity based on full quality assurance (company process certification)
A **notified body** assesses and surveys a **manufacturer's quality management system (QMS)** covering design, development, final product inspection/testing, and vulnerability handling across the support period. Products designed and produced under the approved QMS can be CE-marked.

Note: *Manufacturers may also use an applicable **European cybersecurity certification scheme** where available.*

How to choose the most appropriate procedure (decision guide)

First Distinction*: Product Certification* vs. *Company Process Certification*
When approaching conformity assessment under the CRA, ask yourself:

*Product Certification Path (**Module B + C**):*

- **Focuses on the product itself**. A notified body checks whether a representative specimen (design/type) meets CRA requirements (Module B), then the manufacturer ensures that all units produced match the approved type (Module C).
- Best for manufacturers with specific models or limited ranges, especially if no comprehensive cybersecurity QMS is in place.

*Company Process Certification Path (**Module H**):*

- **Focuses on the manufacturer's processes.** A notified body audits and certifies your full quality management system (QMS) to ensure it consistently delivers compliant products.
- Best for manufacturers with broad product portfolios, frequent updates, or those already running mature QMS (ISO 9001, ISO 27001, etc.).

A. Start from CRA classification & legal triggers
Use Article 32 to determine what is allowed or required for your product category:

- **General products (not "important" or "critical")**
  You may use **Module A** by default. You may voluntarily choose B+C, H, or (where available) an EU cybersecurity certification scheme.
- **Important products – Class I (Annex III)**
  If you **fully apply** the identified harmonised standards/common specifications or an EU cybersecurity certification scheme at assurance level at least "substantial", you may still use Module A.
  If you **do not apply** them (or only partly, or they do not exist), you **must** use **B+C** or **H**.
- **Important products – Class II (Annex III)**
  Conformity assessment **must involve a third party**: choose **B+C**, **H**,

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

or an applicable EU cybersecurity certification scheme (assurance ≥ "substantial").

- **Critical products (Annex IV)**
  Use a **European cybersecurity certification scheme** in accordance with **Article 8(1)**. If the Article 8(1) conditions are **not** met, use any of the options for Important Class II (i.e., **B+C or H**).
- **Products qualifying as Free and Open-Source Software (FOSS) in Annex III categories**
  May use the procedures in paragraph 1 (Module A, B+C, H, or certification scheme) **provided the technical documentation is made public at placement on the market**.

Tip (standards): Applying OJEU-cited harmonised standards gives **presumption of conformity** for covered requirements; where only a partial fit exists, supplement with other technical solutions and document equivalence. (Blue Guide, Section 4.1.2.)

B. Use the Blue Guide's risk-based rationale to pick the module

- **Low risk/complexity & robust internal testing** → Module **A** (self-assessment).
- **Mass production based on a representative design/type** → **B+C** (type approval + manufacturer-controlled production conformity).
- **Higher risk/complexity or desire for scalable, portfolio-wide assurance** → **H** (full QMS assessed by a notified body).

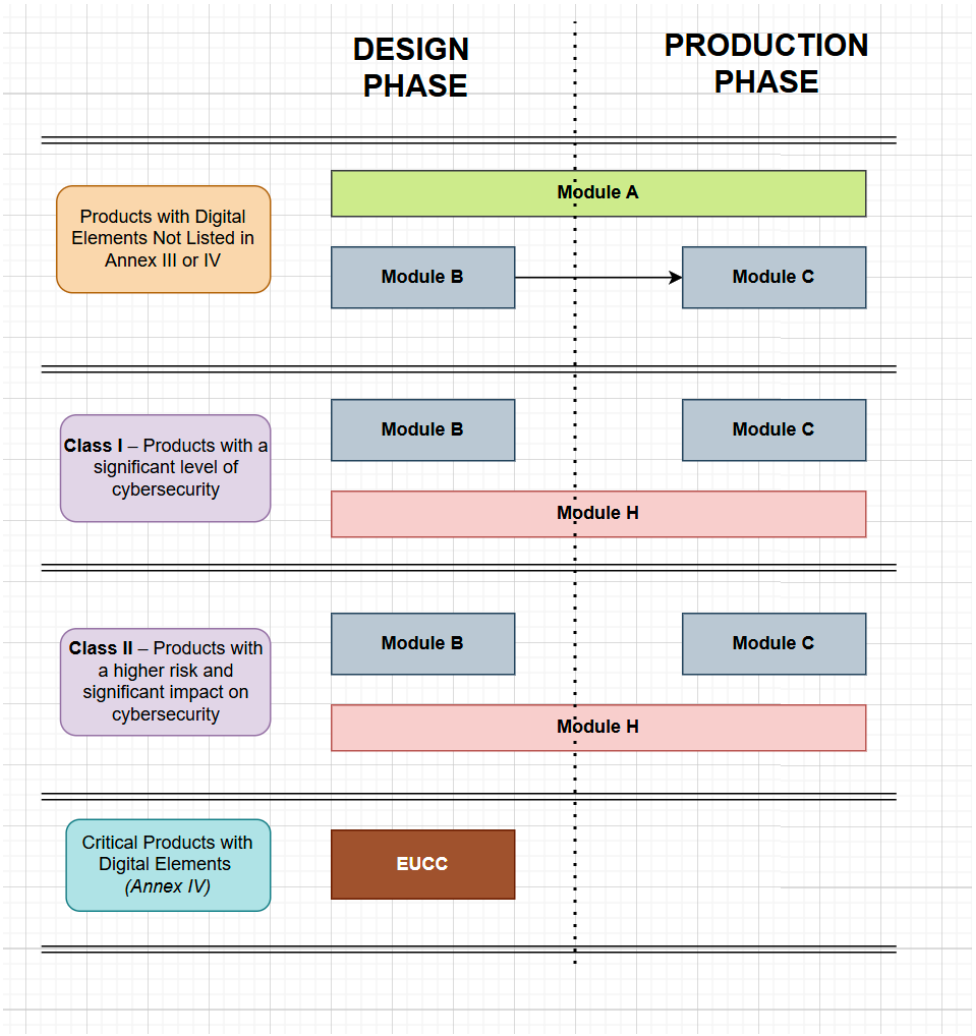
Practical chooser (step-by-step)

1. **Classify the product** (general / Important Class I / Important Class II / Critical). Apply the legal triggers above.
2. **Check standards/certification scheme availability** (OJEU-cited harmonised standards, common specifications, or an EU cybersecurity certification scheme at assurance ≥ "substantial"). Your choice of **self-assessment** vs. **third-party assessment** often hinges here (especially for Important Class I).
3. **Decide product vs. process focus:**
   - **Few models, stable designs** → **Module B+C** (product certification path).
   - **Many variants, frequent updates, mature QMS** → **Module H** (process certification path).
4. **Prepare evidence & documentation** per Annex VII/VIII (risk assessment, testing, vulnerability handling, SBOM where applicable, declaration of conformity). Then **CE-mark** and retain records for the required period.
5. **Maintain conformity with CRA**:
   - under **H**, expect surveillance;
   - under **B+C**, re-assess **Module B** if the approved type changes significantly;
   - under **A**, keep documentation current and reflect the actual integration/environment.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Note: Applying OJEU-cited harmonised standards gives presumption of conformity for covered requirements; where only a partial fit exists, supplement with other technical solutions and document equivalence. (Blue Guide, Section 4.1.2.)



Modules in Detail

Module A — Internal control (manufacturer self-assessment)

What it is:

- The manufacturer ensures and declares, on its sole responsibility, that the product and the manufacturer's processes meet the CRA's essential requirements. No notified body is involved.

What you must do:

- Compile full technical documentation (Annex VII), including risk assessment, design info, testing and vulnerability handling evidence.
- Ensure design, development, production and vulnerability handling processes achieve compliance and are monitored.
- Draw up the EU Declaration of Conformity and affix CE marking before placing on the market; keep the documentation for the required retention period.
- Blue Guide context: A light module used where risks/complexity are low, and the manufacturer can perform all checks internally.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Output:

- *Self-declaration of conformity*

Module B: EU-Type Examination

What it is:

- A notified body examines a specimen (prototype or representative design) of your product with digital elements and verifies it against the CRA's essential cybersecurity requirements.

What you must do:

- Prepare technical documentation: risk assessment, design description, SBOM, vulnerability handling measures, test reports.
- Submit the representative product to a notified body.
- Cooperate with testing/assessments (can include penetration tests, security configuration checks).
- Receive an EU-type examination certificate, valid for the approved design.

Output:

- A certificate confirming that the examined type complies.

Limitation:

- Covers only the tested design; if you significantly change the product, you may need a new Module B assessment.

Module C: Conformity to Type (Internal Production Control)

What it is:

- The manufacturer ensures that series production conforms to the type approved under Module B. No notified body involvement at this stage.

What you need to do:

- Implement internal production control procedures (testing, inspections).
- Ensure consistency with the type certified under Module B.
- Keep records: test logs, quality checks, update history.
- Draw up the EU Declaration of Conformity and affix the CE marking.

Output:

- CE-marked products, with traceable documentation.

Module H: Conformity Based on Full Quality Assurance

What it is:

- A notified body assesses and certifies the manufacturer's quality management system (QMS) covering design, development, production, testing, and cybersecurity maintenance.

What you need to do:

- Set up a QMS: must include secure SDLC processes, vulnerability handling, patch management, supplier controls, incident response.
- Document QMS procedures (align with ISO 9001 for structure, integrate CRA-specific security elements).
- Undergo a notified body audit (initial assessment of your processes).
- Ongoing surveillance audits by the notified body to confirm continued compliance.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- Keep technical documentation available for each product covered under the QMS.

Output:

- Approval of the QMS + CE marking for all products designed and produced under it.

Advantage:

- Easier to bring new products/variants to market without repeating Module B every time.

Practical Guidance: Choosing the Right Module

To determine the most appropriate conformity assessment procedure for your product, please answer the following questions:

1. Organizational Setup & Maturity

- **Question:** Does your organization currently operate a certified Quality Management System (e.g., ISO 9001, ISO 27001)?
  - **Guidance:**
    - **YES: Module H (Full Quality Assurance)** is likely the most efficient path, as it allows you to integrate CRA requirements into your existing certified processes.
    - **NO:** If you lack a comprehensive QMS, **Module B+C (EU-Type Examination)** is more practical, as it focuses on certifying the specific product rather than your entire organizational process.
- **Question:** Do you have the internal resources to maintain continuous surveillance audits and a dedicated cybersecurity QMS?
  - **Guidance:**
    - **YES: Module H** is suitable if you are prepared for periodic audits of your processes by a Notified Body.
    - **NO: Module B+C** is preferable if you want to limit organizational overhead and engage a Notified Body only once per product design.

2. Product Strategy & Lifecycle

- **Question:** What is the anticipated frequency of updates and design changes for the product?
  - **Guidance:**
    - **Stable Designs:** If the product design is stable and updates are infrequent, **Module B+C** is recommended.
    - **Continuous Innovation:** If the product requires frequent updates or continuous feature integration (CI/CD), **Module H** is preferable. It avoids the need for a new Module B assessment for every significant change.
- **Question:** What is the size and diversity of your product portfolio?
  - **Guidance:**
    - **Broad Portfolio:** If you manage many different product variants or lines, **Module H** offers a scalable "process certification" that covers all products designed under that system.
    - **Limited Range:** If you manufacture only a few specific models, **Module B+C** is more cost-effective as it targets specific "types" without requiring a full system audit.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

3. Market Expectations & Criticality

- **Question:** What are the specific compliance expectations of your target market or clients?
  - **Guidance:**
    - **Critical Sectors:** If targeting buyers in critical infrastructure sectors who prioritize organizational maturity and supply chain security, **Module H** is strongly advised.
    - **Consumer Market:** For standard consumer devices where price and speed-to-market are key, **Module B+C** is typically sufficient.

4. Risk & Complexity (General Assessment)

- **Question:** Is your product classified as "Important Class I" and do you fully apply harmonised standards?
  - **Guidance:**
    - **YES:** You may be eligible for **Module A (Internal Control)**, avoiding third-party involvement entirely.
    - **NO (or Partial Application):** You must choose between **Module B+C** or **Module H**, as third-party assessment becomes mandatory.

What Compliance Requires

Under B+C:

- Engage a notified body once (design/type).
- Maintain strong internal controls for consistent production.
- Update certification when designs change substantially.

Under H:

- Build a comprehensive cybersecurity-focused QMS.
- Accept periodic notified body audits.
- Ensure every product under your QMS complies automatically.

Annex: “What do I actually do?” (per module, condensed)

- **Module A (Internal control)**
  Build/operate compliant design-to-support processes; compile Annex VII tech file; DoC; CE mark; keep docs. **No notified body.**
- **Module B + C (Type + production)**
  B: Submit design/specimens to a notified body → obtain EU-type certificate.
  C: Control production internally to match the approved type; DoC; CE mark; keep records. **Notified body in B only.**
- **Module H (Full quality assurance)**
  Implement CRA-ready QMS (design→support + vulnerability handling); apply to notified body for QMS assessment; undergo surveillance; DoC; **CE + NB ID**. **Notified body for QMS**.

Sources used

- **CRA**: OJ L 20.11.2024, Annex VIII (Modules A, B, C, H), Article 32 (procedure choices by class), CE-marking/DoC rules.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- **Blue Guide (2022)**: Section 5 (conformity assessment: definition, modular structure, rationale; roles of notified bodies; overview of modules; risk-based selection); Section 4.1.2 (presumption of conformity via harmonised standards).

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 12

www.oscrat.eu https://www.linkedin.com/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.