



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1.

OSCRAT – Comprehensive Project Requirements Document

Submission date: 30/11/2025

Author: Dariusz Rogowski – Łukasiewicz AI



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
Deliverable Name	Comprehensive Project Requirements Document
Number	101190180
Work package	Work Package 2 – Requirements Gathering and Analysis
Due Date	30/11/2025
Submission Date	30/11/2025
Lead Partner	Łukasiewicz AI
Author name(s)	Dariusz Rogowski
Version	2.0
Status	Final
Type:	R – Document, report
Dissemination level:	PU - Public



Document History			
Version	Date	Modified by	Comments
0	27/10/2025	Łukasiewicz - AI	Started working on draft n.1
1.0	14/11/2025	Łukasiewicz - AI	Finished working on draft n.1
2.0	26/11/2025	Łukasiewicz - AI	Finished working on draft n.2

Abstract
This deliverable, D2.1. – Comprehensive Project Requirements Document provides a detailed overview of the methodologies, analyses, and outcomes achieved within Work Package 2 (WP2) of the OSCRAT project. It defines the scope of the OSCRAT open-source software tools platform, functional and CRA-specific requirements for each tool which aims to support SMEs in achieving compliance with the EU Cyber Resilience Act (CRA) by the following basic functionalities: Conformity Assessment Checklists, Software Bill of Materials (SBOM), Vulnerabilities Disclosure and Handling, Incidents Handling, and Documentation Centralization for: technical and user documentation, vulnerability and incidents reports and policies, SBOM reports, patch release, and finally for EU Declaration of Conformity. The document presents the process of refining the initial project scope, performing a state-of-the-art analysis of existing CRA-related tools and research initiatives, and identifying user needs through dedicated surveys. It also describes the development of key outcomes such as user stories, use cases, activity diagram, CRA-specific requirements and a structured set of CRA security requirement for conformity assessment of products with digital elements. These formed the basis for defining implementation tasks verified through regular coordination meetings with project partners which contributed to WP3 development phase. The results of WP2 constitute the essential input for the software design and implementation activities in WP3, ensuring that the OSCRAT tools are functionally complete, user-oriented, and aligned with CRA obligations.
Keywords
OSCRAT; Cyber Resilience Act; Essential Security Requirements, Digital Europe; Free and Open-Source Tools; SMEs; Cybersecurity; functional requirements.

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.

Table of Contents

1. Executive Summary	10
2. Introduction	12
2.1 WP2 Methodology	12
2.1.1. Adjusting the Scope	12
2.1.3. Identifying user needs	14
2.1.4. Analysing data.....	14
2.1.5. Refining the project requirements.....	15
2.2 MS4 Milestone.....	15
3. Sources of the Requirements	17
3.1 Assumptions, limitations and CRA-specific requirements	17
3.2 State of the Art	20
3.3 Questionnaires.....	21
3.4 Knowledge and experience from partners	21
3.4.1. Lukasiewicz-AI.....	21
3.4.2. OVES Enterprise SRL.....	22
3.4.3. ENERSEC Technology SRL	23
3.4.4. Unicis.Tech OÜ	23
4. Scope Definition (T2.1.).....	24
4.1 CRA conformance activities flow	24
4.1.1. General CRA classification and assessment flow	24
4.1.2. CRA Questionnaire Flow.....	26
4.1.3. CRA Task Management Flow	27
4.1.4. CRA Conformity Assessment Guide	28
4.2 . Functionalities and Limitation of the Tools	31
4.2.1. Limitations.....	31
4.2.2. General Functionalities	34
4.2.3. Checklist.....	37
4.2.4. SBOM	39
4.2.5. Vulnerabilities.....	40
4.2.6. Incidents	41
4.2.7. Documentation.....	42
4.3 User Story – General View.....	44
4.3.1. “Pre-Market” User Story Diagrams	45

4.3.2.	“Post-market” User Story diagrams	50
5.	CRA Requirements Identification (T2.2.)	56
5.1	CRA Essential Security Requirements.....	56
5.1.1.	Purpose and Scope of work	56
5.1.2.	Methodology	57
5.1.3.	Checklist structure, logic and functions.....	60
5.2	. CRA-specific requirements for the tools.....	67
6.	User Needs Analysis (T2.3.)	74
6.1	Analysis according to main categories of questions.....	75
6.1.1.	Stakeholder’s characteristic	75
6.1.2.	Inventory/ labelling (Software Bill of Materials (SBOM))	76
6.1.3.	Risk management	80
6.1.4.	Vulnerability Management.....	83
6.1.5.	Incident Management.....	87
6.1.6.	Security Management, Documentation, Workflow	92
6.1.7.	Needs and expectations	95
6.2.	Conclusions for the whole questionnaire	97
6.3.	Stakeholder Alignment	99
6.4.	Integration of User Needs	101
7.	Data analysis to inform the development process.....	106
7.1.	Methodology	106
7.2.	Use cases – general view.....	106
7.3.	Specification of implementation tasks.....	118
8.	The Final List of Functionalities	119
8.1	Checklist.....	119
8.2	SBOM.....	121
8.3	Vulnerability.....	121
8.4	Incident	122
8.5	Documentation	123
8.6	General Functionalities of OSC RAT Platform	124
9.	Stakeholder Alignment and Project refinement (T2.5)	127
9.1.	Stakeholders training and workshops results.....	127
9.2.	Project Requirements Refinement.....	128
10.	Conclusions.....	129
11.	Conclusions.....	130

12.	References	130
13.	Annexes	131
13.1	Annex 1 – State of the art no. 1.....	131
13.2	Annex 2 – State of the art no. 2.....	131
13.3	Annex 3 – Implementation Tasks	131
13.4	Annex 4 – ESR_TechDoc_Requirements	131
13.5	Annex 5 – Questionnaire User Guide	131
13.6	Annex 6 – Use Cases Diagrams.....	131
13.7	Annex 7 – Stakeholder Questionnaire.....	131
13.8	Annex 8 – Revised Stakeholder Questionnaire	131
13.9	Annex 9 - Documentation Pillar for OSCRAT	132
13.10	Annex 10 – Incident Template	132
13.11	Annex 11 – Vulnerability Template.....	132
13.12	Annex 12 – CRA Conformity Assessment Guide	132
13.13	Annex 13 – Risk Assessment Template	132
13.14	Annex 14 – CRA-specific requirements mapping	132
13.15	Annex 15 – Vulnerability Disclosure Policy Template	132

Figures

Figure 1: OSC RAT Platform - CRA Essential Requirements Tool (from Grant Agreement).....	19
Figure 2: OSC RAT – General CRA Classification and Assessment Flow	25
Figure 3: OSC RAT – CRA Questionnaire Flow	27
Figure 4: OSC RAT - CRA Task management flow.....	28
Figure 5: OSC RAT - CRA Annex VIII conformity assessment modules.....	29
Figure 6: OSC RAT - Declaration of conformity flow.....	30
Figure 7: OSC RAT - User Story (pre-market) activities diagram part 1	46
Figure 8: OSC RAT - User Story (pre-market) activities diagram part 2	48
Figure 9: OSC RAT - User Story (pre-market) activities diagram part 3	48
Figure 10: OSC RAT - User Story - Post-market PDE management in OSC RAT	52
Figure 11: OSC RAT - User story - Post-market vulnerability handling activities	53
Figure 12: OSC RAT - User story - Post-market incident handling activities.....	55
Figure 13: OSC RAT - Product classification and organization role	63
Figure 14: OSC RAT - Role-based questionnaires	64
Figure 15: OSC RAT - Requirement evaluation process flow	65
Figure 16 Requirement reassessment flow.....	65
Figure 17: OSC RAT - Entry to optional module 3c (Technical Documentation)	66
Figure 18: OSC RAT - General view of OSC RAT tool functions for end user.....	107
Figure 19: OSC RAT - Answer question functions.....	109
Figure 20: OSC RAT - Edit selected product related functions	110
Figure 21: OSC RAT - Add product activity related functions	111
Figure 22: OSC RAT - Attach file to product functions.....	111
Figure 23: OSC RAT - Review product incidents functions	112
Figure 24: OSC RAT - Review product vulnerabilities functions.....	112
Figure 25: OSC RAT - View product log functions.....	112
Figure 26: OSC RAT - Finish questionnaire related functions	113
Figure 27: OSC RAT - Review organisation details related functions	114
Figure 28: OSC RAT - Manage external reporting organisation functions	114
Figure 29: OSC RAT - Review reports related functions.....	115
Figure 30: OSC RAT - Review user organisations functions	115
Figure 31: OSC RAT - Review user profile functions	116
Figure 32: OSC RAT - Review user tasks functions	116



List of Tables

Table 1: OSCRAT: Quality review Checklist for WP2 Tasks	16
Table 2: OSCRAT – Integrated application of CRA areas.....	17
Table 3: OSCRAT – The Scope and List of general functionalities for OSCRAT tool ..	36
Table 4: OSCRAT - The scope and list of main functionalities for checklist module	39
Table 5: OSCRAT - The scope and list of main functionalities for SBOM module	39
Table 6: OSCRAT - The scope and the list of main functionalities for vulnerabilities module.....	40
Table 7: OSCRAT – The scope and the list of main functionalities for incident module.....	41
Table 8: OSCRAT – The scope and list of main functionalities for documentation module.....	43
Table 9: OSCRAT: Capabilities and Functionalities of the OSCRAT Tools mapped to CRA Requirements	73
Table 10: OSCRAT - Answers to the question "Which stakeholders' group do you belong to and what type of products do you offer?"	75
Table 11: OSCRAT - Answers to the question "How are you currently handling the labelling (tagging), identifying products, components, and libraries processes in your organization?"	76
Table 12: OSCRAT - Answers to the question "If you use solutions that support SBOM, what types of standards do you use or would like to use?"	77
Table 13: OSCRAT - Answers to the question "Do You use any SBOM preparing / analysis of SBOM supporting tool?"	78
Table 14: OSCRAT - Answers to the question "How are you currently handling the Risk Management processes in your organization?"	80
Table 15: OSCRAT - Most common standards.....	81
Table 16: OSCRAT - Answers to the question "Do You use any governance, risk management, and compliance (GRC) supporting tools?"	82
Table 17: OSCRAT - Answers to the question "How are you currently handling the Vulnerability management processes in your organization?"	83
Table 18: OSCRAT - Answers to the question "Is vulnerability classification implemented (how)?"	84
Table 19: OSCRAT - Answers to the question "Notification Channels of detected / registered / fixed vulnerabilities?"	85

Table 20: OSC RAT - Answers to the question "Information Format of detected / registered / fixed vulnerabilities?"	85
Table 21: OSC RAT - Answers to the question "Do You use any vulnerability disclosure / handling supporting tools?"	86
Table 22: OSC RAT - Answers to the question "How are you currently handling the incident management processes in your organization?"	87
Table 23: OSC RAT - Answers to the question "Is incident classification implemented (how)?"	88
Table 24 :OSC RAT - Answers to the question "Who is notified of detected incidents carried out?"	89
Table 25: OSC RAT - Answers to the question "Notification Channels of detected incidents carried out?"	90
Table 26: OSC RAT - Answers to the question "Do You use any incident detection / analysis, reporting supporting tools?"	90
Table 27: OSC RAT - Answers to the question "Have you implemented any documentation management or security management processes in your organization?"	92
Table 28: OSC RAT - Answers to the question "Do you use any tools for documents / source code / data repository tools (internal for developers, managers and public for customers?"	93
Table 29: OSC RAT - Answers to the question "Do you use any building systems / compilations tools?"	94
Table 30: OSC RAT - Answers to the questions "How important to you is..."	96
Table 31: OSC RAT - Answers to the question "Are you interested in participating in the validation of the tool developed within the project?"	96
Table 32: OSC RAT - Type of an organisation.....	98
Table 33: OSC RAT - Tools importance.....	98
Table 34: OSC RAT - Identified users' needs to be implemented in the tools	104

1. Executive Summary

This document and its 14 annexes provide a detailed functional design of the OSCRAT platform tools. The deliverable specifies the scope, functional requirements, capabilities and limitations of the tools. While the project proposal defined these tools at a conceptual, high level of abstraction, Work Package 2 (WP2) provides a detailed specification to support their effective implementation in Work Package 3 (WP3).

The main objective of WP2 is to elaborate the detailed functional specifications of each tool — Checklist, Software Bill of Materials (SBOM) Solution, Vulnerability and Incident Handling Processes, and Documentation Centralization — based on the identified requirements and expectations of end users, CRA-specific requirements for each tool, and data analysis to inform decision-making throughout the development process in WP3.

The objective of WP2 was achieved through the systematic execution of its defined tasks and the consistent application of the adopted methodologies of work, ensuring alignment with subsequent work packages, especially with WP3.

A general methodology of regular meetings with project's partners was implemented to ensure consistency of the scope and requirements defined for the tools. These meetings included:

- WP2 synchronization meetings to align the scope with design and implementation.
- Regular CRA requirements restructuring weekly review and technical meetings.
- Implementation tasks specification meetings to define implementation-oriented deliverables for the development stage in WP3.
- Regular monthly project meetings were conducted to ensure continuous quality control and progress monitoring.
- Refinement of the scope during the project kick-off meeting and Team Project Meeting (TPM) incorporating feedback from project partners.

A specific methodology was applied which included multiple sources of input, including:

- Preliminary assumptions and limitations defined in the original project proposal.
- An assessment of the project scope and the OSCRAT platform tools.
- Review and analysis of CRA act requirements.
- State-of-the-art analysis of CRA tools and R&D initiatives in Europe.
- Stakeholder surveys to identify user needs and expectations.

- Consortium partners' expertise regarding the OSCRAT platform and its anticipated capabilities.

The methodologies applied in the execution of WP2 tasks enabled the successful achievement of its objectives, which included:

- Defining the scope of functional requirements for each tool within the OSCRAT platform.
- Identifying CRA-specific requirements for all tools of the platform.
- Determining the needs and expectations of prospective users.
- Supporting the software development process through the analysis of data collected in earlier stages.

As a result, WP2 achieved its milestone MS4 — the comprehensive requirements analysis for the OSCRAT platform tools. This deliverable consolidates all major findings, including the scope definition, stakeholder and user requirements, and data on CRA-specific requirements for each tool. These outcomes contribute to the activities in WP3, which will focus on the software design and implementation of the tools in alignment with SMEs expectations and CRA obligations.

2. Introduction

This document identifies and describes a set of functional requirements and CRA-specific requirements for the OSCRAT platform tools.

The objectives of Work Package 2 (WP2) in the OSCRAT project are to precisely define the scope of the CRA tools, identify specific requirements from stakeholders and end-users, analyse user needs and preferences, and collect and analyse relevant data to inform decision-making throughout the development.

The following sections of this chapter provide a concise overview of the results achieved in each task of WP2.

2.1 WP2 Methodology

In WP2 the following tasks were defined:

- T2.1 Define scope.
- T2.2 Identify requirements.
- T2.3 User needs.
- T2.4 Analyse data.
- T2.5 Stakeholder Alignment and Project Requirements Refinement.

The results of the WP2 tasks serve as input for the design and implementation phase of the OSCRAT platform's software in WP3.

2.1.1. Adjusting the Scope

The scope definition consists of CRA conformity activities flow, functionalities and limitations of the tools, general functionalities which in the result were presented in the form of user story diagrams.

To refine the preliminary scope of the OSCRAT tools defined in the project proposal, a state-of-the-art analysis of existing CRA-related tools and ongoing research initiatives in this field was conducted. The detailed results of this analysis are presented in Annex 1. The study covered nine ongoing EU R&D projects and five examples of commercial software tools.

The main outcomes of analysis are the following:

- The OSCRAT platform effectively addresses the needs of digital product developers under the Cyber Resilience Act (CRA), offering precise conformity checking and developer guidance for detected non-conformities.

- Vulnerability and incident management are fully aligned with internationally recognized standards.
- SBOM functionality is implemented at the level required for compliance.
- Future development opportunities include AI integration, interoperability with commercial testing tools, enhanced risk prioritization, lifecycle management, and certification support.
- The most comparable initiatives to OSCRAT are the CRAcoWi and CRA-AI projects.

To define the scope of the tools more precisely, a “General conformance activities flow” diagram for achieving CRA compliance was developed. The diagram enabled the identification of user roles, categories of products, and types of conformity assessment.

It facilitated the construction of a corresponding “CRA questionnaires flow” diagram containing questions that reflect the requirements of the CRA. These questions, linked to specific articles of the Regulation, were documented in a specially designed Excel file. This file includes user guidance and automatically generated tasks to support and gain product compliance with CRA. The structure of these tasks is illustrated in the “CRA Task Management Flow” diagram.

The flow diagrams and the Excel file are the result of the overall design of the OSCRAT platform, modelled as a User Story Diagram in the Enterprise Architect tool. The user story outlines the main functionalities of each tool. This high-level representation enabled the detailed design of functional requirements in the form of use cases for each individual tool.

Next, the user story and use case diagrams, along with the Excel file were used as input for the development of the graphical user interface, which was designed in the FIGMA screens in WP3.

2.1.2. Gathering CRA requirements

Each tool within the OSCRAT platform must address the specific requirements of the Cyber Resilience Act (CRA). To identify these requirements, a comprehensive analysis of the CRA Regulation was conducted. The results of this analysis were compiled into a specially designed Excel file.

The file, “**ESR_TechDoc_Requirements.xlsx**”, has a fixed structure aligned with the CRA requirements, including question sets, product categories, user roles, and evaluation criteria for both the organization and the product. It also defines tool responses, such as automatically generated generic tasks depending on the provided answers and contains comments as well as compliance assessment status indicators.

Consolidating all CRA-related requirements in a single file facilitates verification and monitoring of the completeness of the mapping between the tools and the CRA-specific requirements. Moreover, the fixed structure minimizes future development efforts while still allowing for content updates when necessary.

The Excel file, along with the flow diagrams, user stories, and use cases, constitutes a key input element for the software requirements specification in the WP3 development phase.

2.1.3. Identifying user needs

To ensure that the OSCRAT platform tools accurately reflect user needs and requirements, a dedicated survey was developed containing targeted questions. The collected responses were used to identify users' specific needs and the main challenges they face in understanding and implementing the CRA requirements.

Within WP2, one survey was conducted and a report analysing its results was prepared. Based on the conclusions drawn, a second, updated version of the survey was developed — clearer in structure and containing additional questions. The survey results will be used in next stages of the project to support potential updates to the tools' functionalities.

It should be noted that the identification of future user needs is not limited to WP2 activities. Similar efforts are also carried out within WP4, where feedback will be collected through training sessions, workshops, and CRA conformity assessment use cases conducted with the use of the OSCRAT platform tools.

2.1.4. Analysing data

The purpose of analysing all data collected in the previous tasks is to develop the most effective input material for the design and implementation phase of the software tools in WP3.

The comprehensive analysis of all elements defining the scope and requirements — including user stories, use cases, activity diagrams, FIGMA screens, and the CRA requirements documented in the Excel file — enabled the formulation of implementation tasks for the WP3 software development team. These tasks were reviewed during weekly Task Specification Meetings with project partners.

As a result, more than twenty detailed implementation tasks were defined, describing graphical interfaces, functionalities, possible actions and interactions, and the types of data used within each tool. This approach ensured a seamless transition from high-level requirement definitions to detailed, developer-oriented specifications.

2.1.5. Refining the project requirements

According to the project proposal: “The task involves aligning stakeholders' expectations and refining project requirements within the OSCRAT initiative (...)”.

This task's goal is to ensure consistency between stakeholder expectations and OSCRAT project objectives. It involves validating key decisions and deliverables with stakeholders and refining project requirements to accurately reflect their needs.

For now, within WP2, a new version of stakeholder's survey has been launched, but the final data analysis and requirements specification depend on the forthcoming ENISA directives on harmonised standards expected by January 2026, so after finishing WP2.

2.2 MS4 Milestone

Milestone 4 (MS4) of the project consists of performing a comprehensive requirements analysis for the CRA tools. This deliverable, D2.1, provides a complete summary of the scope definition, user needs and preferences, functional requirements, and CRA-specific requirements for each tool.

All relevant information was gathered through stakeholder surveys and subsequent data analysis. Review meetings with project partners were also conducted to ensure that all relevant inputs were incorporated into the scope and requirements definition for the tools.

All supporting evidence, including survey results, data analysis reports, stakeholder feedback, and meeting minutes, has been documented and stored on the UNICIS platform.

In addition, a set of quality assurance indicators was established to verify the achievement of WP2 objectives, as presented in Table 1 below.

The first two indicators relate to Task T2.1 – Defining Scope. It should be emphasized that all identified functionalities and limitations were properly documented, and all CRA-specific requirements were addressed by the OSCRAT tools. However, since the total number of potential CRA-specific requirements cannot yet be determined (pending updated ENISA regulations for harmonized horizontal and vertical standards), the value of the second indicator cannot currently be evaluated.

The third indicator, referring to Task T2.5 – Stakeholder Alignment and Project Requirements Refinement, can be considered achieved, as the OSCRAT platform documentation and tools include built-in traceability references to all CRA requirements.

Related Task	Quality KPI definition	Source of verification
T.2.1. – Define Scope	The percentage of functionalities and limitations that are fully documented in the scope.	Number of documented functionalities and limitations / Total number of identified functionalities and limitations
T.2.1. – Define Scope	The percentage of CRA-specific requirements identified and documented.	Number of identified CRA-specific requirements / Total number of potential CRA-specific requirements
T.2.5. - Stakeholder Alignment and Project Requirements Refinement	The ability to trace each requirement back to its source and through the development lifecycle	Traceability matrix or tools

Table 1: OSCRAT: Quality review Checklist for WP2 Tasks

The quality assurance indicators confirm that the objectives of WP2 have been successfully achieved. The scope and requirements of the OSCRAT tools were comprehensively defined, CRA-specific needs were thoroughly analysed (see chapter 5.2), and full traceability of requirements was ensured to support the implementation phase in WP3.

3. Sources of the Requirements

3.1 Assumptions, limitations and CRA-specific requirements

The identification and mapping of CRA-specific requirements provided a unified foundation for all OSCRAT tools. Each tool reflects a different aspect of compliance management from organisational readiness and product security to documentation, vulnerability handling, and incident response. Together, they form an integrated framework that supports enterprises, particularly SMEs, in meeting CRA obligations across the entire product lifecycle. This approach ensures consistency, traceability, and interoperability between the tools, while maintaining clear links to the legal and technical provisions of the Cyber Resilience Act.

Each of the five tools (Figure 1) corresponds to one or more of the four general areas of CRA compliance identified during analysis:

CRA area	Supported Tools	Description
Preliminary	CL	Establishes scope and applicability of CRA, identifies actor type, and determines whether exclusions apply.
Organisation	CL, INC, VUL	Covers governance, policies, processes, and responsibilities related to cybersecurity and compliance management.
Product	SBOM, INC, VUL, CL	Focuses on design, security features, update management, and component integrity of products with digital elements.
Documentation	DOC, CL	Ensures completeness and correctness of technical documentation and user information in line with CRA obligations.

Table 2: OSCRAT – Integrated application of CRA areas

In addition to the Cyber Resilience Act directive, to which the OSCRAT project and tool being developed are dedicated, another basic source of requirements is the Grant Agreement (Description of the Action (Part B), chapter 1.1 Objectives and activities) [1], and project plan deliverable D1.1 [2] and the assumptions contained therein regarding the tool and its planned functionality and quality.

The requirements resulting from these sources include such tool functionalities as:

- **Checklist Support:**
 - Checking applicability of CRA requirements for the Product with Digital Elements (PDE) – as specified in Article 2 of CRA,
 - Identification of the digital product category (product classification) – as specified in CRA Articles 7 and 8, Annexes III and IV,
 - generation assessment checklist (Articles from 13 to 25, Annexes I and II) – based on the CRA requirements for PDE's and organization's processes, depending on the role of organization in relation to the product: manufacturers, importers, distributors, open-source software stewards, authorised representatives,
 - producing conformity assessment reports based on the answers provided for the generated checklist (Article 28 and Annexes V and VI specifies requirements regarding the content of the declaration of conformity).
- **Software Bill of Materials (SBOM) handling support** (Annex I Part II (1) of CRA):
 - parsing project description files and SBOM report generation
 - SBOM compliant with standards (like SPDX or CycloneDX).
 - producing vulnerability scan report based on the generated/downloaded SBOM file.
- **Vulnerability support** (based on CRA requirements regarding vulnerability handling, especially Annex I Part II):
 - supporting users (SMEs) in the field of vulnerability handling, providing with a structured approach to manage vulnerabilities
 - enabling the reporting channel to relevant agencies, such as ENISA.
- **Incident handling support** (including requirements described especially in Articles 13 and 14 of CRA):
 - identification the severity (significance) of incidents,
 - enabling the reporting on significant incidents to cybersecurity entities (such as ENISA, EU-CyCLONE, CSIRTs).

- **Documentation Centralization:**

- providing a repository for digital product documentation (such as Conformity Assessment Reports, SBOM reports, Vulnerability Disclosure Policies, Incident Reports, Certifications of Conformity).

These functionalities are also reflected in the figure included in the Grant Agreement, illustrating the main pillars on which the OSCRAT tool will be based. The Figure 1 comes directly from the proposal.

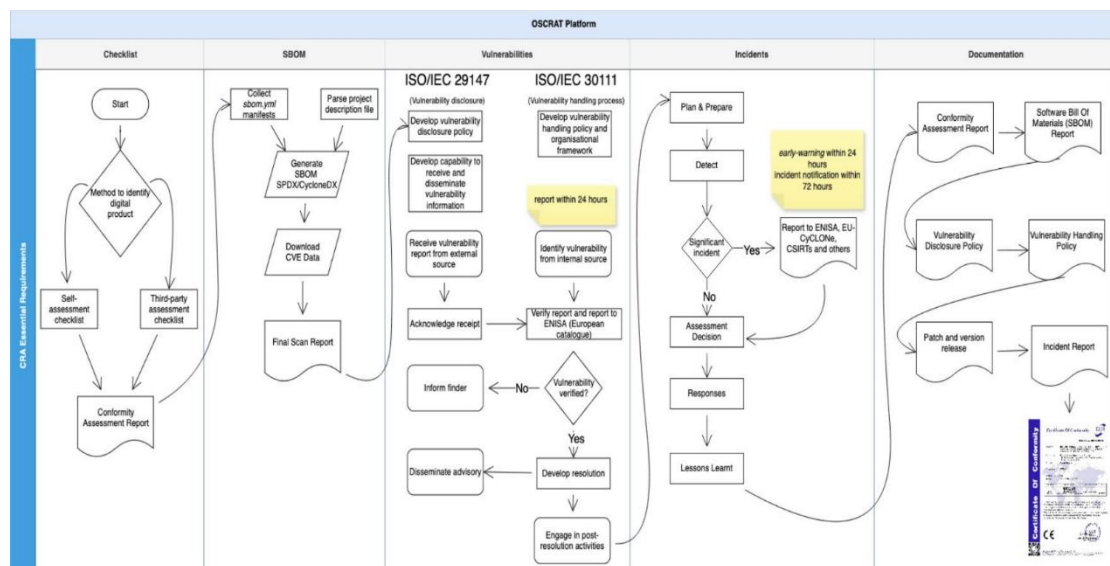


Figure 1: OSCRAT Platform - CRA Essential Requirements Tool (from Grant Agreement)

One of the main assumptions adopted already at the stage of preparing the project proposal and included in the Grant Agreement is the decision to build the OSCRAT tool based on the open-source Unicis Platform Community Edition [<https://www.unicis.tech/docs/>].

It gives the opportunity to use its extended capabilities, available functionalities (such as SAML, SSO, directory synchronization (SCIM), multi-tenant architecture, multi-factor authentication (MFA), REST API, webhooks and events, service logs and internationalization support (i18n)).

The above assumptions and initial requirements were considered when preparing the detailed design requirements for the OSCRAT tool. They were reflected in the user activity flow diagram in the OSCRAT tool (Chapter 4.1), the User Story diagram (Chapter 4.2) and the Use Case diagrams (Chapters 4.2 and 7.2) described later in the report.

3.2 State of the Art

To better define the requirements for the tool and its functionality, an analysis of similar tools, the current work in areas related to the project was conducted. The results were also a significant source of input data in the process of defining the requirements and functionality of the OSCRAT tool.

Annex 1 included an analysis of the current state of the art in assessing the CRA requirements' compliance, available tools supporting achieving and maintaining such compliance (including support for the incident and vulnerability handling processes). The research and analysis included both:

- information on the availability of commercial tools of this type, and
- ongoing projects aimed at developing new tools.

A comparison of the functional scope of the identified tools and projects in relation to the planned elements of the OSCRAT tool is presented in a summary table at the end of Annex 1.

Annex 2 includes the results of the analysis of incident and vulnerability handling aspects that should be considered when planning the functionality of the OSCRAT tool.

The aim was to identify the currently used incident and vulnerability reporting methods provided by European agencies (such as ENISA and local CSIRTs), as well as the scope of data collected by these agencies, especially during the initial stages of handling incidents and vulnerability reporting.

An analysis of available tools for generating **SBOM** (Software Bill of Materials) files and vulnerability scanning tools (based on these files) was also conducted. For selected commonly used, open-source available tools the tests of results they provide were performed and information on the result of the tests is presented in Appendix 2.

The most suitable and commonly used tools for the SBOM generation and vulnerability scanning seem to be:

- **Syft**, which enables generating an SBOM file and converting between CycloneDX, SPDX, and Syft's own format,
- **Trivy** – an SBOM generation tool, based on CSAF language - as stated on ENISA's website, EU vulnerability database (EUVD) builds upon the OASIS CSAF to support automation in the processing, production, and distribution of security advisories.
- **Grype** – a vulnerability scanner that can work with Syft as an SBOM file generator.

As part of the development of the OSCRAT tool, the use of the above ready-made solutions supporting vulnerability handling process with SBOMs usage should be considered.

3.3 Questionnaires

To obtain information on the experience and needs of users representing micro, small, and medium-sized enterprises in the European Union in the Cyber Resilience Act, a series of meetings and discussions were conducted. As a result of these efforts, a stakeholder survey was developed.

The prepared survey was addressed to micro, small, and medium-sized enterprises offering software and hardware solutions. Respondents included manufacturers, distributors, and maintainers of open-source software. In addition, opinions were obtained from enterprises offering cybersecurity services, a telecommunications operator, and research and development departments. In the survey, enterprises presented their current approaches, activities, and practices regarding issues relevant to CRA. Information was collected on their current methods of operation in the areas of risk management, maintaining documentation related to products with digital elements, product labelling, handling SBOM, vulnerabilities, and incidents. Respondents were also asked to indicate their currently used norms and standards, as well as tools supporting these processes.

The survey questions were prepared by the OSCRAT project team and sent to business partners and companies potentially interested in the results of the project.

The complete questionnaire addressed to representatives of micro, small, and medium-sized enterprises in European Union is presented in Annex 7.

3.4 Knowledge and experience from partners

Each partner collaborating within the project consortium has their own experience gained from implementing national and EU projects on security topics. This experience constitutes a contribution from each partner to the project but may also influence the definition of requirements for the tool being developed.

3.4.1. Lukasiewicz-AI

Lukasiewicz-AI took part in several EU security related projects. Team members were involved in developing software and IT security support systems. Some team members are employees of the IT product security assessment laboratory

at Łukasiewicz-AI. Through previous projects and ongoing work, team members acquired experience useful for the project, including:

- Available open-source SBOM analysis tools, obtained in other projects (e.g., OWASP Dependency-check, Intel cve-bin-tool, Trivy, Grape, Bomber),
- SBOM formats: SPDX (ISO/IEC 5962), CycloneDX (OWASP Foundation ECMA-424), SWID (ISO/IEC 19770-2),
- Vulnerability databases: CVE, NVD, OSV, RedHat,
- CVSS – vulnerabilities scoring system,
- Vulnerability scanning/analysis tools: Nmap, Burp Suite, Zap, Nessus,
- Incident detection systems: Wazuh, Snort, Suricata,
- CSA requirements according to cybersecurity certification,
- NIS2 according to incident reporting.

This knowledge was used to develop the requirements for the OSCRAT software.

For commonly used, mainly open-source tools available on the market, state-of-the-art command-line execution tests were conducted (as presented in chapter 3.2), which would allow their use within the OSCRAT tool. Knowledge of vulnerability and incident management tools and standards helped to define the requirements for the description of these elements.

The requirements were described graphically using the software design tools used at Łukasiewicz-AI (primarily Enterprise Architect, which allows for web-based project screenshots for partners, the non-commercial Draw.io tool, and office software).

3.4.2. OVES Enterprise SRL

OVES leads development work related to software development. Experience in product, web platforms delivery, cybersecurity, dual use tech (commercial/military), fintech and outsourcing services. knowledge in Cyber Security and Product Management.

Skills and expertise used in the project (product management, software architecture).

The project leveraged knowledge acquired throughout the software development lifecycle. Based on diagrams (user story and use case diagrams) selected for graphical representation of requirements, and utilizing commonly used techniques and tools, mock-up of screens, the tool prototype was created for the OSCRAT tool.

3.4.3. ENERSEC Technology SRL

Leveraging deep expertise in the evolving European regulatory landscape, Enersec Technology provides comprehensive services throughout the entire lifecycle of security controls for complex systems. The company specializes in aligning security strategies with the stringent requirements of the Cyber Resilience Act (CRA) and the NIS2 Directive, covering planning, assessment, audit, and continuous improvement.

Enersec's team of certified experts delivers high-level advisory services in Information Security Governance, Risk Management, and Compliance (GRC). They focus on helping organizations navigate the complexities of privacy regulations and the enhanced security obligations mandated by EU legislation.

Within the OSCRAT project, the team applies this regulatory knowledge to strengthen governance frameworks, risk analysis methodologies, and audit processes. This expertise is pivotal in defining requirements for the product evaluation process, preparing compliance-focused assessment criteria, and establishing a product lifecycle scope that adheres to the security-by-design principles of the CRA.

3.4.4. Unicis.Tech OÜ

A micro-SaaS dedicated to streamlining compliance, security, risk, and privacy management for small and medium-sized enterprises (SMBs).

An important contribution from the partner is the Unicis open-source platform, which, in accordance with the initial assumptions of the project (as stated in the Grant Agreement), is the basis for building the OSCRAT tool.

Defining the platform requirements required considering the current functionality and limitations of the Unicis platform itself. So, Unicis contributed to the project with experts and open-source contributors, and the resulting experience in cybersecurity, data protection, risk management, and compliance. Team members (with ISO certifications, Data Protection Officer, Chief Information Officer, and more) participated in defining requirements, preparing task specification for the tool development.

4. Scope Definition (T2.1.)

Defining the scope of the CRA tools is outlining its basic functionalities and limitations. It provides a presentation of the tools including full traceability from CRA regulation to implemented features and user needs integration.

4.1 CRA conformance activities flow

To present all CRA conformance workflows the flow diagrams for all CRA activities have been developed:

- **Figure 2:** General CRA classification and assessment flow - presents generally guidance for CRA product classification and assessment,
- **Figure 3:** CRA questionnaires flow - presents in details process of questionnaires self-assessment according to CRA requirements based on questionnaires,
- **Figure 4:** CRA Task management flow - presents workflow for task management related with incidents and vulnerabilities management (CRA obligatory post-market activities).
- **Figures 5, 6:** – CRA Conformity Assessment Guide according to modules A, B + C, and H (Annex 12).

4.1.1. General CRA classification and assessment flow

The diagram presents an overview of the required actions related to CRA compliance. It illustrates the procedure that each stakeholder should follow to meet the CRA requirements and achieve conformity. These actions can be divided into the following phases presented on Figure 2 General CRA classification and assessment flow:

- **Categories of entities** – assessment of the role of the entities as defined in the CRA (manufacturer, importer, distributor, authorized representative or open-source steward).
- **Product evaluation** – Preliminary product evaluation of whether the product falls within the scope of the CRA and meets the criteria specified therein.
- **Classification of the product** – classification of the product according to the categories and annexes defined in the CRA.
- **Conformity** – determination of the appropriate conformity assessment procedure in accordance with the CRA (self-assessment, third-party assessment, or the need to comply with additional standards).

- **Identifying security requirements** – determination of the applicable conformity requirements based on the product's classification under the CRA and its annexes, as well as any relevant external standards.

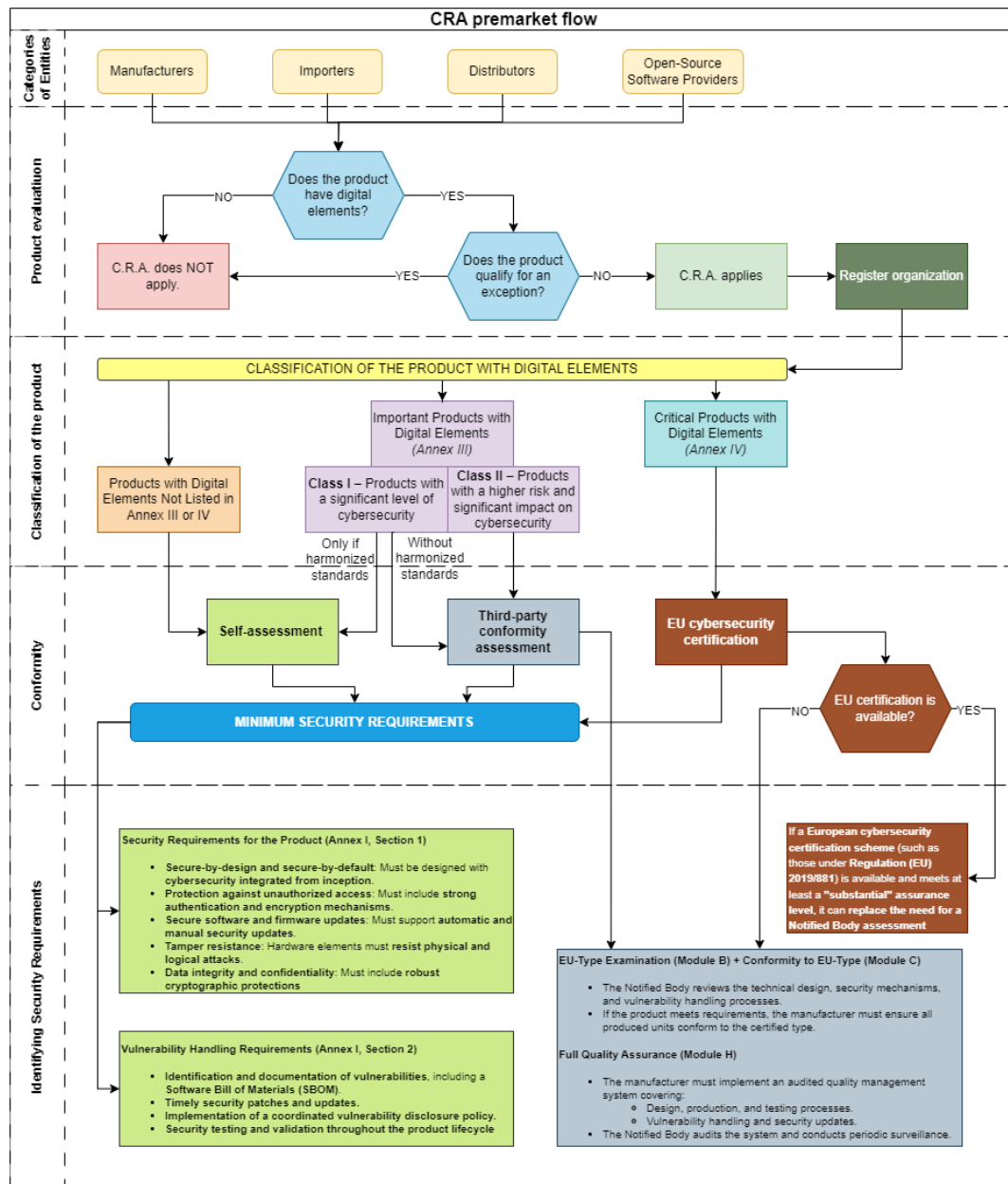


Figure 2: OSCRAT – General CRA Classification and Assessment Flow

4.1.2. CRA Questionnaire Flow

The CRA conformity assessment is conducted as questionnaires based on a defined list of requirements to be met. These requirements cover aspects related both to the product itself and to the organization. The specific set of applicable requirements depends on the type of organization, as different organizational types may be subject to different questions.

For this reason, the CRA requirements and their corresponding questions have been organized by topic and assigned to the respective organization types. The diagram Figure 3 CRA questionnaires flow (in its upper section) illustrates how the questions associated with the requirements have been classified and structured.

The second part of the diagram presents a proposed approach for taking actions within the system based on the answers provided to the questions. The proposal includes the creation of tasks (either automatically or manually by the user) for the requirements that are not fulfilled. The objective of this solution is to enable the management of non-compliant requirements by establishing tasks that will facilitate meeting these requirements and achieving full compliance.

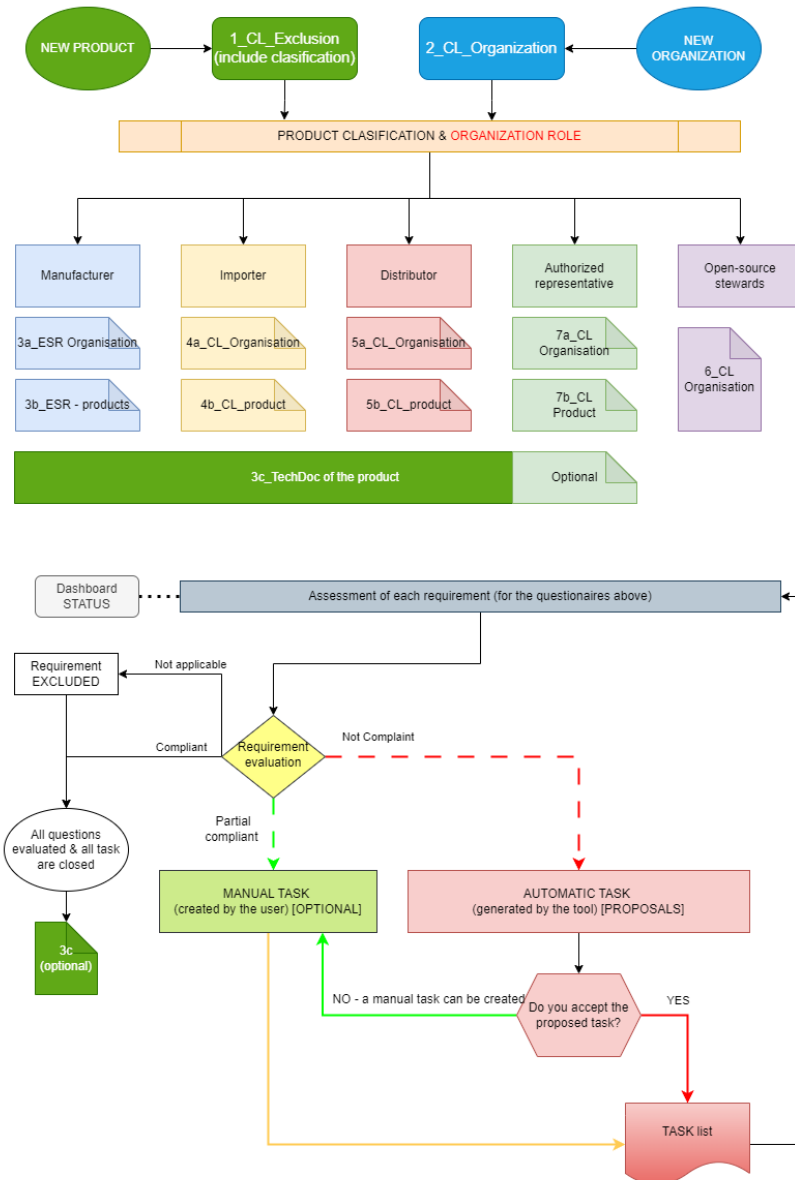


Figure 3: OSCRA – CRA Questionnaire Flow

4.1.3. CRA Task Management Flow

The application of compliance management tasks described in the previous paragraph for the assessment stage may be extended to include activities related to incident and vulnerability management. In accordance with the CRA, maintaining compliance requires the fulfilment of information obligations (reporting) as well as active management of incidents and vulnerabilities. Therefore, it is proposed to also generate tasks related to the management and handling of incidents and vulnerabilities, so that the user has a complete

overview of the current situation and the actions required to maintain compliance with the CRA during the post-market phase as well.

The diagram Figure 4 CRA Task management flow presents the proposed task management system for the conformity assessment stage, extended to include the activities related to incident and vulnerability management described above.

As a result, the user will have a list of tasks whose completion ensures full compliance with the CRA both at the pre-market and post-market stages, while simultaneously providing information on elements that may lead to non-compliance.

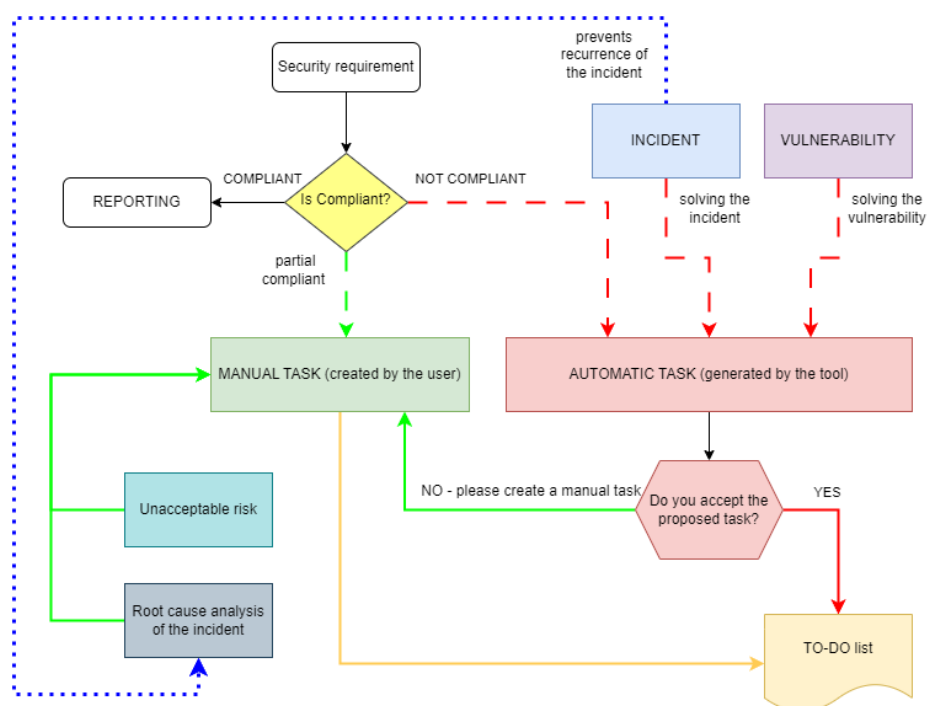


Figure 4: OSCRAT - CRA Task management flow

4.1.4. CRA Conformity Assessment Guide

Integrated directly into the compliance workflow, the CRA Conformity Assessment Guide serves as a strategic decision-support mechanism that bridges the gap between product classification and the technical self-assessment phase. This feature is triggered immediately after the user establishes the product's risk class, ensuring that the selection of the conformity

procedure (based on CRA Annex VIII) occurs before any detailed evaluation begins. Rather than navigating raw regulatory texts, the OSCRAT tool simplifies this complexity by automatically filtering available compliance pathways based on the product's defined classification, presenting the user only with legally viable options.

To assist in making an informed decision, the tool provides interactive guidance distinguishing between Product Certification (Module B+C) and Process Certification (Module H). It prompts the user to consider operational factors—such as the presence of an existing Quality Management System (e.g., ISO 27001) or the frequency of product updates—to recommend the most efficient route. For instance, the tool helps users understand when a full QMS audit (Module H) offers better scalability compared to repeated type examinations for individual products. Once the user finalizes this selection, OSCRAT locks the compliance strategy and dynamically configures the subsequent Self-Assessment questionnaires and documentation requirements to align strictly with the chosen module. CRA Annex VIII conformity modules for the given categories of products are presented on Figure 5.

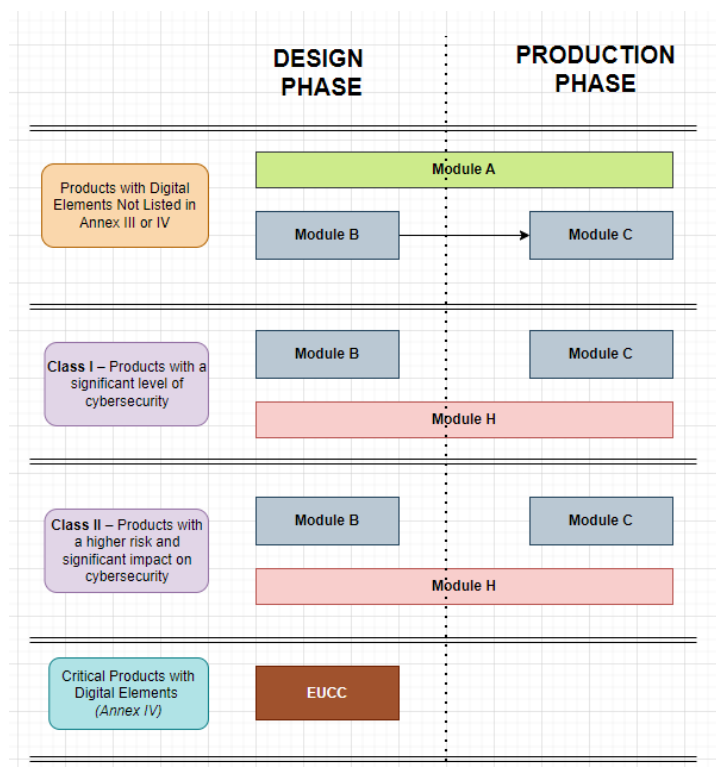


Figure 5: OSCRAT - CRA Annex VIII conformity assessment modules

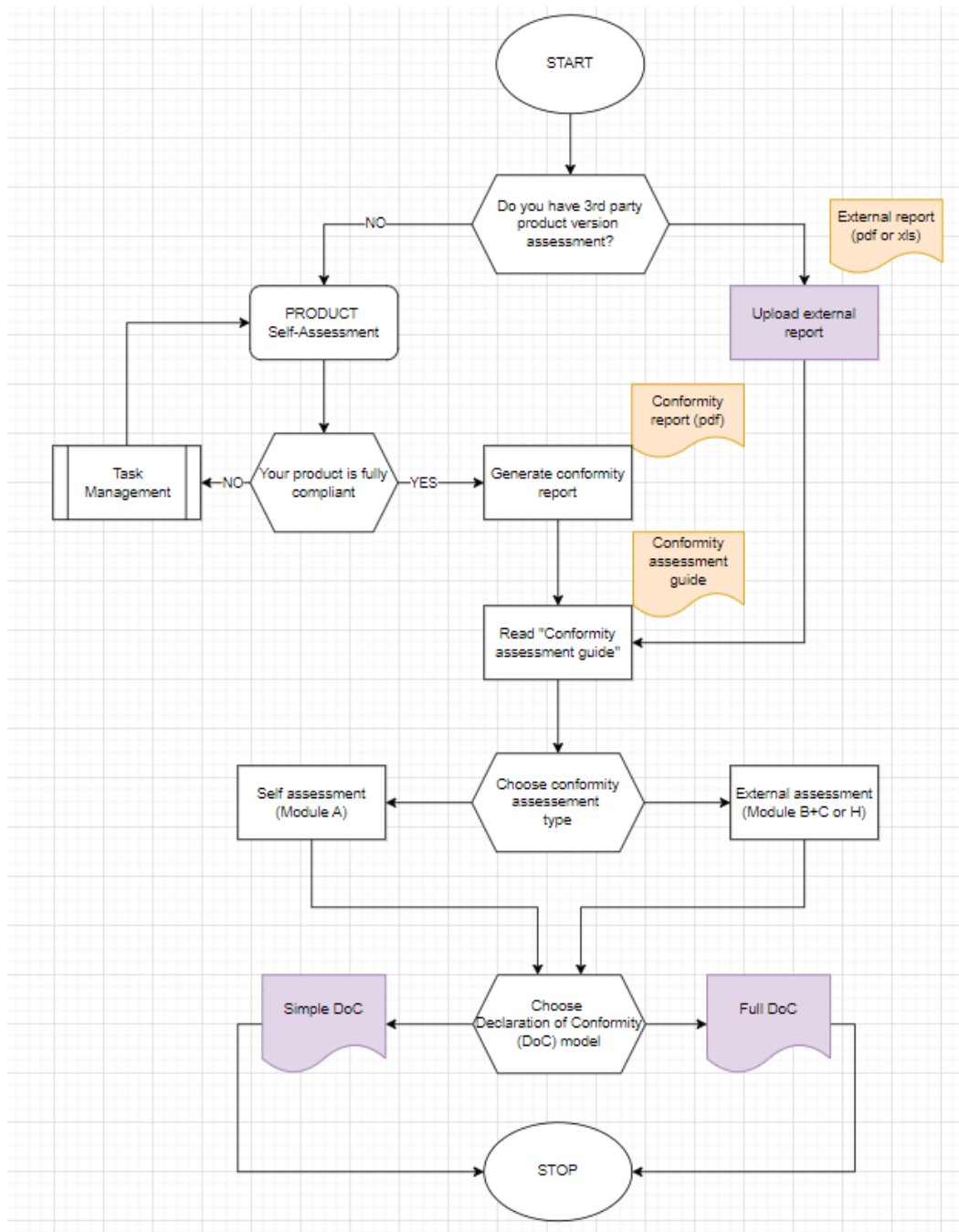


Figure 6: OSCRAT - Declaration of conformity flow

4.2. Functionalities and Limitation of the Tools

The tool consists of two main parts. First one relates to management of the user. The tool allows to register a user, recover password, etc. This part mainly applies for a registered user, where it is possible to manage information about the product or the organization. The second part is connected verifying the product and organization. The tool allows to make a verification without user registration.

This unregistered user can only carry out the applicability check, which includes verification if the CRA requirements apply to product, and, if applicable, classification of the product. The full verification is allowed only for registered user. The tool allows for this short verification to terminate the evaluation process if the product is not subject to CRA. In this case, the user does not need to go through the entire product and organization evaluation process.

The second part of the tool consist of 5 main modules (pillars) for verification and support in achieving compliance with CRA: Checklist, SBOM, Vulnerabilities, Incidents and Documentation. The division into the above modules is consistent with the division given in the grand agreement - Figure 1.

Each of these modules performs specific tasks to analyse given product and organization to deduce the compliance with Cyber Resilience Act.

The modules correspond to the natural course of work during the verification of a product and organization, from receiving information about the product to issuing a declaration of conformity, including also gathering data on related vulnerabilities and incident (presented as block of User Story diagrams: “Product assessment to find potential CRA conformity gaps” – Figure 8). Details about the modules are provided below.

4.2.1. Limitations

List of known limitations of the OSCRAT tools:

- **User Management:**
 - no comprehensive user management in terms of assigning permissions, roles, and deleting users
 - no storage of detailed user information - limited to the necessary minimum
 - user management is based on the Unicis platform functions, and the scope of management depends on its functionality
- **Organisation Management:**
 - registering only CRA applicable organisations
 - no organisation administrator role

- no option to completely delete data from databases
 - no storage of detailed information about the organisation - limited to the minimum necessary
 - no support for performing periodic activities for the organisation
 - organization management is based on the functions of the Unicis “teams management” and the scope depends on Unicis functionality
- **Product Management:**
 - registering only CRA applicable products
 - no full support for managing different product versions - limited only to introducing versions and registering vulnerabilities, incidents, SBOM and any other files related to that version
 - no integration with external software development supporting tools (e.g. bug tracker, source code repository, product documentation repository) – limited integration relates to possibility of SBOM generation for a git repository specified by the user
 - no support for performing periodic activities for the product
 - **User Tasks and Notifications:**
 - tasks (to be performed by the user, in the form of notifications) will only be implemented to the extent permitted by the UNICIS platform
 - no consideration of periodic notifications for the implementation of activities, e.g. periodic vulnerability scanning, periodic organisation's self-assessment activities
 - **Vulnerability Module:**
 - vulnerability registration notification only to the extent and in the manner that ENISA and national CSIRTs will make available at a given stage of the project (e.g. e-mail)
 - no automated alerts for detected vulnerabilities
 - no support in vulnerability disclosure
 - **Incident Module:**

- incident registration notification only to the extent and in the manner that ENISA and national CSIRTs will make available at a given stage of the project (e.g. email)
 - no automated categorization and prioritization
 - no automatic detection of suspicious activity (potential vulnerabilities) leading to an incident
- **SBOM Module:**
 - no function allowing SBOM file generation and analysis within the tool - uses of external open-source tools
 - no automated alerts for vulnerabilities - the user decides which of the found vulnerabilities he wants to register and handle in the tool (e.g. based on severity of the vulnerability)
- **Documentation Module:**
 - no support for multiple users working on a single document within the tool
 - documentation management limited to providing the most necessary documentation templates (for vulnerabilities, incidents, risk analysis) with the possibility of editing them on the platform
- **CRA Conformity Assessment Module:**
 - conformity assessment limited only to a self-assessment checklist in accordance with module A
 - conformity assessment according to the remaining modules B+C, H are not implemented on the platform, the platform will only provide a user guide with a flow diagram as an aid for a user (see Annex 12)
 - CRA compliance self-assessment divided into two parts: one for the organization and its processes related to secure product development, vulnerability management, incident management, and the other – checking the requirements for a specific product version
 - Checklist limited only for organizations and products applicable to CRA.

4.2.2. General Functionalities

General functionalities are available to the user from the main application window. This applies to both logged-in and logged-out users. The main functionalities include such OSCRAT tool features as:

- Organisation management
- Account and organisation permission management
- Organisation product management
- Dashboard review

The table 3 lists all the basic and most important functionalities available in the OSCRAT tool. The first column of this table presents the issue, the second column presents the capabilities and functionalities of the tool, and the third column contains a reference to the annex and chapter where all the detailed information can be found.

All subsequent tables in sections 4.2.1. – 4.2.7. contain similar information.

Issue, subject	Capabilities and Functionalities	Details
Account Creation Flow for Unregistered Users	Navigation (landing page) - unregistered users can create an account directly from the landing page. Users provide: Personal details (Name, Email, Password), Organization type (Natural Person or Legal Person), Organization details (Name, Role such as Manufacturer, Authorized, Representative, OSS Steward, Importer, Distributor).	D2.1 - Annex 3, Chapter 2 (Task #309)
Organization creation for Logged-In Users	Logged-in users can create additional organizations. Users select the organization type (Natural Person or Legal Person) and enter organization details.	D2.1 - Annex 3, Chapter 3 (Task #310)

	The creator is automatically added as a member of the newly created organization.	
New Product Creation for Logged-In Users	Users can create new products under their organization (from scratch, data taken from cache – form the last Applicability Check, based on existing product data). Users enter product information such as Name, Version and Description. Applicability check is integrated into the product creation flow. System guidance ensures that only products appropriate for the organization's role are added. Users can create new products under their organization (from scratch, data taken from cache – form the last Applicability Check, based on existing product data).	D2.1 - Annex 3, Chapter 4 (Task #311)
Product Details Page	Full view of product information and properties: Name, Category, Organisation Role, Incidents Count, Vulnerabilities Count, External Reporting, Assessment Type, Description Users can Edit, Withdraw or Delete the product Users can view or edit the Applicability Survey Product versions section fields and buttons Product versions are grouped into two tabs: Supported, Not Supported	D2.1 - Annex 3, Chapter 11 (Task #319)
Product Version Details Page	Comprehensive view of all Product Version details Displays key properties such as: Name, Status, Open Incidents Count, Open Vulnerabilities Count, Open Tasks Count Provides access to: CRA Compliance Assessment – View and Edit CRA compliance assessment of the product version, Declaration of Conformity – View and Download “Declaration of Conformity”, Related Information via multiple tabs (Tasks, Files, SBOM, Vulnerabilities, Incidents, Version Logs, Repositories).	D2.1 - Annex 3, Chapter 12 (Task #320)
Add New Product Version	Users can create new product versions.	D2.1 - Annex 3, Chapter 15 (Task #323)



Users can define version-specific fields such as Name, Description, and Supported / Not Supported status

Table 3: OSCRAT – The Scope and List of general functionalities for OSCRAT tool

4.2.3. Checklist

The process begins with an initial screening in the form of a high-level checklist. The primary objective at this stage is to determine whether the product falls within the scope of the CRA. Products deemed out of scope are filtered out immediately, preventing unnecessary further assessment. For applicable products, the user must next define their organization's role (Manufacturer, Importer, Distributor, or Authorized Representative), as this determines the specific legal obligations to be met (the methodology for defining these requirements is detailed in Section 5).

Before initiating the detailed technical self-assessment, the user is directed to the CRA Conformity Assessment Guide (refer to Chapter 4.1.4). This step is crucial for selecting the appropriate compliance path - whether Module A, B+C, or H - ensuring the subsequent evaluation is aligned with the correct regulatory framework.

During the questionnaire phase, the tool is designed to facilitate third-party validation where required. If the chosen path involves a Conformity Assessment Body (CAB), the tool structures the collected data to streamline the external audit process, thereby accelerating the issuance of the CRA compliance certificate. Finally, depending on the questionnaire results, the system either generates a list of generic tasks to address any unmet requirements or, if full compliance is achieved, produces the final conformity assessment report.

Issue, Subject	Capabilities and Functionalities	Details
Applicability Check for CRA for Unregistered User	Accessing the Applicability Check (Button on Landing Page) – to determine whether the product falls under the scope of CRA	D2.1. – Annex 3, Chapter 1 (Task #307)
	Questionnaire Logic (based on <i>CRA – XLS Sheet CL_Exclusion</i>) – users are guided through a structured set of questions evaluating product applicability	
	Outcome Path: product is eligible or not, eligible product classification: • Critical, Important • Class I, Important • Class II, Other	
	User session data persistence (product details and results)	

CRA Compliance Assessment for a Product Version	Automatically initiated CRA compliance self-assessment, when a new product version is created	D2.1. – Annex 3, Chapter 5 (Task #312)
	Self-Assessment supports a structured self-evaluation process aligned with CRA requirements	
	Hierarchical level of questionnaire: Area or requirements / Requirement / Question	
	Organization role-specific questionnaires references	
Administration of a Product Assessment Questionnaire Template	Compliance self-assessment questionnaires are not hardcoded.	D2.1. – Annex 3, Chapter 6 (Task #314)
	Define a questionnaire template in a structured (JSON) format (based on the CRA Requirements Spreadsheet)	
	Modify questionnaire template (template can be updated over time via an import mechanism)	
	Mechanism to upload/import new questionnaires	
Product Assessment Dashboard, Visualization, PDF Export	A dynamic dashboard summarizing compliance progress for each product assessment	D2.1. – Annex 3, Chapter 7 (Task #315)
	Dashboard includes assessment status tables, product assessment charts, progress bar/indicators	
	Export Conformity Assessment Report (pdf document)	
Administration of an Organization Assessment Questionnaire Template	Compliance self-assessment questionnaires did not hardcode	D2.1. – Annex 3, Chapter 8 (Task #316)
	Define a questionnaire template in a structured (JSON) format (based on the CRA Requirements Spreadsheet)	
	Modify questionnaire template (template can be updated over time via an import mechanism)	
	Mechanism to upload/import new questionnaires	
CRA Process Assessment for an Organization	Automatically initiated CRA organizational process self-assessment, when a new organization is created.	D2.1. – Annex 3, Chapter 9 (Task #317)
	Hierarchical level of questionnaire: Area or requirements / Requirement / Question	
	Organization Role-Specific Questionnaires references	

Organization CRA Compliance Dashboard, Visualization & PDF Export	A dynamic dashboard summarizing compliance progress for organizational assessment	D2.1. – Annex 3, Chapter 10 (Task #318)
	Dashboard includes assessment status tables, product assessment charts, progress bar/indicators	
	Export Conformity Assessment Report (pdf document)	
Requirements Evaluation – Automatic Task Generation new	Automatic task creation based on requirement-level self-assessment results (Not Compliant / Partially Compliant / Compliant / Not Applicable).	D2.1. – Annex 3, Chapter 21 (Task #336)
	Tasks include predefined fields and product version association	
	Additional logic for marking assessments as completed when all requirements are Compliant or Not Applicable	

Table 4: OSCRAT - The scope and list of main functionalities for checklist module

4.2.4. SBOM

A user of the tool performs operations to generate Software Bill of Materials (SBOM) in format SPDX or CycloneDX. The SBOM can be imported by suitable manifests or generated by the parsing the project description file. In either case, the final SBOM is scanned by CRA tool to generate the list of vulnerabilities connected with product.

Issue, Subject	Capabilities and Functionalities	Details
SBOM Management	Display a list of all SBOMs associated with the selected product version	D2.1. – Annex 3, Chapter 20 (Task #328)
	Generate SBOMs directly within the system	
	Import externally generated SBOMs	
	Download existing SBOMs	
	Scan SBOMs for vulnerabilities, resulting in a generated Vulnerability Report	
	Review the Vulnerability Report and selectively add identified vulnerabilities to the Vulnerability Module	
	Configuration of the project path and access data to generate SBOM	

Table 5: OSCRAT - The scope and list of main functionalities for SBOM module

4.2.5. Vulnerabilities

Vulnerabilities can be assigned using generated list after the scan of the SBOM, importing the list or manually adding the vulnerability. The tool supports gathering data and handling vulnerabilities. The tool is generating the tasks for the user automatically. The user can agree with generated task or deny it. A task also can be added manually. More about task management can be found in the section 4.1. Handling all vulnerabilities requires for example introducing corrective actions (mitigations) or reporting vulnerability to corresponding CSIRT.

Issue, Subject	Capabilities and Functionalities	Details
Add New Vulnerability	Create a new vulnerability record	D2.1. – Annex 3, Chapter 16 (Task #324)
	Associate vulnerability with a specific product and version	
	Input key details such as name, status, severity, date of discovery, etc.	
	Attach supporting documents related to vulnerability	
Edit Vulnerability	Modify existing vulnerability records	D2.1. – Annex 3, Chapter 18 (Task #326)
	View read-only fields and update editable information	
	Attach or manage related documents	
Vulnerability Details Page	View complete vulnerability details	D2.1. – Annex 3, Chapter 13 (Task #321)
	Access an attachment section showing all associated files	

Table 6: OSCRAT - The scope and the list of main functionalities for vulnerabilities module

4.2.6. Incidents

Incidents are handled the similar way as vulnerabilities. In the first step the incident needs to be registered into the tool, then the tool supports handling the incidents e.g. by introducing corrective actions (mitigations) or reporting vulnerability to corresponding CSIRT.

Issue, Subject	Capabilities and Functionalities	Details
Add New Incident	Create a new incident record	D2.1. – Annex 3, Chapter 17 (Task #325)
	Associate the incident with a specific product and version	
	Input details such as: ID, status, classification, attack type, asset details, reports, etc.	
	Attach supporting documents related to the incident	
Edit Incident	Modify existing incident records	D2.1. – Annex 3, Chapter 19 (Task #327)
	View read-only fields and update editable information	
	Attach or manage related documents	
Incident Details Page	View complete incident details	D2.1. – Annex 3, Chapter 14 (Task #322)
	Access an attachment section showing all associated files	

Table 7: OSCRAT – The scope and the list of main functionalities for incident module

4.2.7. Documentation

Product documentation is collected throughout the assessment process. Documents provided regarding the product, organization, or procedures assist in assessing whether the product meets CRA requirements. Documents are delivered to the tool during the operation of each of the above modules.

Issue, Subject	Capabilities and Functionalities	Details
General Description	Open text sections to describe products, versions	D2.1 - Annex 3, Chapters: 4, 7, 11, 12, 15 (Task #311, #315, #319, #320, #323)
	Adding images, uploading related documents	
	Support period determination of the product version	
	Data saved per product version and automatically included in the published report	
Specification, description of the design & development processes of the product	Open text sections, description fields to allow users to describe how design principles ensure CRA compliance	D2.1 - Annex 3, Chapters: 4, 11, 12, 15 (Task #311, #319, #320, #323))
	Adding images, related documents (diagrams, files)	
Vulnerability handling process	Documents' templates for vulnerability handling process available for the users	D2.1 - Annex 3, Chapter 20 (Task #328)
	Users can adjust the pre-filled (templates) content.	
	SBOM files management (generating, uploading, downloading).	
	Reports generation from the vulnerability scan	
	Possibility to publish vulnerability disclosure policy, selected product documentation	
Production & Monitoring processes documentation	Questionnaires for the self-assessment of the organization documentation elements and content (to check missing documents)	D2.1 - Annex 3, Chapters: 6, 7, 8, 10, 11, 12 (Task #314, #315, #316, #318, #319, #320)
	Uploading evidence documents for the self-assessment activities, documentation related to the processes production within the organization, monitoring processes related to the production activities	
	Reports for the organization's compliance self-assessment	

Cybersecurity Risk Assessment	Risk assessment template available, including information how the essential cybersecurity requirements (CRA Annex I) are applicable - (users can modify predefined sections)	D2.1 - Annex 3, Chapter 13, 14, 16, 17, 18, 19 (Task #321, #322, #324, #325, #326, #327)
Conformity Verification	For the product with self-assessment - support in preparation of Declaration of Conformity (DoC) document for the product - document template available.	D2.1 - Annex 3, Chapter 7, 10, 12, 20 (Task #315, #318, #320, #328)
	For the product assessed by 3rd party – upload of the assessment report and signed DoC.	
	DoC available in the tool, can be downloaded	
	Evidence of conformity files available in the OSCRAT tool (SBOM files, vulnerability scan reports, self-assessment reports).	

Table 8: OSCRAT – The scope and list of main functionalities for documentation module

The documentation pillar provides functionality for creating, maintaining, and verifying all forms of documentation required under the CRA. This includes both technical documentation and user-facing information such as installation instructions, security guidance, and update procedures. The module acts as a unifying repository, linking documentation with evidence generated by other OSCRAT tools (checklists, SBOM records, incident and vulnerability reports, logs). It ensures completeness, consistency, and readiness for conformity assessments or inspections.

The documentation module developed within the OSCRAT environment defines how the system supports the creation, maintenance, and publication of technical documentation required under Annex VII of the CRA. The module covers the following key elements:

- Editable and guided text sections for CRA Annex VII requirements.
- Integration with other OSCRAT components such as the Checklist (CL), SBOM, Vulnerability (VUL), and Incident (INC) modules.
- Evidence collection from compliance assessments, vulnerability, incident logs, reports.
- Template-based structure for risk assessment (see Annex 13 – Template for Risk Assessment), vulnerability and incident handling, conformity verification.

- Publication and public release of documentation under the tenant's namespace.
- Non-functional requirements covering usability, security, auditability, and performance criteria.

The module consolidates information from all OSC RAT components to generate complete, CRA-compliant technical documentation. It ensures that every Product with Digital Elements developed or managed within OSC RAT can produce regulator-ready documentation aligned with CRA Annex VII. A detailed functional and technical specification of the DOC module is provided in Annex 9 Documentation pillar for OSC RAT, attached to this report. Furthermore, as part of this work, templates for vulnerability and incident reporting were developed. They are included in Annexes 10 and 11 attached to this report.

4.3 User Story – General View

To present the description of general concept and architecture of the OSC RAT tool presented above, and for a high-level visualization of the course of user activities, User Story diagrams have been developed.

The purpose of preparing the User story diagrams was to serve as the input for:

- development of guidelines, tasks for developers (so-called task specifications) developed during regular meetings of partners (Enersec, Łukasiewicz-AI, Unicis) as a part of Work Package 2 activities,
- preparation by the developers (OVES) an end user mock-up screens and presenting these activities using the mock-up screens in Figma tool, as a part of Work Package 3 activities.
- use while working on the tool prototype in Work Package 3.

The developed diagram was the first attempt at a high-level description of how the OSC RAT tool should work. The initial vision was analysed in Task 2.4, so it was later changed, modified several times, and during the task's specification activities, because of analysis, consortium members' discussions. Some activities initially defined in the User Story diagrams were further adapted to expected user needs.

User activities (primarily the PDE manufacturer) can be divided into two groups:

- so-called, in OSC RAT project “pre-market” activities, encompassing activities prior to product placement in the EU market, including product classification, conducting CRA compliance assessment activities, and preparing the CRA Declaration of Conformity.
- “post-market” activities, encompassing further activities after placement in the EU market, encompassing functions that maintain compliance

with CRA requirements, such as vulnerability and incident management, and periodic compliance reassessment, especially in the event of significant changes or new product versions.

Further down in the report, **Errore. L'origine riferimento non è stata trovata., Errore. L'origine riferimento non è stata trovata.** Present functions for the pre-market phase, planned for implementation in the OSC RAT tool. **Errore. L'origine riferimento non è stata trovata., Errore. L'origine riferimento non è stata trovata.** and **Errore. L'origine riferimento non è stata trovata.** present functions for the post-market phase, divided into product management, vulnerability management, and incident management.

The User story diagrams show the actions that the "Applicant for the product assessment" should be able to perform in the OSC RAT tool.

4.3.1. “Pre-Market” User Story Diagrams

For the pre-market phase, these activities are divided into main areas, within areas – groups of activities (as presented and described below).

1. Starting work with OSC RAT tool (Figure 7)
 - a. Home page - the user should start interaction and working with OSC RAT on the start screen (Home page). The user should have possibility to perform CRA applicability check for his product, prior to registering himself on the OSC RAT platform. Based on the requirements, and as discussed and agreed during the project consortium’s meetings, workshops, the user should be able to take the following actions on the start screen:
 - i. An **Unregistered User** may:
 - carry out the so-called Applicability check for his product, which includes:
 - verification that the CRA requirements apply to its product, and (if applicable),
 - classification, i.e. assistance in assessing which class the product is in accordance with Annexes III and IV of the CRA (Important Class I, Important Class II, Critical, or other types of PDE),
 - **Register**, create a user account on the OSC RAT platform, by completing registration form and setting a password
 - ii. A **Registered User** may:
 - Login to OSC RAT account,
 - Perform a password recovery activity using e-mail addressed provided during registration.

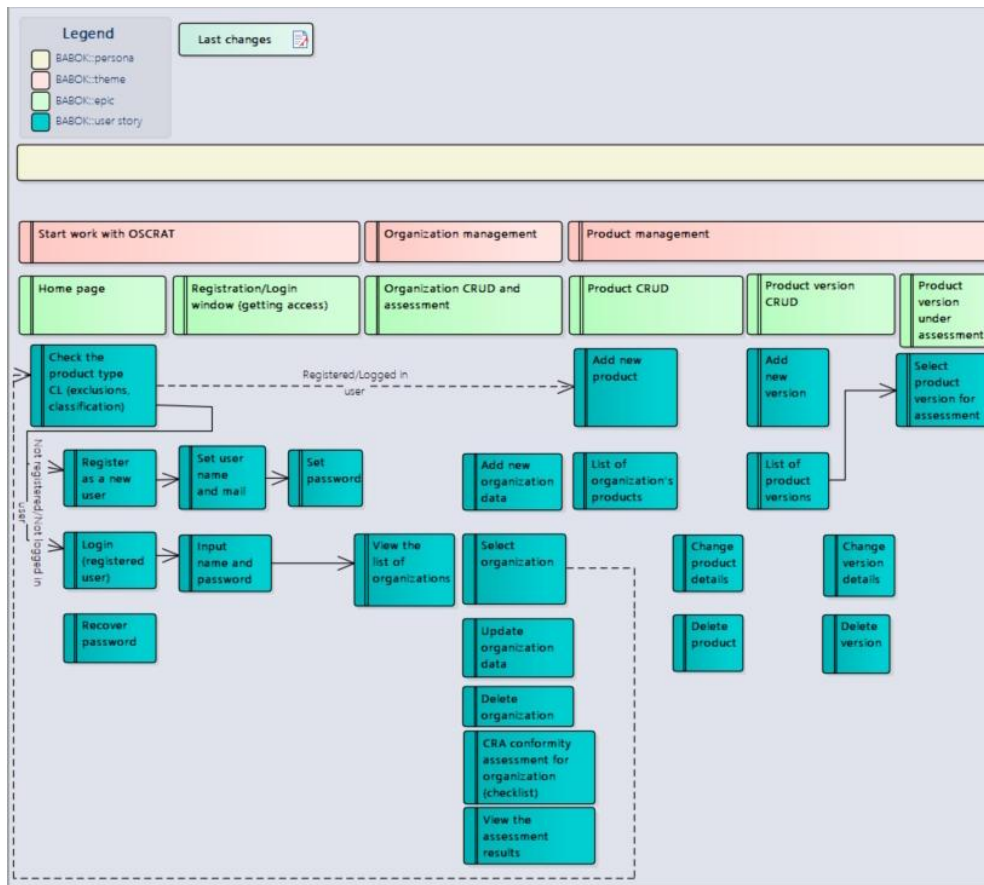


Figure 7: OSCRAT - User Story (pre-market) activities diagram part 1

2. Organization management (**Errore. L'origine riferimento non è stata trovata.**) - the part where the registered user can manage the organization, its products, where the user can perform the CRA requirements check of his organization (the process-oriented part of the CRA conformity assessment).

- A registered and logged in user should have possibility to conduct activities in the context of various organizations and their products, depending on the organization selected during login or selected later from the list of available organizations.
- For selected organization, the user should have possibility to:
 - manage the organizations data: add a new organization, edit the information of currently selected organization from the list, delete the organization.

- perform the CRA conformity assessment for the organization's processes, as required by the CRA, using predefined questionnaires (checklists) - the organization can be reassessed (periodically or on the user's demand – e.g. if significant changes in processes occurs).
 - View the organization's assessment results.
- 3. Product management (**Errore. L'origine riferimento non è stata trovata.**) – the functionality should give the user possibility to manage the products and their versions within the organization.
 - User may add new product on different ways:
 - using data stored in a browser cache collected during the “Applicability check” (when the applicability check was performed before user’s registration in OSCRAT),
 - entering all product data from the beginning (“from scratch”) and performing an Applicability check for PDE,
 - using data from existing product and changing selected data
 - For already existing product – edit data or delete selected product.
 - Article 13(10)(11), Annex VII (1)(b) refer to a product at the version level - since the CRA compliance assessment should be performed at the product version level, the user can manage and perform the CRA compliance assessment for each product version. Planned functionality includes:
 - Adding new and editing selected versions of the product – each product version has got its own properties, information about the assessment, SBOM files, related vulnerabilities and incidents (if any have been identified),
 - List of related incidents – adding and editing information collected as part of incident analysis and handling),
 - List of related Vulnerability (adding and editing information collected as part of vulnerability analysis and handling),
 - List of related Software Bill of Material (SBOM) files.

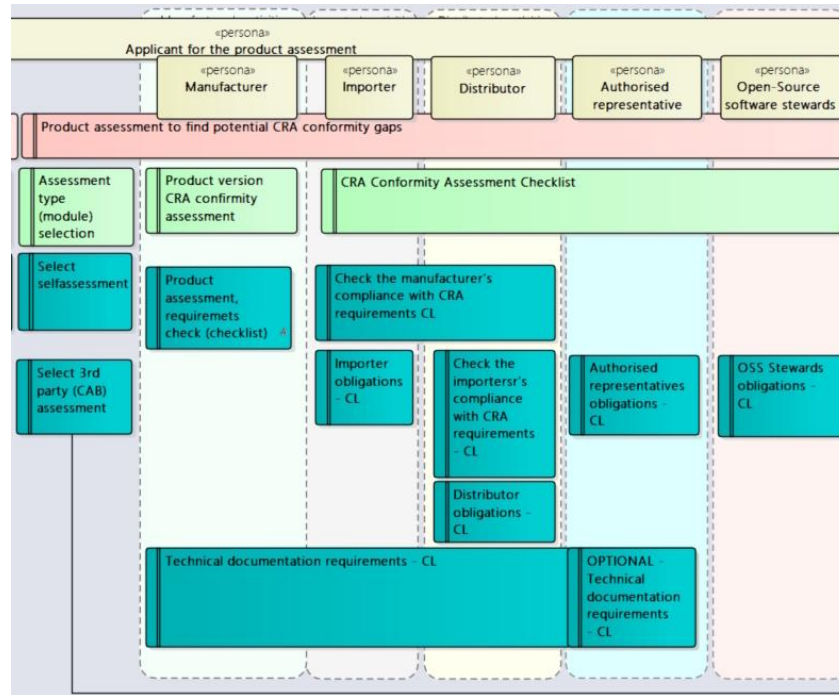


Figure 8: OSCRAAT - User Story (pre-market) activities diagram part 2

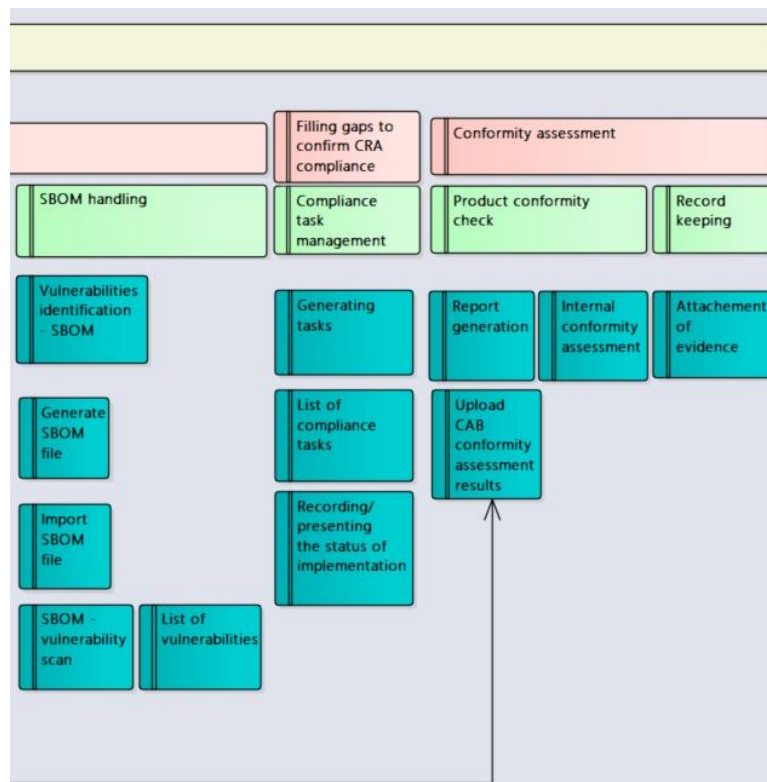


Figure 9: OSCRAAT - User Story (pre-market) activities diagram part 3

4. Product assessment to find potential CRA conformity gaps (Figure 8) – for selected product version user needs a functionality to perform the CRA conformity assessment. Together with the organization CRA conformity assessment (as described in point 2)) this phase should give the answer on the level of the product version compliance with CRA requirements.
 - The user can select if he wants to perform self-assessment or import the external assessment report from the Conformity Assessment Body (CAB) – depending on the product classification (the class is determined during the applicability check) the self-assessment can be performed (using the tool), or the assessment can be performed by CAB (for important/critical products).
 - The product version assessment is performed using dedicated checklist/questionnaire with selected CRA requirements, depending on the user's role: manufacturer, importer, distributor, open-source software (OSS) steward, authorised representative.
 - The technical documentation checklist – manufacturer, importer, distributor may check if required documentation for the product is available. Not required for OSS steward and optional for authorised representative (depending on the scope of the authorization made by the manufacturer).
 - Vulnerability scanning, based on the SBOM file for the product version (Figure 9) – as a part of the product compliance assessment, the vulnerability scan helps to identify potential vulnerabilities related to the product version and eliminate them before placing product on the market, as required by CRA. OSCRAT gives the possibility of performing such scan based on the SBOM files. OSCRAT user should be able to:
 - generate an SBOM for the software project Git repository, or
 - import an SBOM file generated in an external tool (in a required file format).
 - perform a vulnerability scan for selected SBOM, and view the results of the scan
 - for selected vulnerabilities found (if any), add the selected to the list of vulnerabilities related to the product version.
5. Filling gaps to confirm CRA compliance (Figure 9) – based on CRA conformity assessment reports, if non-compliance is detected, the user should be able to set tasks to be performed to eliminate the deficiencies in achieving CRA compliance.

6. Conformity assessment (Figure 9) - once the previously planned tasks have been completed, the user can generate a compliance assessment report and prepare it in the OSCRAT tool or import a self-prepared Declaration of Conformity - it should contain the elements listed in Annex V (for the full version) and Annex VI (for the simplified version of the document).

4.3.2. “Post-market” User Story diagrams

After registering in the tool, adding products for the organization, making the conformity assessments, the tool may be used for further handling of the products with their versions and related documents, files, vulnerabilities and incidents, to keep the CRA conformity.

1. For this, so-called “**post-market**” phase, Figure 10 shows the actions that the user can perform for PDEs. Products registered in the tool are subject to CRA requirements (in accordance with the applicability check and classification carried out in the “pre-market” phase). In the “post-market” phase, to perform product handling activities user gets access to the tool (Login functionality) and sets the Context of activities:

- selects the organization within which he logs in and performs product management activities,
- selects one of the products of this organization that he wants to manage (edit, delete, add a version).

Then, for selected product user should be able to:

- add new version – it requires an applicability check and assessment like for each new product during the “pre-market” phase,
- view and select existing product versions available on the list,
- edit selected product versions – the user can view the version details, which include:
 - description of the version,
 - editing CRA conformity assessment and preview of the assessment results - a dashboard to show status of the assessment (how many questions are answered, how many of them is fulfilled, etc.). When all the requirements are fulfilled, the user can generate (or upload external document) the Declaration of Conformity, where he declares that (based on the answers from the

questionnaire) the product is compliant with the CRA requirements.

- handling the SBOM files of the product version – as described above in point 4),
- incidents and vulnerabilities handling for the product version – as presented below in the description of diagrams:
 - Figure 11 User story - Post-market vulnerability handling activities and
 - Figure 12 User story - Post-market incident handling activities.

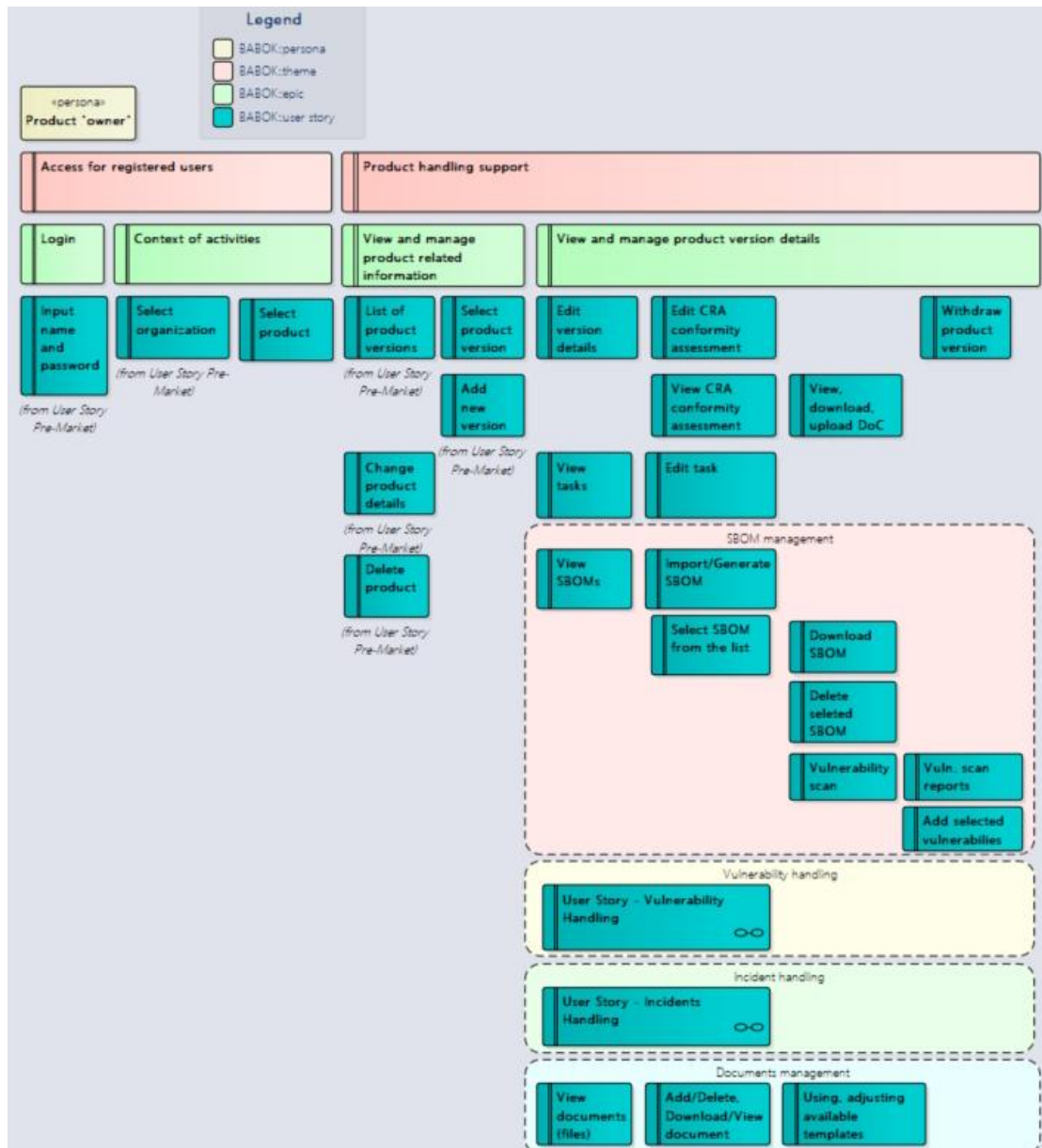


Figure 10: OSCRAT - User Story - Post-market PDE management in OSCRAT

- Next “post-market” related functionalities shown in **Errore. L'origine riferimento non è stata trovata.** are the vulnerability handling activities. Vulnerabilities are associated with a specific product version. Therefore, to manage vulnerabilities in OSCRAT, the user should select the product and version after logging in. Each version should allow the user to:

- add related vulnerabilities,
- view and edit data describing the vulnerability (as required by Article 14(2) of the CRA), including:

- basic information describing the nature of the vulnerability, its possible impact, and severity,
 - information about security updates or other corrective measures available to address the vulnerability,
 - information concerning any malicious actor that has exploited or is exploiting the vulnerability,
- add/remove files and additional documentation related to the vulnerability,
- import vulnerabilities; for example, in the case of a vulnerability scan based on an SBOM file, the user should be able to download from the list of detected vulnerabilities that are relevant and that the user wants to address in their security measures for the given product version.

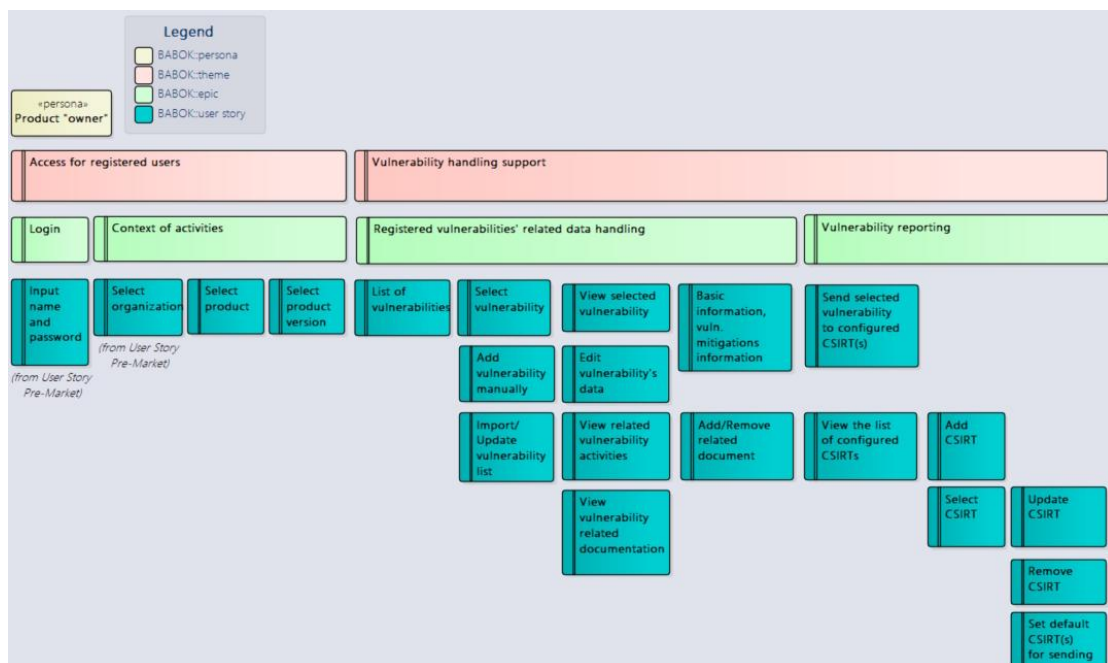


Figure 11: OSCRAT - User story - Post-market vulnerability handling activities

According to CRA requirements (Article 14(1)), the manufacturer should report actively exploited vulnerabilities to the relevant CSIRTs and ENISA. Depending on the established contact points within these institutions, the development of the OSCRAT tool should consider the possibility of notification via currently available channels. Therefore, once established by ENISA and the national authorities, the following options should be considered:

- sending a vulnerability notification via an available channel (email in the simplest case) to the authority configured in the OSCRAT tool to send such information),
 - configuring and managing the list of points (adding, removing, updating, selecting authorities) to which such information should be sent.
3. Post-market incident handling activities, like vulnerabilities, are also associated with a specific product version. The user should select the product and version (after logging in) to manage related incidents. For each version it should be possible to:
- add new incident,
 - view and edit data describing the incident (as required by Article 14(4) of the CRA), including:
 - description of the incident: initial assessment, nature of the incident, information on the impact and severity, type of threat, root cause
 - information about ongoing mitigation measures, corrective or mitigating measures that users of the product can take.
 - support the user in the incident classification (based on the definitions in Article 14(5) of the CRA),
 - add/remove files and additional documentation related to the incidents.

As with vulnerabilities, there is an obligation (according to CRA requirements, Article 14(3)), to report relevant CSIRTs and ENISA any severe incident having an impact on the security of the product. Therefore, similarly to what was described for vulnerability reporting (point 2) above), also in case of incidents, the possibility of sending incident notifications to ENISA and local authorities contact points should be considered, depending on the level of availability of such points at the time of tool implementation.

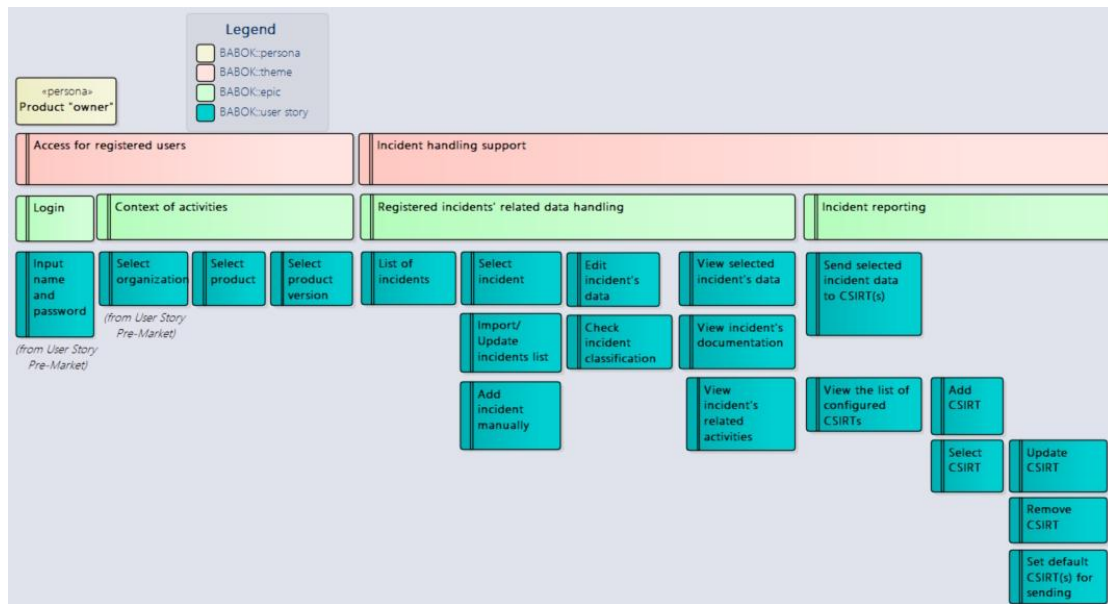


Figure 12: OSCRAT - User story - Post-market incident handling activities

5. CRA Requirements Identification (T2.2.)

5.1 CRA Essential Security Requirements

5.1.1. Purpose and Scope of work

The work involved a detailed analysis and interpretation of the Cyber Resilience Act (CRA) to identify key obligations, requirements, and references. The findings were implemented as structured checklists within the Checklist (CL) tool, which guides the self-assessment and maps each control to CRA articles, annexes, and recitals.

The detailed analysis of the CRA further supported the definition of the requirements and scope for the remaining OSCRAT tools:

- Software Bill of Materials (SBOM): component visibility and supply-chain traceability.
- Vulnerabilities (VUL): coordinated vulnerability disclosure and handling (intake, triage, remediation, reporting).
- Incidents (INC): recording, management, and reporting of security incidents affecting products with digital elements.
- Documentation (DOC): creation and verification of CRA-required technical and user documentation.

In addition to the CRA analysis, the work was guided by the principles of key international standards, including:

- ISO/IEC 27035 – Information Security Incident Management,
- ISO/IEC 29147 – Vulnerability Disclosure,
- ISO/IEC 30111 – Vulnerability Handling Processes.

These standards were used to align the interpretation of CRA obligations with widely accepted best practices in information security and incident management.

The work was carried out in close collaboration with other members of the project consortium, ensuring that all findings and assumptions were regularly reviewed, validated, and harmonized across the different tool development streams.

The activity focused on reviewing the entire content of the CRA and translating its legal and technical provisions into a clear and practical form that can be used in further implementation or compliance processes. The outcome is particularly relevant for small and medium-sized enterprises (SMEs), which often face challenges in understanding and applying complex regulatory requirements.

The final product of the work is a set of checklists compiled in the Annex 4 “**ESR_TechDoc_Requirements.xlsx**” spreadsheet, attached to this report. The

document contains a standardized set of questions, references to specific articles and recitals of the CRA, and short explanatory notes to help interpret the provisions.

This structure also served as the foundation for the Checklist component of the OSCRAT tool suite, designed to support automated compliance assessments under the CRA.

5.1.2. Methodology

The work included a comprehensive review of the CRA, covering its articles, recitals, and annexes. The goal was to map all obligations and responsibilities that apply to different types of actors involved in the life cycle of products with digital elements. The analysis was carried out in several logically connected stages.

Stage 1. Identification of requirements and development of control questions

The first stage focused on a detailed analysis of the CRA to identify all provisions introducing obligations or requirements for economic operators. Each identified requirement was reformulated into an operational statement that could be used either as a control element for compliance self-assessment (mainly in the Checklist tool) or as a functional requirement supporting the operation of other OSCRAT tools (SBOM, VUL, INC, DOC).

The analysis considered organizational, technical, and documentation-related obligations, as well as those concerning reporting and communication. Each item was linked to its source provision in the CRA, including the corresponding article, annex, and, where necessary, the recital clarifying the legislative intent.

To ensure consistency with recognized good practices, the interpretation was supported by the following international standards:

- **ISO/IEC 27035** – Information Security Incident Management
- **ISO/IEC 29147** – Vulnerability Disclosure
- **ISO/IEC 30111** – Vulnerability Handling Processes

These standards provided practical guidance for translating regulatory language into implementable requirements concerning incident response, vulnerability reporting, and lifecycle security. The outcome of this stage was a consolidated repository of CRA-derived requirements serving as a common reference for all OSCRAT tools.

Stage 2. Identification of stakeholders

The second stage focused on identifying and categorizing the main stakeholder groups covered by the CRA, along with their specific responsibilities and interrelations within the digital product ecosystem. The regulation distinguishes several roles throughout the product lifecycle, each subject to a distinct set of obligations. The following key stakeholder categories were identified and analysed:

- **Manufacturer** – responsible for ensuring the product's conformity with CRA requirements, covering secure design, production, testing, updates, and post-market activities. Main CRA reference: Article 13, 14
- **Authorized Representative** – acting on behalf of the manufacturer, maintaining communication with supervisory authorities and ensuring availability of required documentation. Main CRA reference: Article 18.
- **Importer** – responsible for placing products on the market and ensuring that each imported product is compliant, properly documented, and traceable to the manufacturer. Main CRA reference: Article 19.
- **Distributor** – ensuring that products remain compliant while being made available on the market, maintaining correct labelling, documentation, and reacting to security-related information. Main CRA reference: Article 20.
- **Open-Source Steward** – coordinating the development and distribution of open-source software, ensuring transparency, vulnerability management, and responsible disclosure in line with CRA principles. Main CRA reference: Article 24.

This classification enabled a clear mapping of roles, responsibilities, and dependencies, supporting the definition of tool functionalities tailored to each group's obligations.

Stage 3. Classification of requirements by assessment areas

In the third stage, all identified obligations were grouped into four general areas reflecting the logical structure of the CRA and supporting consistent implementation across OSCRAT tools. Each area represents a distinct aspect of compliance assessment and tool functionality but remains interconnected through shared data and processes.

1. Preliminary Area – Scope, exclusions and classification

This area focuses on the initial stage of compliance analysis, enabling organisations to determine whether their products and operations fall within the CRA's scope. It covers verification of applicability and exclusions, classification of the organisation's role, and identification of product categories and criticality levels. The Preliminary area provides the logical

entry point for compliance evaluation, ensuring that subsequent assessments in other areas are relevant and correctly scoped. Main CRA reference: Recital (5), (9), (93); Article 1, 2, 3, 13, 17, 18, 19, 20, 24 and Annex III, IV.

2. Organisational Area – Governance and Management processes

This area includes requirements related to how organisations manage cybersecurity, risk, and compliance. It focuses on internal structures and processes such as security and vulnerability management policies, incident reporting and communication procedures, monitoring and response mechanisms, and allocation of responsibilities. It ensures that the organisation can maintain compliance and supports the secure lifecycle of its products. Main CRA reference: Article 13, 14, 15, 18, 19, 20, 24; Annex I Part I and II.

3. Product Area – Design and Technical Security

The product area covers requirements that relate directly to the design, development, and technical characteristics of products with digital elements. It includes secure design principles, update and patch management, integrity verification, event logging, and data protection. This area forms the technical core of compliance, ensuring that products are built and maintained according to essential cybersecurity and resilience requirements. Main CRA reference: Article 13, 18, 19, 20, 24, Annex I Part I and II.

4. Documentation Area – Technical and User Documentation

This area concerns the creation, maintenance, and verification of documentation demonstrating compliance with CRA obligations. It covers both technical documentations describing the product, its components, and security measures, and user information ensuring that users understand security-relevant functions, updates, and responsibilities. It also links with reporting and post-market surveillance processes, ensuring traceability and readiness for authority requests. Main CRA reference: Annex II and VII.

Together, these four areas create a structured framework for analysing, mapping, and implementing CRA requirements across the OSCRAT tools. By combining legal interpretation with operational modelling, the methodology ensures that each tool addresses a complementary part of the CRA compliance process, from determining applicability and organisational readiness to verifying product security and ensuring documentation completeness.

5.1.3. Checklist structure, logic and functions

The “**ESR_TechDoc_Requirements.xlsx**” file represents the central analytical output of the CRA interpretation process. It provides a structured, traceable framework that translates the legal and technical provisions of the CRA into operational questions and compliance evaluation elements.

The structure of the file evolved through several iterative development cycles carried out in close collaboration with project partners. Initially, the checklist existed as a single list of CRA obligations; over time, it was expanded to include a dual perspective: organisational and product-based and further divided according to the specific stakeholder roles defined in the CRA. Regular coordination meetings and validation workshops with consortium members ensured alignment between the analytical work and the ongoing development of OSCRAT tools.

Overall structure of the ESR_TechDoc_Requirements.xlsx file

The final version of the file consists of multiple interconnected sheets corresponding to different stakeholder roles and CRA compliance areas. This structure enables a comprehensive assessment of compliance across the entire product lifecycle and for each actor defined in the regulation.

Main stakeholder-specific tabs include:

- Exclusion – preliminary assessment verifying whether the organisation or product falls within the scope of the CRA, considering exemptions and special cases including relevant digital product categories.
- Organisation – general organisational checklist identifying the actor type.
- ESR Organisation Evaluation and ESR Product Assessment – dedicated to Manufacturers, covering both organisational and product-related obligations.
- Importer Organisation Evaluation and Importer Product Assessment – for Importers, verifying documentation completeness, supply-chain data, and traceability.
- Distributor Organisation Evaluation and Distributor Product Assessment – for Distributors, addressing verification of markings, documentation, and incident response obligations.
- Authorized Representative Organisation Evaluation and Authorized Representative Product Assessment – for Authorized Representatives, focusing on maintenance of technical documentation and communication with authorities.
- Open-Source Stewards – checklist for entities managing or coordinating open-source software products.

Additional functional tabs include:

- INC_ISOReq – dedicated to incident management and reporting obligations (CRA, ISO/IEC 27035-1).
- Vulnerability_ISOreq – focused on vulnerability handling and disclosure (CRA, ISO/IEC 29147, ISO/IEC 30111).
- Tech doc of the product – dedicated to verification of documentation completeness based on Annex VII (Technical Documentation) and Annex II (Information and instructions to the user).

This modular architecture allows each stakeholder to be evaluated according to both their role and the technical, organisational, and documentary aspects relevant to CRA compliance.

Column Structure and Logical Consistency

All main and supplementary sheets share a unified column structure, ensuring comparability, traceability, and integration with OSCRAT. The typical column layout includes:

- Area of Requirement – defines the thematic scope (e.g., Cybersecurity in Product Lifecycle, Incident Handling, Documentation).
- Req ID – unique identifier for each requirement.
- Requirement – short description summarizing the obligation.
- CRA Reference – specific article, recital, or annex point in the CRA.
- Hint for the User – explanatory text translating legal language into operational guidance.
- Question ID – reference for traceability.
- Question – operationalized requirement formulated as a YES/NO or open-ended question.
- Answer – response field.
- Evidence / Evidence Hint – upload area and instruction on what supporting material should be provided.
- Compliance Assessment – standard four-level evaluation: Fully Compliant, Partially Compliant, Not Compliant, Not Applicable.
- Generic Task – recommended corrective or maintenance action supporting compliance (e.g., Implement secure-by-design architecture and risk-based controls).

This structure ensures that every CRA requirement can be traced from the legal provision through the corresponding question to the provided evidence and

resulting compliance status. It also allows for dynamic updates and automated aggregation of results across all tools.

Consistency across all functional areas

The same logical structure applies across all functional and thematic tabs:

- **Organisational and Product checklists** – assess internal processes, governance, risk management, and technical design requirements in accordance with Articles 13, 14,15, 18,19, 20, 24 and Annex I (Essential Cybersecurity Requirements).
- **INC_ISOreq and Vulnerability_ISOreq** – use the same structure of requirement -question - evidence - compliance status but refer to CRA Articles and ISO standards (ISO/IEC 27035, 29147, 30111), enabling consistent evaluation of incident and vulnerability management processes.
- **Tech doc of the product** – differs slightly in layout, using simplified TRUE/FALSE fields to confirm whether required elements of Annex VII and Annex II documentation and information are present (e.g., product purpose, version details, photographs, markings, internal layout).

By maintaining a consistent logic across all tabs, the **ESR_TechDoc_Requirements.xlsx** file ensures a coherent and transparent mapping between regulatory obligations and real organisational practices.

Overview of the flow (CL):

Figure in subchapter 4.1.2 CRA questionnaires flow presents the checklist flow diagram co-developed with the consortium through a series of joint design workshops. The diagram captures the end-to-end logic implemented in the Checklist (CL) tool—from scoping and role identification to requirement evaluation and corrective task management.

1. Entry and Scoping

Start with a new product or new organisation.

- **1_CL_Exclusion (incl. classification):** the objective is to determine whether the product falls within the scope of the CRA and to which product category it belongs. Binary outcome: out of scope, or in scope with an assigned category
- **2_CL_Organisation:** it identifies the market role under the CRA: manufacturer, importer, distributor, open-source steward, or authorized representative. The selected role drives activation of the corresponding questionnaires. For organisations that hold multiple roles, more than one path can be launched in parallel, with separate assessments.

Questionnaires 1 and 2 consist of single choice closed questions and are used to deterministically define scope and role.

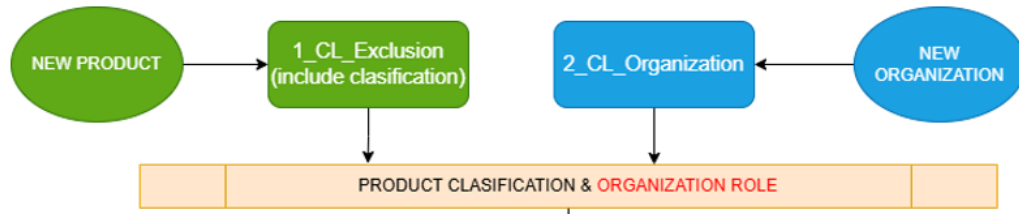


Figure 13: OSCRAT - Product classification and organization role

2. Role-Based Questionnaires

After classifying the product and defining the organisation's role, each role proceeds to its dedicated questionnaire:

- **Manufacturer:** 3a_ESR Organisation and 3b_ESR – product assessment
- **Importer:** 4a_CL_Organisation and 4b_CL_product assessment
- **Distributor:** 5a_CL_Organisation and 5b_CL_product assessment
- **Open-source stewards:** 6_CL Organisation
- **Authorized representative:** 7a_CL Organisation and 7b_CL_product assessment

Questionnaires 3–7 are organized into security areas, each containing security requirements. Requirement elements include:

- the name,
- CRA/ISO references,
- a brief interpretive hint,
- the set of questions and answers (including an upload section for evidence) - each requirement is tested with a mixed set of questions:
 - Closed: YES/NO (with Not applicable, where relevant).
 - Open: short descriptive answer.
- an Additional information field for special cases,
- a conformity assessment selected from Compliant / Partially Compliant / Not Compliant / Not Applicable, with Rationale.

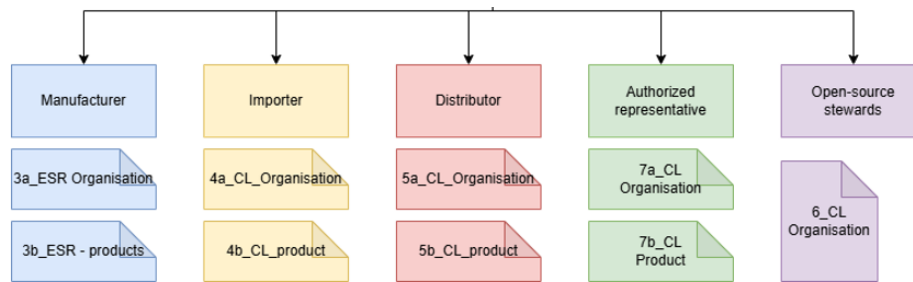


Figure 14: OSCRAT - Role-based questionnaires

3. Completeness, evaluation rules, and tasks

Certain fields are marked in the questionnaire (*) as mandatory: Mandatory question, Mandatory upload, technical file. For example, if a Mandatory upload is missing, the requirement assessment is considered incomplete.

Question statuses and their impact on the requirement assessment:

- Unanswered - 0%, blocks requirement assessment (Not evaluated).
- Answered with complete upload - 100%.
- Required upload missing - 50% (intermediate state, reflected in progress).

A requirement can be evaluated only after 100% of its questions are completed. Requirements marked Not applicable are excluded from the assessment. When full conformity is not achieved, the tool proposes creating a task:

- Not Compliant: an automatic task is proposed; once accepted, the task is added to the Task list and linked to the requirement. If not accepted, a manual task may be created instead.
- Partially Compliant: a manual task (maintenance/improvement) may be added; the task is added to the Task list and linked to the requirement.

For Compliant items, all required answers for the requirement's questions have been provided and any related tasks are closed.

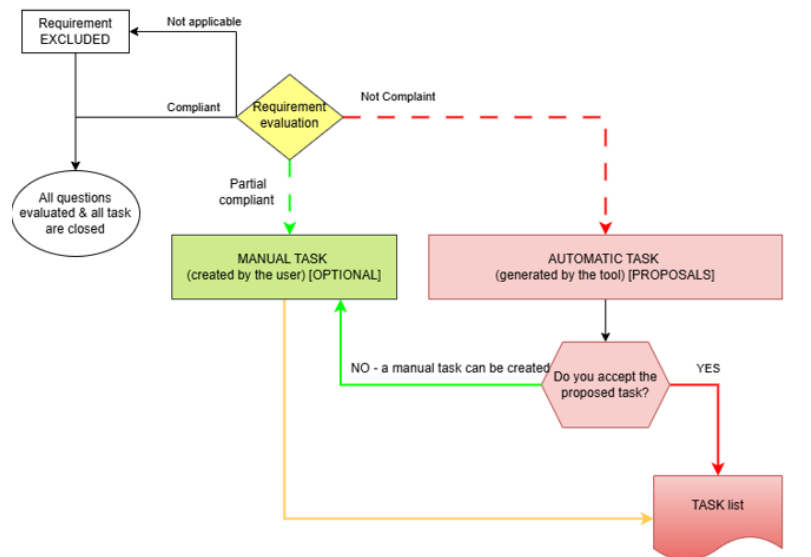


Figure 15: OSCRAT - Requirement evaluation process flow

4. Versioning (questions and assessments)

After the task is closed, the requirement is reassessed (versioning at the requirement level).

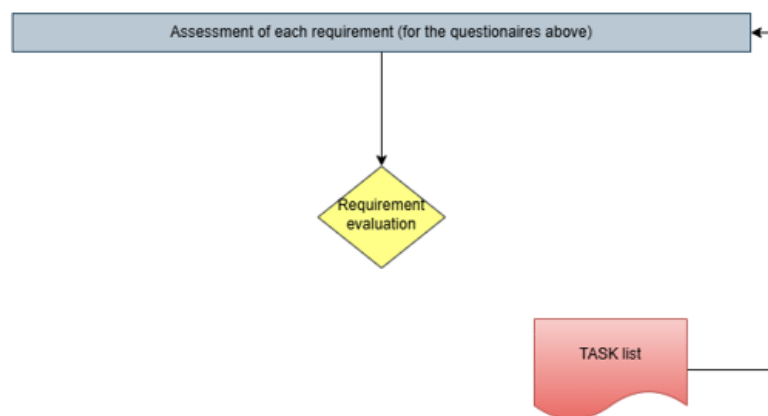


Figure 16 Requirement reassessment flow

5. Technical Documentation

An optional module based on “**3c_Tech.Doc.**” of the product. It is a practical checklist that verifies the completeness of technical documentation per product and becomes available after the full assessment is completed. It reuses answers and attachments tagged technical file from other questionnaires and checks for the required elements (e.g., product purpose, versioning, markings, photographs, internal layout).

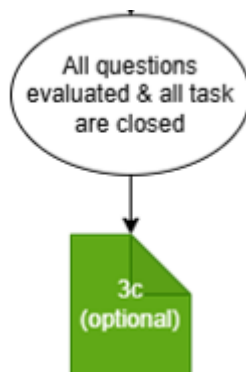


Figure 17: OSCRAT - Entry to optional module 3c (Technical Documentation)

6. Dashboard and Reporting

The Dashboard/Status panel is conceived as a consolidated view of progress and conformity across all requirements. For each requirement, it is proposed to display two independent dimensions:

- Requirement Status (Evaluated / Not evaluated), driven solely by answer completeness and mandatory uploads, and
- Conformity Status (Compliant / Partially Compliant / Not Compliant / Not Applicable), assigned after the formal evaluation. This separation distinguishes items still being completed from those already substantively assessed.

The visual layer proposed for the dashboard comprises the following core metrics and charts:

- an Evaluated vs. Not evaluated chart to indicate assessment maturity,
- a conformity breakdown chart (Compliant / Partially Compliant / Not Compliant / Not Applicable) to support remediation prioritisation,
- a task status chart (e.g., proposed / in progress / closed) to show workload and closure pace,
- a global progress bar computed as the arithmetic average across all requirements (Evaluated = 100%; Not evaluated contributes its current question-level completeness).

It is also proposed to include a PDF export with a full audit trail (answers, assessment rationales, evidence, and references to the applicable provisions).

During the work, a Questionnaire User Guide was prepared and is attached to this document in Annex 5. Its purpose is to support users in consistently using the CL questionnaires from launching the appropriate path to completing the assessment and closing tasks.

5.2. CRA-specific requirements for the tools

CRA-specific requirements were identified and applicable articles to the OSCRAT tools were marked. The table in Annex 14 shows the tools' capabilities to be implemented to cover identified CRA-specific requirements.

Articles of the CRA that did not directly impact the planned functionality of the OSCRAT tool (e.g., those concerning obligations imposed on Member States, the Commission, authorities, and ENISA) were not considered and are marked as not applicable ("N/A") in the table in the annex.

The main modules and capabilities of the OSCRAT tool were derived from the CRA requirements of the act. These were then translated into task specifications, which described the detailed functions and responses for the tool. Based on these task specifications, the OSCRAT tool functions were implemented within WP3.

Table 9 below presents the concise version of the CRA-specific requirements analysis presented in Annex 14.

The following table 9 presents the mapping between the implemented functionalities and the corresponding requirements of the Cyber Resilience Act (CRA). For each functionality, the CRA requirements are indicated, providing a clear view of how specific modules of the OSCRAT platform support regulatory compliance.

Issue, Subject	Capabilities and Functionalities	Details
Applicability Check (CL)	Accessing the Applicability Check (Button on landing page)	Article 2
	Questionnaire Logic (based on CRA – XLS Sheet CL_Exclusion)	Annex I, Annex II
	Outcome Path (product is eligible or not, eligible product classification)	Articles 7 and 8, Annex III Annex IV
CRA Compliance Assessment for a Product Version (CL)	Automatically initiated CRA compliance self-assessment, when a new product version is created.	Article 13(10)(11), Annex VII (1)(b)

	Self-Assessment supports a structured self-evaluation process aligned with CRA requirements	Articles from 13 to 16 and from 18 to 24, Article 12 (high-risk AI systems inclusion) Annex VIII part 1 Article 32 (1a)
	Hierarchical level of questionnaire: Area or requirements / Requirement / Question	Article 6, 32 Articles from 13 to 16 and from 18 to 24, Annex I Annex II Annex V Annex VI Annex VII
	Organization role-specific questionnaires references	Articles from 13 to 16 and from 18 to 24
Product Assessment Dashboard, Visualization, Export (CL)	A dynamic dashboard summarizing compliance progress for each product assessment	Article 13 Article 28 Annex V Annex VI
	Dashboard includes assessment status tables, product assessment charts, progress bar/indicators	Article 13 Articles 18 to 21 Article 24 Article 28 Annex V Annex VI
	Export Conformity Assessment Report (pdf document)	Article 28 Annex V Annex VI

Administration of an Organization/Product Assessment Questionnaire Template (CL)	Compliance self-assessment questionnaires did not hardcode	Annex VIII part 1 Article 32 (1a)
	Define a questionnaire template in a structured (JSON) format (based on the CRA Requirements Spreadsheet)	Articles from 13 to 16 and from 18 to 24, Annex I Annex II
	Modify questionnaire template (template can be updated over time via an import mechanism)	Article 27 Annex VIII
	Mechanism to upload/import new questionnaires	Article 27 Annex VIII
CRA Process Assessment for an Organization (CL)	Automatically initiated CRA organizational process self-assessment, when a new organization is created.	Annex VIII part 1 Article 32 (1a)
	Hierarchical level of questionnaire: Area or requirements / Requirement / Question	Article 6, 32 Articles from 13 to 16 and from 18 to 24, Article 12 (high-risk AI systems inclusion) Annex I Annex II Annex V Annex VI Annex VII
	Organization Role-Specific Questionnaires references	Articles from 13 to 16 and from 18 to 24
Organization Assessment Dashboard, Visualization, Export (CL)	A dynamic dashboard summarizing compliance progress for organizational assessment	Article 13 Article 28 Annex V Annex VI
	Dashboard includes assessment status tables, product assessment charts, progress bar/indicators	Article 13 Articles 18 to 21 Article 24 Article 28 Annex V Annex VI

	Export Conformity Assessment Report (pdf document)	Article 28 Annex V Annex VI
Automatic Task Generation (CL)	Automatic task creation based on requirement-level self-assessment results (Not Compliant / Partially Compliant / Compliant / Not Applicable)	Annex VIII part 1 Article 32 (1a)
	Tasks include predefined fields and product version association	Annex VIII part 1 Article 32 (1a)
	Additional logic for marking assessments as completed when all requirements are Compliant or Not Applicable	Annex VIII part 1 Article 32 (1a)
SBOM Management (SBOM)	Display a list of all SBOMs associated with the selected product version	Annex I Part II (1) Annex VII
	Generate SBOMs directly within the system	Annex I Part II (1) Annex VII
	Import externally generated SBOMs	Annex I Part II (1)
	Download existing SBOMs	Annex I Part II (1) Annex VII
	Scan SBOMs for vulnerabilities, resulting in a generated Vulnerability Report	Annex I Part II (1)
	Review the Vulnerability Report and selectively add identified vulnerabilities to the Vulnerability Module	Annex I Part II (1) Annex VII
	Configuration of the project path and access data to generate SBOM	Annex I Part II (1)
Add New Vulnerability (VUL)	Create a new vulnerability record	Annex I Part II Article 13, 14
	Associate vulnerability with a specific product and version	Annex I Part II Article 13, 14
	Input key details such as name, status, severity, date of discovery, etc.	Annex I Part II Article 13, 14

	Attach supporting documents related to vulnerability	Annex I Part II Article 13, 14
Edit Vulnerability (VUL)	Modify existing vulnerability records	Annex I Part II Article 13, 14
	View read-only fields and update editable information	Annex I Part II Article 13, 14
	Attach or manage related documents	Annex I Part II Article 13, 14
Vulnerability Details Page (VUL)	View complete vulnerability details	Annex I Part II Article 13, 14, 15, 16
	Access an attachment section showing all associated files	Annex I Part II Annex VII Article 13, 14, 15
Add New Incident (INC)	Create a new incident record	Article 13, 14
	Associate the incident with a specific product and version	Article 13, 14
	Input details such as: ID, status, classification, attack type, asset details, reporter, etc.	Article 13, 14
	Attach supporting documents related to the incident	Article 13, 14
Edit Incident (INC)	Modify existing incident records	Article 13, 14
	View read-only fields and update editable information	Article 13, 14
	Attach or manage related documents	Article 13, 14
Incident Details Page (INC)	View complete incident details	Article 13, 14, 15, 16

	Access an attachment section showing all associated files	Article 13, 14, 15 Annex VII
General description (DOC)	Open text sections to describe products, versions	Annex VII Article 13, 14, 23, 31
	Adding images, uploading related documents	Annex VII Article 29, 30, 31, 53
	Support period determination of the product version	Annex VII Article 31 Article 13
	Data saved per product version and automatically included in the published report	Annex VII Articles from 13 to 16, Article 31
Specification, description of the design & development processes of the product (DOC)	Open text sections, description fields to allow users to describe how design principles ensure CRA compliance	Annex VII Article 13 Article 31
	Adding images, related documents (diagrams, files)	Annex VI Article 13 Article 31
Vulnerability handling process (DOC)	Documents' templates for vulnerability handling process available for the users	Article 13, 14 Annex I Part II
	Users can adjust the pre-filled (templates) content	Article 13, 14 Annex I Part II
	SBOM files management (generating, uploading, downloading)	Annex I Part II Annex VII
	Reports generation from the vulnerability scan	Article 13, 14 Annex I Part II Annex VII
	Possibility to publish vulnerability disclosure policy, selected product documentation	Annex I Part II Annex VII
Production & monitoring processes documentation (DOC)	Questionnaires for the self-assessment of the organization documentation elements and content (to check missing documents)	Article 13 Annex II Annex V Annex VI Annex VII Article 28

	Uploading evidence documents for the self-assessment activities, documentation related to the processes production within the organization, monitoring processes related to the production activities	Article 13 Annex II Annex V Annex VI Annex VII Article 28
	Reports for the organization's compliance self-assessment	Annex V Annex VI Annex VII Article 28
Cybersecurity Risk Assessment (DOC)	Risk assessment template available, including information how the essential cybersecurity requirements (CRA Annex I) are applicable - (users can modify predefined sections)	Article 13 Annex I Annex VII
Conformity Verification (DOC)	For the product with self-assessment - support in preparation of Declaration of Conformity (DoC) document for the product - document template available	Article 13, 28, 32 Annex V Annex VI
	For the product assessed by 3rd party – upload of the assessment report and signed DoC	Article 13, 28, 32 Annex V Annex VI
	DoC available in the tool, can be downloaded	Article 13, 28, 32 Annex V Annex VI
	Evidence of conformity files available in the OSC RAT tool (SBOM files, vulnerability scan reports, self-assessment reports)	Article 13, 28, 32 Annex V Annex VI
General functionalities of OSC RAT tool	User/Organisation management	Article 6, 13, 63
	Product / Product version management (Add / Edit / View details)	Article 6, 13, 53 Annex VII

Table 9: OSC RAT: Capabilities and Functionalities of the OSC RAT Tools mapped to CRA Requirements

Findings

The conclusion of the analysis presented in the table above indicate that the OSC RAT tools provide consistent and comprehensive support for manufacturers and other actors involved in the lifecycle of products with digital elements in maintaining compliance with CRA requirements and obligations. This covers both product-related obligations and the requirements that apply to organisational processes and procedures.

6. User Needs Analysis (T2.3.)

To identify the exact expectations and needs of users, a survey was conducted during the project. Its purpose was to learn about current habits and practices. It was also designed to identify real needs and expectations in relation to specific issues addressed in the project: product development, incidents, documentation management, and source code vulnerability. The detailed list of questions is presented in subsection 4.3. This section presents the results and conclusions drawn from the responses obtained.

The survey questions were viewed by 70 different people, probably working for 70 different organizations. However, only 24 people answered all the survey questions. The rest were answered only partially or stopped after viewing the first question. Due to the high degree of uncertainty as to where the survey responses were abandoned, it was decided to analyse only those records that indicate that all questions were answered. Therefore, this analysis focuses on discussing only 24 results.

Among these 24 responses, only 5 people indicated the type of organization they worked for: Manufacturer/Importer/Distributor/Open-source software steward - providing support, not a manufacturer - Article 3 (14) of CRA. Two of these five indicated that they were hardware manufacturers, one indicated that he was a software distributor, and the last two indicated that they were open-source software stewards, with one indicating software directly and the other indicating “nothing”. Of the remaining 19 of the 24 complete responses mentioned at the beginning, all that is known is that 85% of them relate to software. However, it is not known to what extent and in what capacity. Absolutely nothing is known about the remaining 15%.

6.1 Analysis according to main categories of questions

6.1.1. Stakeholder's characteristic

At the beginning, the respondents were asked about the profile of their business activity:

a. **Survey questions related to stakeholder's characteristic:**

Which stakeholders' group do you belong to and what type of products do you offer?	
Answer	Number of Selections
Hardware Product	2
Software Product	19
Manufacturer	2
Importer	0
Distributor	1
Open-Source software Steward – Providing support, not a manufacturer- Article 3 (14) of CRA	2
Other (Cybersecurity services, CAB, Services, Telco Operator, R&D Company)	1 per each organization type

Table 10: OSCRAT - Answers to the question "Which stakeholders' group do you belong to and what type of products do you offer?"

b. **Summary:**

As many as 79% of respondents offer software products with focus on software requirements, including SBOM, vulnerability management, incident management, and documentation.

Only a few individuals declared their role as open-source producer, distributor, or steward. This may indicate that most respondents are service providers or integrators, or that they do not identify with these categories despite their potential obligation under the CRA.

Indications such as cybersecurity services, CAB, telco operator, or R&D company suggest that some participants play supporting or expert roles, rather than strictly product-related ones. It's worth considering their perspective in further activities—for example, tool validation, training, and consulting.

6.1.2. Inventory/ labelling (Software Bill of Materials (SBOM))

a. *Survey questions related to inventory, labelling and Software Bill of Materials (SBOM):*

Answers to the question: “How are you currently handling the labelling (tagging), identifying products, components, and libraries processes in your organization?” are presented in the Table 11.

How are you currently handling the labelling (tagging), identifying products, components, and libraries processes in your organization?	
Answer	Number of Selections
We are using a tool / automated process for this (input tools name or details in comments)	2
We are doing it on an informal basis, with no records kept	1
We are doing it using manual processes and written / informal records	9
We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC or other relevant standards, SBOM files, etc., please input details in comment)	5
We are not doing it	7

Table 11: OSCRAT - Answers to the question "How are you currently handling the labelling (tagging), identifying products, components, and libraries processes in your organization?"

When it comes to how products, components, and libraries are labelled in an organization, respondents said that the most common method (9 responses) is manual processes and informal records, which might mean there aren't any standardized tools or procedures in the organization.

Formal processes in line with best practices (e.g., ISO/IEC, SBOM) are used by 5 respondents, which is a sign that some of the surveyed organizations are striving for professionalization.

Automated tools are used by only two organizations, which may suggest a low level of implementation of modern solutions or process automation.

The **lack of any formalization** (one response) is rare, but still present.

However, as many as 7 organizations do not carry out the component marking process at all, which may indicate a significant gap, especially in the context of CRA requirements. In addition, respondents were asked to comment on the **use of standards or tools** to support the process of identifying and monitoring software components.

Some respondents indicated the following solutions:

- **Syft,**
- **ISO 27001 procedure, json/xml files in Github,**
- **Our organization follows formal SBOM practices aligned with ISO/IEC 5230 (OpenChain standard) and ISO/IEC 27001 controls for asset and configuration management.**

Attention should be paid to the comprehensive approach to formal SBOM analysis in conjunction with ISO/IEC 5230 and ISO/IEC 27001 standards, which ensure the licensing compliance of open-source software with the information security management system.

In the next step, respondents were asked about the use of specific SBOM standards in their organization: **"If you use solutions that support SBOM, what types of standards do you use or would like to use?"** The respondents' answers are presented in the Table 12.

If you use solutions that support SBOM, what types of standards do you use or would like to use?	
Answer	Number of Selections
None (we have no solutions to support SBOM)	18
None (we have no solutions to support SBOM)	5
CycloneDX – OWASP Foundation ECMA-424 standard	3
SWID (Software Identification Tagging) – ISO/IEC 19770-2	2
Other - json files in Github	1

Table 12: OSCRAT - Answers to the question "If you use solutions that support SBOM, what types of standards do you use or would like to use?"

As many as **18 out of 24 respondents (75%) declared that they do not use any SBOM support solutions**. This indicates a large space for education and implementation of such tools, as well as the potential risk associated with the lack of transparency of the software components they create. The most frequently mentioned standard was SPDX (5 mentions), supported by the Linux Foundation and recognized as ISO/IEC 5962. The popularity of this standard may be due to its widespread support in open-source tools.

Developed by OWASP and compliant with ECMA-424, CycloneDX (3 mentions) is often chosen in DevSecOps environments and for the automation of the software development and delivery process.

SWID (2 mentions) but compliant with ISO/IEC 19770-2, mainly used in corporate and government environments.

The use of Json files in GitHub (1 mention) illustrates a proprietary, non-standard approach to documenting components or a lack of knowledge of standards or tools to support this process. In addition, the Netrise tool was mentioned.

Do You use any SBOM preparing / analysis of SBOM supporting tool?	
Answer	Number of Selections
OWASP dependency-check	7
cve-bin-tool	3
Grype	2
Trivy	2
None / No	15

Table 13: OSCRAT - Answers to the question "Do You use any SBOM preparing / analysis of SBOM supporting tool?"

15 out of 24 respondents (over 60%) do not use any SBOM tools. This confirms earlier observations about the low level of implementation of such solutions in organizations.

The most frequently used tool by respondents is: OWASP Dependency-Check (7 mentions). It is a popular tool for detecting known vulnerabilities in project dependencies.

Other tools used by respondents include: cve-bin-tool (3), gype (2), trivy (2) for vulnerability analysis and offering SBOM generation or utilization.

One respondent also mentioned Netrise, a Software Bill of Materials (SBOM) management platform designed for software supply chain security, especially in the context of XIoT (Extended Internet of Things) devices, firmware, and embedded systems.

b. **Summary:**

Based on the survey results, several gaps or deficiencies in respondents' awareness of SBOM (Software Bill of Materials) handling can be identified:

- Low level of SBOM implementation in organizations - 75% of respondents do not use any SBOM support solutions, and over 60% do not use any tools for its preparation or analysis. This may indicate a lack of awareness that SBOM is not only documentation, but also an element of risk, security, and compliance management.
- Limited knowledge of standards – only a few respondents indicated specific standards such as SPDX, CycloneDX, or SWID. On the other hand, some respondents use their own formats (e.g., JSON in GitHub), which can hinder interoperability and automation. This points to the need for education on existing, recognized SBOM standards and their advantages (e.g., CRA and ISO compliance, tool support).
- A small number of tools in use – the most frequently mentioned tool is OWASP Dependency-Check, which does not generate a complete SBOM, but only analyses dependencies. Tools such as Syft, Gype, Trivy, and cve-bin-tool are known only to a few. Such a small number of tools in use may suggest that respondents may not be familiar with tools dedicated to generating and analysing SBOMs or may not know how to integrate them into their own software creation and delivery automation (CI/CD) processes.
- Lack of connection between SBOM and security and compliance – only a few respondents indicated a connection between SBOM and ISO/IEC 27001 and 5230 standards, while the majority do not perceive SBOM as part of their information security strategy. It is therefore necessary to show how SBOM supports regulatory compliance (e.g., CRA, NIS2, ISO/IEC), vulnerability management, and supply chain transparency.

Based on the analysis of the survey results and the requirements of the Cyber Resilience Act (CRA), it can be concluded that the level of preparedness of respondents to meet the CRA requirements for SBOM handling is currently low, although approximately 20% of them use formal processes in line with best practices (e.g., ISO/IEC).

The role of the OSCRAT project may therefore be to support the education (workshops) of SMEs in perceiving SBOM as an element of software management and security, as well as to provide tools for SBOM handling.

6.1.3. Risk management

a. *Survey questions related to risk management:*

Among the 24 responses to the question “How are you currently handling the Risk Management processes in your organization?”, the following answers were obtained:

How are you currently handling the Risk Management processes in your organization?		
Answer	Number of Selections	Comment
We are not doing it	3	
We are doing it on an informal basis, with no records kept	3	
We are doing it using manual processes and written / informal records	7	ISO 27005 EBIOS ISO 31000 ISO/IEC 27001
We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27005, 31000, etc., please list standards in comments)	11	
We are using a tool / automated process for this (please input tool name or description in comments)	1	Unicis Platform

Table 14: OSCRAT - Answers to the question "How are you currently handling the Risk Management processes in your organization?"

The summary shows that almost half of the respondents comply with one of the risk management standards. At the same time, only six companies indicated

which standard they comply with. In addition, some companies comply with more than one standard.

A significant proportion of respondents indicated that they manage risk, but their approach is not consistent with any of the proposed standards. Despite the noteworthy decision to manage risk, its scope is unknown, so it seems reasonable to assume that it is done to a limited extent. In addition, one organization indicated that it uses a specific platform for risk management but did not indicate the compliance of this platform with any of the risk management standards.

Among companies complied with standard, most commonly are presented in the Table 15.

Most Common Used Standards	
Answer	Number of Selections
ISO/IEC 27005	4
ISO/IEC 27001	3
ISO/IEC 31000	1
EBIOS	1
Security Profile	1

Table 15: OSCRAT - Most common standards

Of all respondents, only six companies reported using a risk management tool, and only four of those specified which one. It is worth noting that such a tool was also indicated by a company that considered itself non-compliant with any of the proposed standards (even though the tool itself is declared by the manufacturer as based on ISO/IEC 27001 and ISO/IEC 27005:2022). Among the other responses, the OneTrust platform and a set of templates compliant with ISO/IEC 27001 and ISO/IEC 31000 were mentioned twice.

Do You use any governance, risk management, and compliance (GRC) supporting tools?		
Answer	Number of Selections	Comment
Yes	6	Unicis Platform ISO/IEC 27001 ISO/IEC 31000 RSA Archer ServiceNow GRC ISMS.online OpenGRC OneTrust
No	18	

Table 16: OSC RAT - Answers to the question "Do You use any governance, risk management, and compliance (GRC) supporting tools?"

It is also worth noting that compliance with any standard was declared by companies that are software manufacturers (including open-source software stewards) and one company that is a distributor.

b. Summary:

Please note! The authors are aware that the number of responses obtained is insufficient to draw any valid conclusions — the data recorded in the survey responses is not representative. However, based on the responses obtained, several basic facts can be established.

Risk management is not an unfamiliar topic. Companies approach it in a comparable manner, both in an organized and standard-compliant way, as well as managing risk using their own methods and developed procedures. However, the responses obtained do not allow us to determine where there were gaps or discrepancies between declarations and practice.

Among hardware product manufacturers, exactly half of the organizations indicate that they do not manage risk or that they manage it informally, internally.

Among software manufacturers, more than half of the respondents indicated that they manage risk in accordance with one of the standards. At the same time, 10% of companies indicated that they do not manage risk in any way. The

remainder (~40%) declared that they manage risk, but in a manual and informal manner.

Among distributors, only one company completed the survey, which complies with one of the standards and uses the OneTrust platform.

Among companies – open-source software stewards – two companies completed the survey. One of them declares that it complies with one of the standards and uses the OneTrust platform. The other admits that it uses specific software in which risk management is based on two standards: ISO/IEC 27001 and ISO/IEC 31000. However, it does not indicate compliance with either of these standards.

6.1.4. Vulnerability Management

a. Survey questions related to vulnerabilities:

How are you currently handling the Vulnerability management processes in your organization?		
Answer	Number of Selections	Comment
We are not doing it	4	
We are doing it on an informal basis, with no records kept	3	
We are doing it using manual processes and written / informal records	7	Wazuh
We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 30111, 29147, etc.)	5	C5, ISO27001
We are using a tool / automated process for this (please input tool name or description in comments)	7	Netrise, Qualys, Prisma Cloud, OpenVAST

Table 17: OSCRAT - Answers to the question "How are you currently handling the Vulnerability management processes in your organization?"

During the survey, the question “How are you currently handling the Vulnerability management processes in your organization?” was asked, to which

24 respondents answered. The responses indicate that vulnerabilities are handled in most companies. Only four companies do not manage vulnerabilities in any way, and three do it informally. Seven companies use vulnerability management tools, of which four indicated the following: Netrise, Qualys, Prisma Cloud, and OpenVAST. The remaining three companies did not indicate the name of the tool in their responses.

The responses show considerable variation – some organizations do not conduct formal activities or operate in an undocumented manner, while others use manual procedures. However, half participants have implemented process automation tools (e.g., Netrise, Qualys, OpenVAST, Prisma Cloud) and are referred to ISO standards, which indicates commitment to vulnerability management.

Is vulnerability classification implemented (how)?		
Answer	Number of Selections	Comment
Own (internal) classification	7	
Compliant with standard / guideline / regulation (e.g. CVSS, please list them in comments)	10	CVSS score, Tenable VPR
No	7	

Table 18: OSCRAT - Answers to the question "Is vulnerability classification implemented (how)?"

Standard classification systems such as CVSS are most used, sometimes supplemented with additional risk indicators. However, some organizations use their own internal assessment methods, and about one-third have not implemented a systematic vulnerability classification system at all.

Notification Channels of detected / registered / fixed vulnerabilities?	
Answer	Number of Selections
None	3
E-mail	18
Dashboard / Internal System	11

Public Advisory / Website	4
Automated Alerts (e.g., SIEM, Monitoring tools)	10
Other	0

Table 19: OSCRAT - Answers to the question "Notification Channels of detected / registered / fixed vulnerabilities?"

When asked about "**Notification Channels of detected/registered/fixed vulnerabilities?**", most respondents indicated that they have a channel through which vulnerabilities are reported. These include emails, internal company tools, websites, and SIEM tools. Only three respondents do not have a channel through which they collect information about vulnerabilities. Two of these companies indicated in an earlier statement that they do not handle vulnerabilities at all. One company handles vulnerabilities informally.

The most popular notification channel is email, but many companies also use dashboards and automated alerts (e.g., from SIEM systems). Public announcements are used much less frequently, which shows that organizations focus mainly on internal communication.

Information Format of detected / registered / fixed vulnerabilities?	
Answer	Number of Selections
Internal (Proprietary Format)	10
Standard-Compliant (e.g., CVE, ISO, NIST, EUVD) if so, which provide in comments)	10
Other (if so, which provide in comments)	0
None/No	5

Table 20: OSCRAT - Answers to the question "Information Format of detected / registered / fixed vulnerabilities?"

The results show a balance between the use of internal formats and standard formats (e.g., CVE, NIST, ISO). However, several organizations admitted that they do not use any established formats, which may hinder collaboration between teams and process automation.

Do You use any vulnerability disclosure / handling supporting tools?	
Answer	Number of Selections
Nmap	8
Nessus	3
ZAP	2
BurpSuite	5
None	12
Other (Wazuh, Netrise, Qualys, OpenVAST, GitHub Security Advisories, Wireshark)	1 per each tool

Table 21: OSCRAT - Answers to the question "Do You use any vulnerability disclosure / handling supporting tools?"

In one of the answers to the "**How are you currently handling the Vulnerability management processes in your organization?**" question, seven respondents declared that they use tools during the vulnerability handling process. The next question in the survey was designed to clarify the tools that are used to discover vulnerabilities. The question was: "Do you use any vulnerability disclosure/handling supporting tools?" The analysis of the responses shows that 13 out of 24 respondents use some kind of tool that helps with vulnerability management.

The most used tools are basic scanning tools such as **Nmap, Nessus, BurpSuite, and ZAP**. Some organizations also use more advanced solutions (e.g., OpenVAST, Qualys, GitHub Security Advisories). It is very common to organizations, that there is more than one tool used for vulnerability disclosure. It may indicate rather high knowledge. However, a large group still does not use any tools, which shows the varying levels of expertise among participants.

b. Summary:

When it comes to vulnerabilities, most respondents indicated that managing them is at least important (~96%). At the same time, the level of vulnerability management in accordance with standards leaves much to be desired. **Only ~20% of respondents indicated that they comply with standards**, with one case where the standards did not directly relate to vulnerabilities. When asked

about the tools used for vulnerability management, 29% indicated that they had such tools in place, but only 16% indicated specific tools. Only two of those specifically mentioned were based on vulnerability management standards.

Vulnerability classification is carried out using generally accepted standards in ~41% of cases, most often using CVSS. The remaining companies either do not classify vulnerabilities or have internal arrangements.

Notifications of detected vulnerabilities are most often sent to companies by email (75%), although organizations have various parallel notification channels in place. In 41% of cases, they also use automated tools and instant notifications. Also, in ~41% of cases, the format and description of vulnerability comply with one of the standards, with CVE being the most indicated.

In the case of vulnerability disclosure tools, exactly half indicated that they use some kind of tool. The most common is Nmap, with companies using more than one solution.

6.1.5. Incident Management

a. Survey questions related to incidents:

How are you currently handling the incident management processes in your organization?		
Answer	Number of Selections	Comment
We are not doing it	5	
We are doing it on an informal basis, with no records kept	1	
We are doing it using manual processes and written / informal records	6	
We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27035, etc., please list standards or practices in comments)	9	ISO27001, C5, Jira
We are using a tool / automated process for this (please provide tool name or description in comments)	3	ISO27001, C5, Jira

Table 22: OSCRAT - Answers to the question "How are you currently handling the incident management processes in your organization?"

All 24 respondents answered the question “How are you currently handling the incident management processes in your organization?” As with vulnerability, most respondents handle incidents in some way. Five organizations do not take any action, and only one does so, but informally. Others, half, apply formal processes compliant with ISO27001, C5, or ISO/IEC 27035. Some companies have implemented tools and SOC centres.

Is incident classification implemented (how)?		
Answer	Number of Selections	Comment
Own (internal) classification	13	Based on C5
Compliant with standard / guideline / regulation (e.g. NIS2 directive) if so, which provide in comment	5	Common Criteria, FIDO, etc.
No	6	
Other if so, please provide details in comment	0	

Table 23: OSCRAT - Answers to the question "Is incident classification implemented (how)?"

When asked about how they classify incidents, most respondents said they had their own classification system—13 respondents answered this way. One of these responses pointed to their own implementation based on the C5 (Cloud Computing Compliance Criteria Catalogue) standard. Five of the responses indicated that incidents were handled in accordance with one of the standards or guidelines. Respondents referred to the Common Criteria and FIDO standards, as well as criteria based on ISO/IEC 27035, Article 23 of NIS2, and Articles 17–20 of the DORA Regulation. Six respondents stated in the survey that they do not classify incidents in any way.

Who is notified of detected incidents carried out?	
Answer	Number of Selections
None	3
Internal Security Team	21
Affected Customers	11
Regulatory Authorities	9
Public Disclosure	2
Other	0

Table 24 :OSCRAT - Answers to the question "Who is notified of detected incidents carried out?"

Most incidents are reported to internal security teams. In many cases, customers and regulatory authorities are also notified, although public disclosures are very rare.

Notification Channels of detected incidents carried out?		
Answer	Number of Selections	Comment
None	2	
E-mail	21	
Dashboard / Internal System	11	
Public Advisory / Website	1	
Automated Alerts (e.g., SIEM, Monitoring tools)	10	

Other		Slack or MS Teams notifications via webhook integration from detection tools and ticketing systems. In high-impact cases, phone/SMS alerts are triggered for escalation.

Table 25: OSCRAT - Answers to the question "Notification Channels of detected incidents carried out?"

Email remains the dominant channel, supported by dashboards and alerts from monitoring systems. Some organizations also use notifications via Slack/MS Teams, and in critical situations, channels are activated via telephone or SMS.

Do You use any incident detection / analysis, reporting supporting tools?	
Answer	Number of Selections
No	15
Wazuh	5
Snort	2
Suricata	3
Other (Azure, ThreatSpike, Elastic SIEM, OpenVAST)	1 per each tool

Table 26: OSCRAT - Answers to the question "Do You use any incident detection / analysis, reporting supporting tools?"

When asked, "**Do you use any incident detection/analysis, reporting supporting tools?**", most respondents said that they do not use any incident management tools. This was the case in 15 out of 24 responses. Most other respondents opted for the Wazuh tool. Three respondents declared that they used several tools, selecting multiple answers. Four respondents mentioned tools that were not listed in the survey: Azure, ThreatSpike, Elastic SIEM, and OpenVAST.

b. Summary:

For **incidents**, most respondents indicated that managing them is at least important (~96%). At the same time, only half of the organizations declare that they manage incidents in accordance with standards or use appropriate tools for this purpose. Only one organization indicated that it manages incidents in accordance with the ISO 27035 standard. The other half either does not do so at all or does so using internal methods.

Incidents are classified using generally accepted standards in 20% of cases, with only one organization indicating NIS2 and ISO 27035. In ~55% of cases, classification is based on internal arrangements and only in one case in accordance with C5. The remaining companies do not classify incidents.

Incident notifications to companies are most often sent by email (~87%), although organizations have various parallel notification channels in place. In 41% of cases, they also use automated tools and instant notifications.

Incident notifications are sent to both consumers (41%) and supervisory authorities and the public (also 41% in total). In these cases, companies notify both parties. However, the remaining companies (almost 60%) do not notify any external partners about incidents. Approximately 87% of companies notify internal teams about incidents.

Only ~38% of companies use incident detection tools. The most popular tool is Wazuh, with companies using more than one solution.

The results indicate that, although almost everyone considers incident management important, few organizations indicate they have implemented solutions compliant with recognized standards. It is difficult to pinpoint the cause of this situation. However, it can be assumed that high awareness should translate into a willingness to implement appropriate solutions in organizations in the future.

6.1.6. Security Management, Documentation, Workflow

a. Survey questions related to documentation management:

Have you implemented any documentation management or security management processes in your organization?		
Answer	Number of Selections	Comment
We are using a tool / automated process for this (please provide names or details in comment)	1	Unicis Platform
We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27001 or other relevant standards, etc., please provide names or details in comment)	13	ISO/IEC 17025 ISO/IEC 27001 ISO 9001
We are doing it using manual processes and written / informal records	2	
No	4	
We are doing it on an informal basis, with no records kept	4	

Table 27: OSCRAT - Answers to the question "Have you implemented any documentation management or security management processes in your organization?"

Among the responses collected through the survey, **most organizations have implemented a system for managing documentation.**

Among those based on specific standards, ~70% indicated ISO/IEC 27001. ISO 9001 and ISO 17025 were also indicated, but only once.

Overall, **~54% of companies indicated that they have implemented a document management system** based on a specific standard, and another ~30% indicated that they have a system in place, but without indicating compliance with any standard. Only 16% do not have such a system in place.

In the case of source code or document exchange and collaboration tools, the most prevalent systems are those that allow version management, individual access, and support resource sharing and group work, both on documentation and source code. In addition, these companies most often use more than one system simultaneously. It is also worth noting that approximately 50% of

companies use cloud solutions provided globally by large technology companies. The company profile is irrelevant when using this type of solution.

It is also worth noting that only ~8% of companies do not have any documentation management or security management process.

The most used solutions for document and source code management are:

Do you use any tools for documents / source code / data repository tools (internal for developers, managers and public for customers?)	
Answer	Number of Selections
GIT	12
SVN	3
One Drive	6
Google Drive	9
Windows shared folders/Samba	3
SharePoint	3
iCloud	1
Confluence	2
ISO/ISMS	1
Jira	2
None/No	4

Table 28: OSCRAT - Answers to the question "Do you use any tools for documents / source code / data repository tools (internal for developers, managers and public for customers?"

At the same time, **companies with a central source code repository** in place most often use a system that allows them to automatically compile and build the solutions they are developing. Among those mentioned are:

Do you use any building systems / compilations tools?	
Answer	Number of Selections
GitLab CI/CD	12
Ansible	4
Jenkins	5
Maven	3
GitHub	1
None/No	9

Table 29: OSCRAT - Answers to the question "Do you use any building systems / compilations tools?"

The most common system is a solution based on **GitLab**.

b. Summary

In the case of **documentation and source code management**, the analysis of responses shows that actual implementation in most cases corresponds to the declared importance of the issue. Among the responses obtained, only ~8% indicated that this area is not important to them, while the rest indicated the importance or very high importance of this issue.

However, there are organizations that consider this aspect to be of little importance and yet have implemented mechanisms for group work, sharing, or a system of continuous solution building. Interestingly, these are companies that have defined themselves as software products.

There are also opposite situations – companies declare this aspect to be important, but the organization does not have the appropriate tools in place.

6.1.7. Needs and expectations

Next, respondents were then asked ***how important they considered tools*** to support the CRA self-assessment checklist, SBOM, risk management, vulnerability management, incident management, security management, document management, and workflow processes. Their responses are presented in the tables below.

a. Survey questions related to respondents' needs and expectations:

Checklist Automation (CRA self-assessment checklist)	
Answer	Number of Selections
Very important	5
Important	13
Unimportant	5

SBOM - Software Bill of material – preparing/analysis supporting tool	
Very important	7
Important	9
Unimportant	6

Vulnerability management supporting tool	
Very important	10
Important	11
Unimportant	1

Incident management supporting tool	
Very important	8
Important	13

Unimportant	1
Documentation tool (central repository)	
Very important	7
Important	11
Unimportant	4

Table 30: OSCRAT - Answers to the questions "How important to you is..."

Finally, the respondents were asked about their **willingness to participate in the validation of tools** created within the project.

Are you interested in participating in the validation of the tool developed within the project?	
Answer	Number of Selections
Yes	16
I am not sure	6
No	2

Table 31: OSCRAT - Answers to the question "Are you interested in participating in the validation of the tool developed within the project?"

b. Summary:

Vulnerability and incident management are the highest priority for survey participants, with 95% of respondents rating them as important or very important. This suggests that vulnerability and incident management is crucial for survey participants in the context of CRA.

A **central documentation repository and the automation of the CRA self-assessment checklist** are also considered important by survey participants – 82% and 78%, respectively. This indicates the need for a structured approach to documentation and self-assessment.

SBOM received the lowest priority (73%), although this does not mean that the issue is unimportant. This may indicate that the topic of software component materials is less understood or less urgent for respondents.

More than two-thirds of respondents expressed their willingness to participate in the validation of the tools developed as part of the project. This is a good sign that entrepreneurs are interested in the topic, engaged, and ready to collaborate.

For those who are undecided, it may be worth encouraging them, for example by showing the benefits of participation (e.g., early access, impact on features) and providing support (e.g., training).

In summary, the high percentage of responses indicating the importance of these issues to organizations demonstrates their awareness of the issues.

However, the significantly lower level of implementation/launch of appropriate tools may suggest that organizations will undertake such actions in the future. The availability of a single supporting tool, developed as part of the OSCRAT project, may contribute to even greater interest among SMEs.

6.2. Conclusions for the whole questionnaire

Considerations regarding the survey and responses obtained:

- The survey was fully completed by a relatively small number of organizations (24), which may limit the representativeness of the results.
- Certain questions could have introduced ambiguity by addressing multiple aspects within a single item, for example:
 - *“Which stakeholder group do you belong to and what type of products do you offer?”*
 - *“If you use solutions that support SBOM, what types of standards do you use or would like to use?”*
 - *“Have you implemented any documentation management or security management processes in your organization?”*
- The survey did not include questions that would enable more detailed company profiling (e.g., size, number of cybersecurity-related products).
- It also lacked items that could help identify gaps related to CRA-driven needs, whether within organizations or in commercially available solutions.
- In some cases, responses may have been provided by individuals without complete knowledge of the topics addressed, which could affect accuracy.

- Consequently, interpretation of the results is challenging, as only five entities provided clear identification, while the remaining 19 did not specify their profile.

Type of organisation	Number of Selections
Manufacturer	2
Importer	0
Distributor	1
Open-Source software Steward – providing support, not a manufacturer – Article 3 (14) of CRA	2

Table 32: OSCRAT - Type of an organisation

Crucial to the implementation of the OSCRAT project is the fact that most respondents (over 70%) declared that the issues and tools supporting them in this regard relevant to CRA compliance were important or even very important to them. The importance of the following supporting tools was indicated accordingly:

Tool	Respondent's Assessment
Checklist Automation (CRA self-assessment checklist)	78%
Software Bill of material – preparing/analysis supporting tool	78%
Vulnerability management supporting tool	95%
Incident management supporting tool	95%
Documentation tool (central repository)	82%

Table 33: OSCRAT - Tools importance

It should also be emphasized that **67% of respondents expressed a willingness to actively participate in the validation process of tools developed within the OSCRAT platform.**

The percentage of entrepreneurs (ranging from 5% to 33%, depending on the issue) who indicated that the above-mentioned issues were not important to them and expressed a lack of interest in tools supporting activities in areas relevant to CRA compliance confirms the thesis that there is market demand for training and workshops on this topic, which is also the subject of the OSCRAT project.

6.3. Stakeholder Alignment

The analysis of the results from the initial stakeholder survey indicated that certain questions required simplification, others needed to be expanded or supplemented, and the sequence of some should be revised to obtain more precise information. Consequently, a revised version of the survey was developed.

In particular, the section concerning the profiles of the organizations represented by the survey participants was expanded to obtain a more detailed profile of the companies. Additionally, respondents were also asked to indicate their level of readiness for the implementation of the Cyber Resilience Act.

Moreover, questions related to respondents' expectations were formulated with greater precision, allowing for more freedom in expressing their experience and needs regarding the tool being developed within the framework of the project.

A change in the naming of question groups was also proposed (Organization profile, CRA readiness, Inventory/ labelling <SBOM - Software Bill of Materials>, Risk management, Vulnerability management, Incident management, Security management, documentation, workflow and Users' needs and expectations, Participation in workshops and training sessions on the OSCRAT platform), in order to better reflect the context of the questions they contain.

The added and revised questions as well as full content of the revised questionnaire is presented in the Annex 8.

The **revised version 2.2 of the Stakeholder Survey** has been shared again. The questionnaire was used, among other things, during workshops organized in WP4. The immediate goal was to provide more detailed information about the business profile and size of enterprises, as well as the resulting needs.

Survey results are being continuously collected and analysed. By the end of October 2025, 23 responses were received, with 13 fully completed questionnaires. At this stage of the survey, responses were mainly obtained from micro (7) and small (6) enterprises, as well as open-source stewards (2). All of them (100%) offered software products. Regarding the level of readiness to implement CRA, only approximately 13% of respondents declared full familiarity with CRA requirements, 20% indicated partial knowledge of the subject, while around 67% reported no knowledge at all.

Respondents emphasize the need for OSCRAT tools (Inventory / SBOM Management, Vulnerability Handling, Incident Handling, Risk Management,

Security Management Support, Documentation & Workflow) that provide process automation, seamless integration with existing systems, and intuitive user interfaces. Core functionalities should include real-time monitoring, rapid detection and handling of vulnerabilities and incidents with easy-to-use dashboards. Additionally, support for documentation, team collaboration, and transparent reporting is considered essential. These tools must deliver proactive alerts, detailed reporting and decision-support mechanisms to enhance organizational efficiency and security.

6.4. Integration of User Needs

The table below presents a comprehensive overview of user needs around tools supporting security, risk, and IT process management.

It has been developed based on an analysis of key expectations regarding functionality, integration, and usability, which are essential for the effective operation of organisations under the Cyber Resilience Act requirements.

The table is structured into main tool categories (a table rows created from merged cells, e.g., Inventory/SBOM Management Tools, Vulnerability Handling Tools) and their respective features (first column: Feature, e.g., Tracking and Visibility), providing a detailed view of the requirements identified by respondents (User Needs column) within the specific context.

Finally, the last column presents the scope of functionality to be implemented within the respective tools, along with accompanying comments.

Feature	User Needs	Functionality to be implemented - comments
Inventory / SBOM Management Tools		
Automation	Real-time updates	The system will enable:
	Automated scanning	
Tracking and Visibility	Easy tracking of dependencies, versions, licenses	• Importing SBOMs from external sources and tools
	Visibility of components and stock	• Validating SBOM integrity
	Notifications for updates/replacements	• Managing SBOM versions
Integration and Usability	Seamless integration with existing systems	• Analysing SBOMs for vulnerabilities (using an external tool)
	Intuitive dashboards	
Alerts and Compliance	Automated alerts for vulnerabilities	• Only a manual scanning triggered by a user
	Version control	
	Compliance tracking	

Collaboration

Team collaboration features

Feature	User Needs	Functionality to be implemented - comments
Vulnerability Handling Tools		
Detection and Alerts	Real-time alerts	The system will enable: • Entering vulnerability information along with its classification and detailed attributes • Notifying an external organization about the vulnerability • Updating the vulnerability status throughout its lifecycle • Attaching evidence and documentation related to the vulnerability
	Automated alerts for detected vulnerabilities	
Risk Assessment and Prioritization	Detailed risk assessments	
	Prioritization based on criticality	
Integration and Reporting	Integration with security tools	
	Clear reporting	
Remediation Support	Streamlined workflows	
	Suggestions for fixes	
	Immediate alerts for urgent issues	
Disclosure Process	Supporting vulnerability disclosure	

Feature	User Needs	Functionality to be implemented - comments
Incident Handling Tools		
Real-Time Response	Real-time alerts	The system will enable: • Entering incident information along with its classification and detailed attributes • Notifying an external organization about the incident
	Automated categorization and prioritization	
Logging and Integration	Detailed incident logs	
	Integration with other security tools	

Investigation and Resolution	Clear workflows	- Updating the incident status throughout its lifecycle - Attaching evidence and documentation related to the incident
	Step-by-step guidance	
Reporting and Analysis	Post-incident reporting	
	Assistance in report generation	
Threat Detection	Detection of suspicious activity	

Feature	User Needs	Functionality to be implemented - comments
Risk Management Tools		
Identification and Assessment	Identifying potential risks	The system will not have a risk management tool and only will allow documenting the organization's risk management approach (by attaching documents that describe the organization's risk management processes as supporting evidence for assessment). The Documentation tool will provide a Template for Risk Assessment (Annex 13) for manual evaluation of risks.
	Assessing impact and likelihood	
Prioritization and Mitigation	Prioritizing risks	
	Providing actionable mitigation strategies	
Tracking and Visualization	Tracking risk status	
	Visualizing risks during changes or new implementations	
Decision Support	Highlighting highest risks	
	Suggesting ways to reduce them	

Feature	User Needs	Functionality to be implemented - comments
Security Management Support Tools		
Monitoring and Detection	Real-time monitoring	The system will not have a security management tool and only will allow documenting the organization's security management approach (by attaching documents that describe the organization's security management processes as supporting evidence for assessment).
	Automated threat detection	
Integration	Seamless integration with security infrastructure	
Reporting and Compliance	Detailed incident reporting	
	Customizable alerts	
	Compliance support	
Feature	User Needs	Functionality to be implemented - comments
Documentation and Workflow Tools		
Usability	Easy-to-use dashboards	The system will not have documentation management system.
	Long-term planning without excessive manual effort	
Version Control and Collaboration	Version control	
	Easy collaboration	
	User-friendly interface	
Customization and Integration	Customizable templates	The system will support documentation storage and basic edition based on documentation templates only to the extent required to achieve CRA compliance, i.e., CRA conformity self-assessment, vulnerability management, and incident management.
	Integration with other tools	
Task Management	Tracking task progress	
	Automated notifications	
Document Management	Creating and updating documents easily	
	Organizing of work	
	Clear responsibility assignments	

Table 34: OSCRAT - Identified users' needs to be implemented in the tools

It should be emphasized that **the information obtained regarding user needs for the tools indicates expectations comparable to those for fully developed commercial products** (e.g. automation or integration with external tools). The tools being developed will be open-source software, ensuring transparency and adaptability to specific requirements.

The OSCRAAT system will focus on supporting processes and reporting in the areas of conformity self-assessment, SBOM, vulnerabilities, and incidents, guaranteeing compliance with CRA requirements, while some needs - such as comprehensive risk and security management - will be addressed solely through documentation.

Ensuring clear communication of limitations (as presented in subsection 4.2.1) is crucial to avoid discrepancies between expectations and the project scope.

7. Data analysis to inform the development process

7.1. Methodology

The OSC RAT tool specification process consisted of several stages.

In the first stage, **all requirements relevant to the CRA document were collected**, both those relating to the product and those relating to the tool that could support the manufacturing process of such a product. This process covered both the CRA document itself and standards related to incident and vulnerability management. In the latter context, it also covered the scope of support offered by tools for scanning SBOM files. The results of this work are described in the previous chapters: Sources of the requirements, CRA specific requirements identification.

The next stage involved **learning about the real needs of users**, their experiences with existing tools, and their suggestions. For this purpose, a survey was used, the analysis of which is presented in the chapter: User needs analysis.

With this knowledge, the first designs of the OSC RAT tool were created, which were defined user stories, presented in the chapter: **User story – general view**.

All this work led to the definition of the final set of functionalities, which were described on two levels: in the form of use cases for the tool and in the form of detailed descriptions of functionalities.

The process of creating use cases consisted of a detailed analysis of the needs, requirements, and recommendations obtained from external partners. The process of creating a detailed specification of functionalities, on the other hand, consisted of analysing the developed use cases and dialogue between all interested parties involved in the project. The process was enhanced by weekly WP2 Synchronization meetings with projects' partners who contributed with their insights on the functionalities defined in the use cases.

Two levels are presented in this chapter, but at a general level. All detailed information used at the tool implementation stage is included in the appendices to this document.

7.2. Use cases – general view

Below is a description of the basic functions available in the OSC RAT tool. The description is prepared as a combination of graphic elements (representing individual functionalities, operations, or actions) with their descriptions. The diagrams show cases of use of the tool by the end user, but not only. Additional information is provided in Appendix 6 to this document.

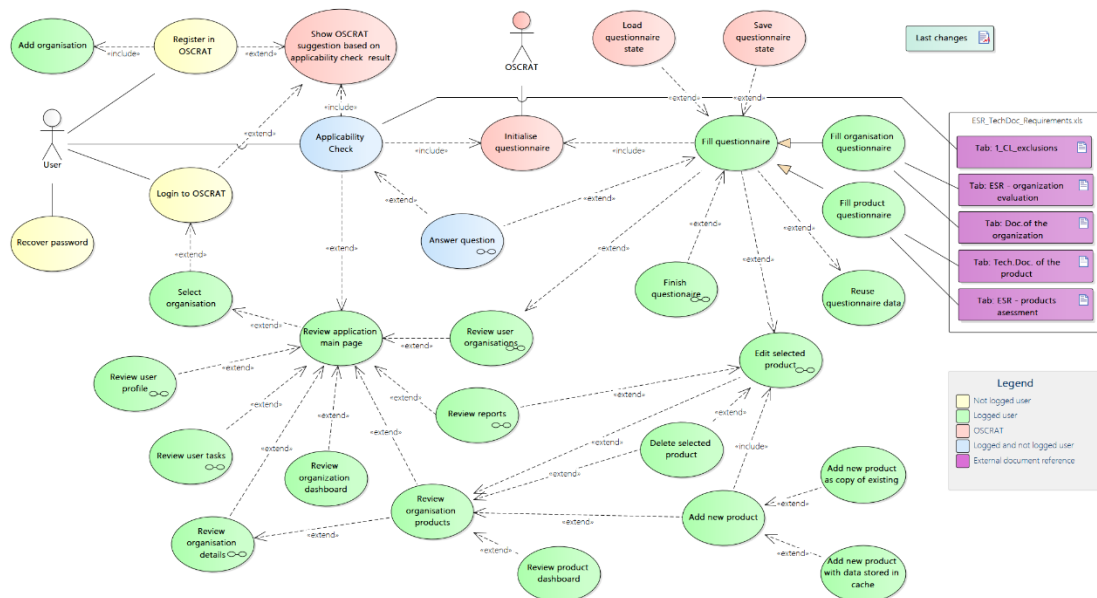


Figure 18: OSCRAT - General view of OSCRAT tool functions for end user

The diagram presents a **Use Case model of the OSCRAT system**, it reflects the interactions between users and system functionalities. It presents definitions of relationships user type -> functionality and functionality -> functionality, helping to understand what action (or sequence of actions) can be performed by a specific user.

The diagram in its upper right corner shows elements grouped under the name **“ESR_TechDoc_Requirements.xls.”** It is important to note that this document is a spreadsheet with multiple tabs, which contains all the detailed product requirements resulting from the CRA document.

These are not direct requirements for the OSCRAT tool, but in a way, they partially enforce a specific functional scope. However, these requirements directly affect the content of the surveys available in the tool.

Actors defined in the diagram:

- User and sub-roles (logged/not logged/logged and not logged) – organization
- OSCRAT – system entity responsible for automatic actions related to questionnaire

As an unregistered user, you can only perform a limited number of actions in the system. These actions are related to two separate areas: the user and their account, and quick verification of the need to apply CRA requirements. Within the account, an unregistered user can:

- **UC:** register in the system
- **UC:** log in to the system
- **UC:** recover the password to their account

Regardless of whether the user has an account in the OSCRAT system, they can verify the need to apply CRA requirements (UC: Applicability check) at any time by completing a specially prepared questionnaire (UC: answer question).

Quick verification of the need to apply CRA requirements ends in two ways (UC: show OSCRAT suggestion based on pre-questionnaire result):

- no such need and no further action.
- the possibility to log in to the system and perform further support activities offered by the OSCRAT tool.

The functions available to logged-in users include:

- **UCs:** add, select, edit, and review organization (and details);
- **UCs:** edit and review user profile
- **UCs:** review user tasks
- **UCs:** add, edit, delete, and review product
- **UCs:** review organization and product dashboards
- **UCs:** review reports (i.e. for product)
- **UCs:** fill additional questionnaires.

It is worth noting here that the user has the option of using previously provided information (when completing the first questionnaire) when adding a product (UC: add new product with data stored in cache). However, when completing the same questionnaire again, it is pre-filled with the previously provided answers (UC: reuse questionnaire data).

Completing each questionnaire is supported by actions performed by the OSCRAT system in the background, which cause initialization of the questionnaire (UC: initialize questionnaire), saving its status after each answer provided by the user (UC: save questionnaire state), and restoring it to its previous status in the event of interruption (UC: load questionnaire state).

At any time, from the main application window, the user has access to the most important functions and views of the tool:

- products
- organization
- dashboards
- reports
- tasks

- user profile

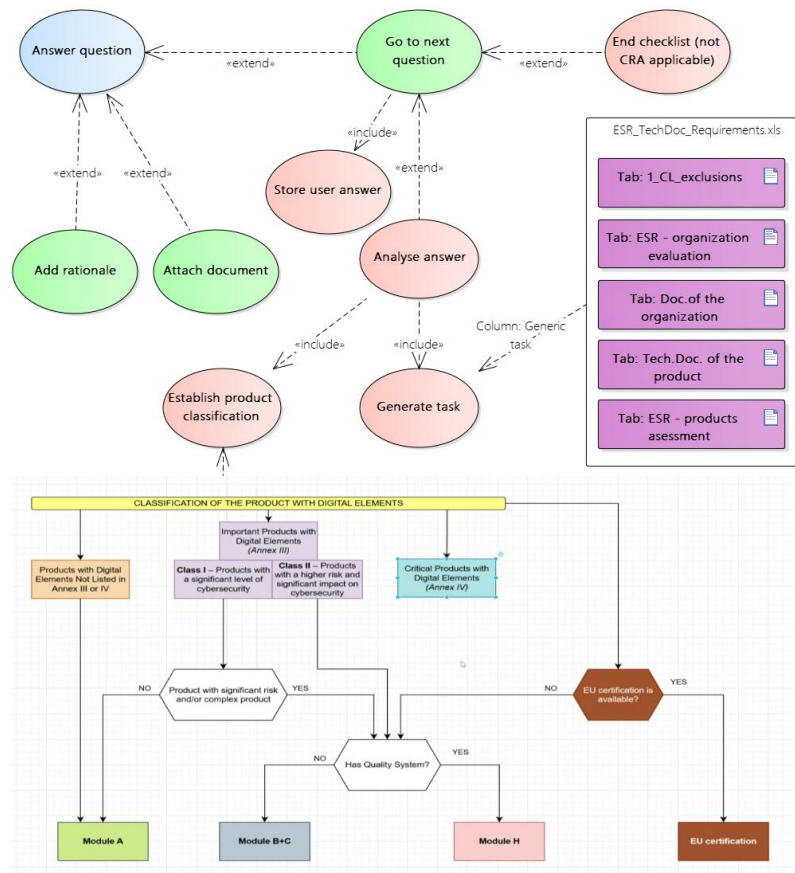


Figure 19: OSCRAT - Answer question functions

When answering survey questions, users can supplement their answers by adding additional information in the form of external program files (UC: attach document). Users can also add a justification (UC: add rationale) at any time. Users can move on to the next question at any time (UC: go to next question).

In the background, the OSCRAT tool performs several tasks.

First, it saves the user's answer (UC: store user answer). If this is the last question, the system ends the survey and displays a recommendation (UC: end checklist).

In some cases, the system analyses the answer provided (UC: analyse answer) and performs additional tasks that may make it easier for the user to work with the tool in the future (UCs: establish product classification, generate task).

To establish product classification, there is a diagram (product classification workflow), which could be helpful.

To generate right task - there is the technical document with additional information (**ESR_Tech_Doc_Requirements.xls**).

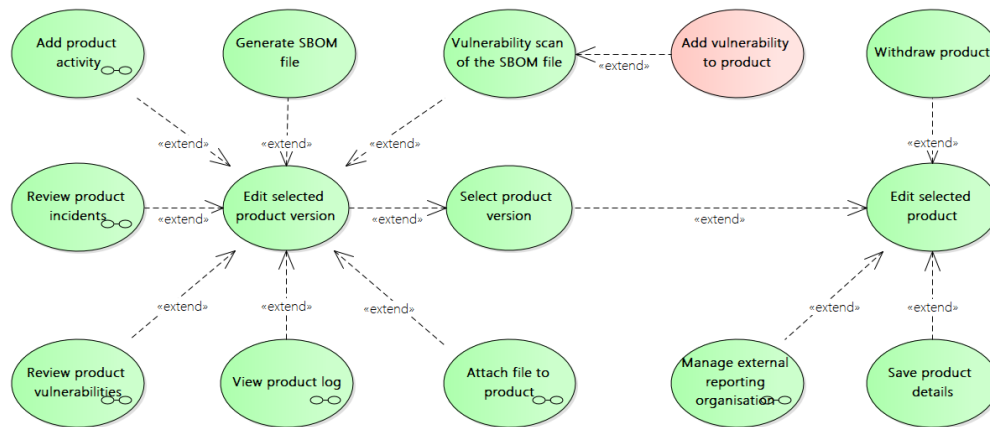


Figure 20: OSCRAT - Edit selected product related functions

Editing a selected product is divided into two separate parts: editing the entire product and managing product versions.

For the entire product, the logged-in user can manage external reporting organizations, withdraw the product, and save basic product information (UCs: manage ext. organizations/save/withdraw).

Extended information is available for a specific product version, selected from a list. This information includes:

- viewing the history of operations performed for the product (UC: view log)
- adding an additional external file (UC: attach file)
- adding an activity performed for the product (UC: add activity)
- viewing vulnerabilities and incidents (UCs: review vulnerabilities/incidents)
- analysing the SBOM file (UC: analyse SBOM)

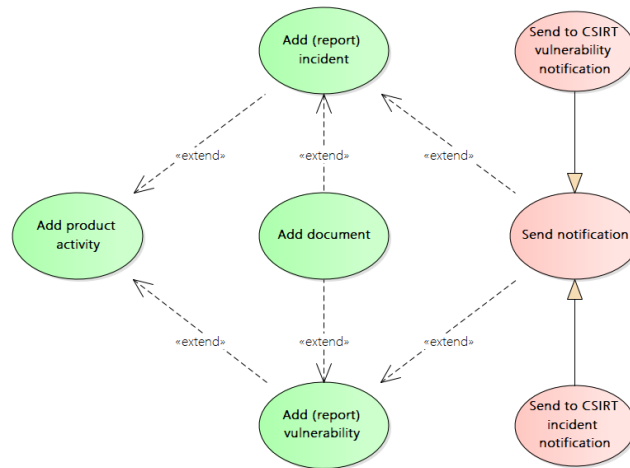


Figure 21: OSCRAT - Add product activity related functions

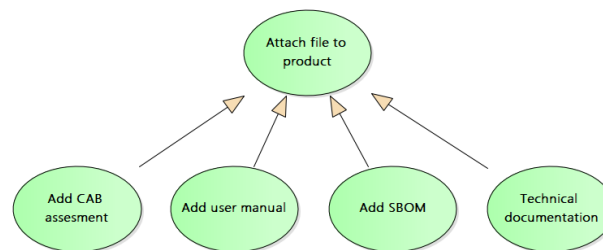


Figure 22: OSCRAT - Attach file to product functions

Adding an external file for a product means that you can add one of the following types of documents:

- CAB assessment
- User manual
- SBOM
- Technical documentation

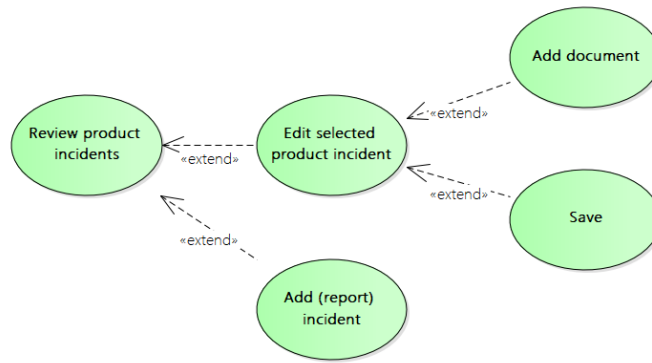


Figure 23: OSCRAT - Review product incidents functions

From the **incidents overview level for a product**, it is possible to view the details of a selected incident and edit its parameters (UCs: edit, add document, save). It is also possible to register a new incident (UC: add incident).

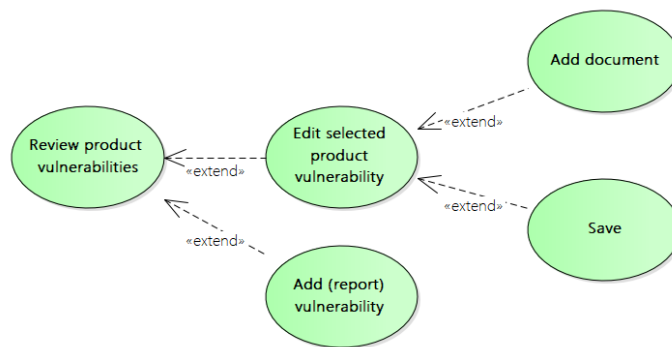


Figure 24: OSCRAT - Review product vulnerabilities functions

From the **vulnerabilities overview level for a product**, it is possible to view the details of a selected vulnerability and edit its parameters (UCs: edit, add document, save). It is also possible to register a new vulnerability (UC: add vulnerability).



Figure 25: OSCRAT - View product log functions

Viewing the **activity history for a product** means viewing the history of recorded vulnerabilities or incidents.

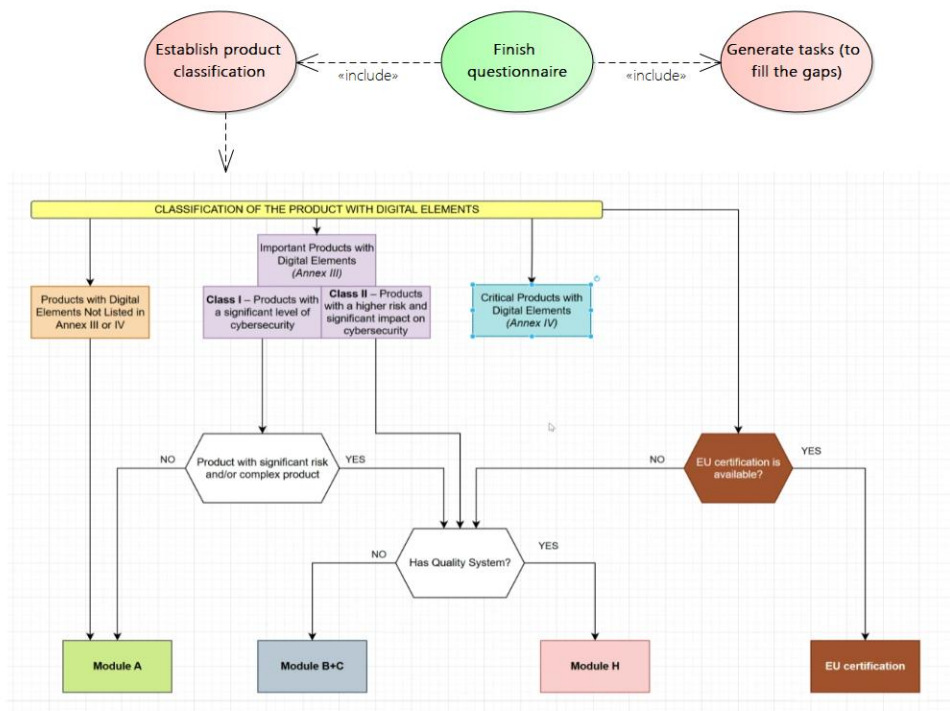


Figure 26: OSCART - Finish questionnaire related functions

The user can finish **filling out the questionnaire at any time** (UC: finish questionnaire). In this case, the OSCART tool performs additional tasks that may make it easier for the user to work with the tool in the future (UCs: establish product classification) and generate tasks for product classification based on presented workflow, for applicability questionnaire.

To establish product classification, there is a diagram (product classification workflow), which could be helpful.

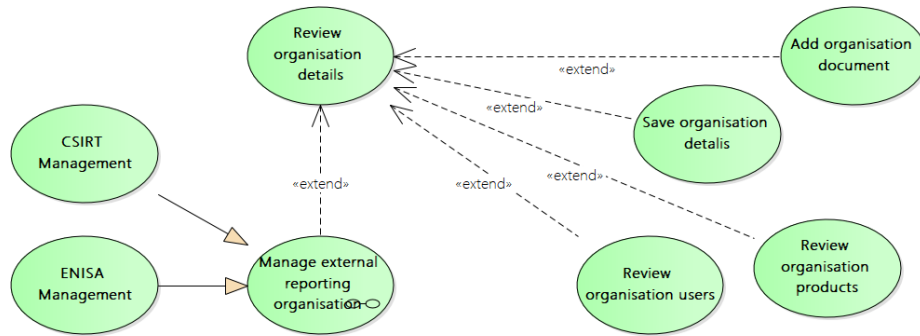


Figure 27: OSCRAT - Review organisation details related functions

A logged-in user can view data about their organizations. To do this, they select an organization in the main window of the tool. For this organization, the tool allows them to view its users, documents, and products (UCs: review users/products).

It also allows them to edit and save changes made to the organization's data (UC: save).

Each organization can have external organizations defined for each product, which will be notified of vulnerabilities or incidents, for example. The global list of such external organizations can be managed from the organization level (UC: manage external reporting organization).

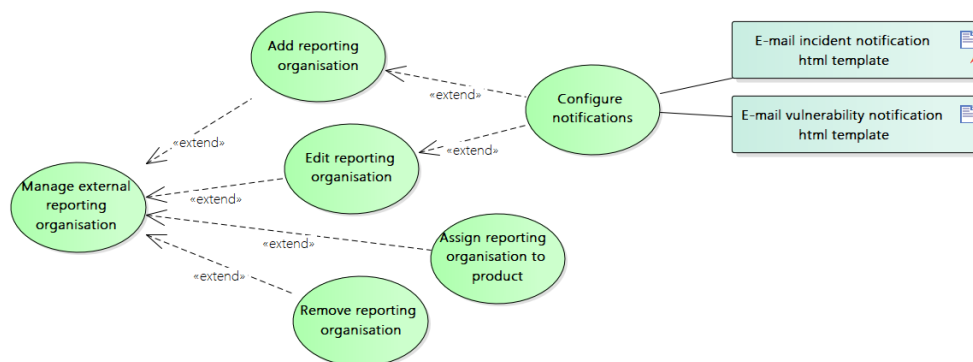


Figure 28: OSCRAT - Manage external reporting organisation functions

Managing external organizations involves viewing and editing the list of such organizations. Adding and editing an external organization involves entering the appropriate values in the relevant fields and configuring notifications sent to it (UCs: add/edit organization, configure notification). Each external organization can also be removed from the list (UC: remove).

Additionally, **each product of an organization can be linked to other external organizations** (UC: assign reporting organization to product).

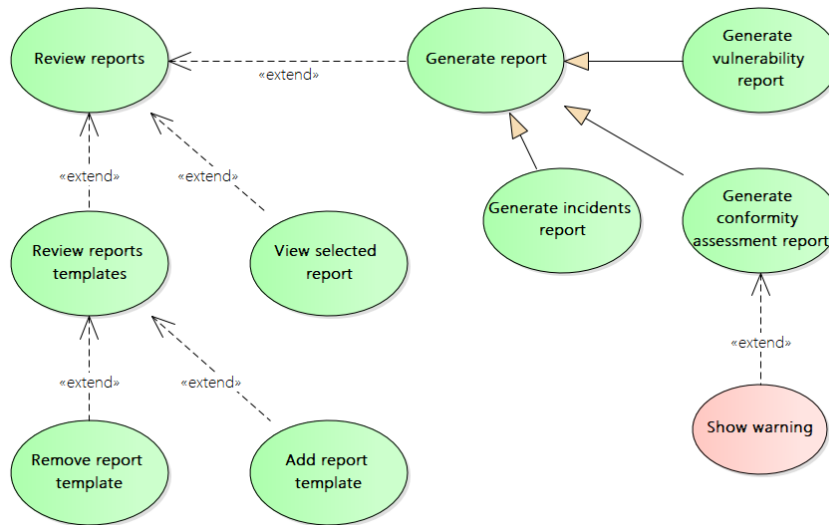


Figure 29: OSCRAT - Review reports related functions

The OSCRAT tool can generate various types of reports (UCs: generate report).

Reports are based on templates that logged-in users can add to their own organization (UCs: review reports templates, add/remove report template).

Currently, there are **three different types of reports**:

1. conformity assessment,
2. incidents and
3. vulnerabilities.

Each generated report can be viewed in the tool (UC: view selected report).

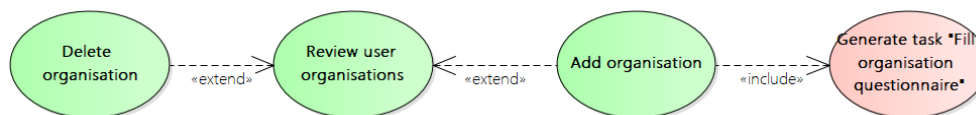


Figure 30: OSCRAT - Review user organisations functions

Each user registered in the OSCRAT tool can be assigned to any number of organizations. In the OSCRAT tool, due to the lack of such a necessity, it was decided not to implement advanced organization management.

Therefore, each user can add or join a selected organization or a new organization they have created themselves. They can also delete their organization, with the proviso that all data related to that organization will be unavailable.

Additionally, when creating an organization, the OSCRAT tool will generate a reminder task for that user (UC: generate task - fill organization questionnaire).



Figure 31: OSCRAT - Review user profile functions

Logged-in users can manage their own accounts. This means they can change their password (UC: change password), edit and save basic user information (UC: save user profile details).

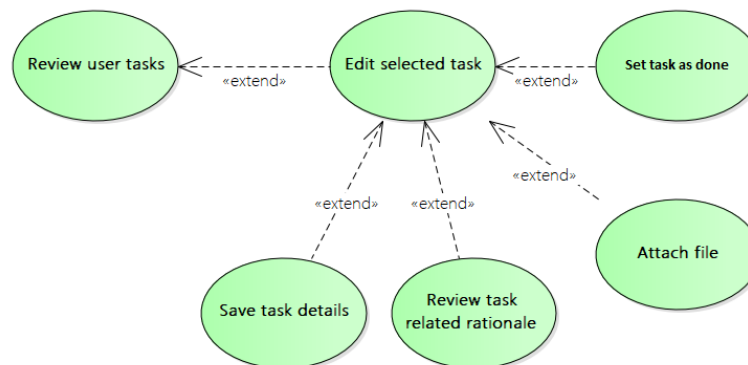


Figure 32: OSCRAT - Review user tasks functions

For each user, **the OSCRAT tool can generate tasks that can help meet CRA requirements.**

Tasks take the form of recommendations to be carried out either in the OSCRAT tool or in another tool used by the user in their daily work.

All the user's current tasks can be viewed directly from the main application window. In the next steps, it is possible to: edit and save the selected task (UCs:

edit selected task, save task details), complete its processing (UC: set task as done), attach an additional file to the task (UC: attach file), and view the task-related rationale.



7.3. Specification of implementation tasks

The developed system assumptions and requirement have been consolidated and documented to serve as input for the design of the system architecture and subsequent software development activities. The requirements and assumptions were prepared using various tools and methodologies and have been collected and grouped as follows:

- **User Story Diagrams** – describing the overall system concept, functionality, and operational flow from the user's perspective, including the main user interactions and workflows within the system (Section 7.2).
- **Use Case Diagrams** – providing detailed descriptions of the functionalities to be implemented, the user interactions, and the corresponding system responses (Section 7.3).
- **Figma Diagrams** – presenting interface design concepts and proposed layouts for the system's user interface.
- **draw.io Diagrams** – illustrating the logical workflow of system operations, the activities workflow required under the CRA, and the planned process flows within the system (Section 4.1).

Due to the significant variation in both the level of detail and the substantive scope of the collected requirements and descriptions, **it was decided to organize additional recurring coordination meetings.**

The purpose of these meetings is to synchronize and refine the gathered information, ensuring that the system design and implementation teams operate based on consistent and unambiguous requirements.

The outcome of these meetings consists of detailed task descriptions developed and maintained within the task management system. Each task specifies and documents particular elements of system functionality. The task descriptions aggregate information from all the sources and form the primary reference material for designers and developers.

All prepared, analysed, and finalized tasks have been compiled in Annex 3.

8. The Final List of Functionalities

The chapter is the summary of the detailed descriptions of functionalities in Annex 3.

8.1 Checklist

Applicability check for CRA (Unregistered User)

See detailed information in: Annex 3, Chapter 1

- **Accessing the Applicability Check** (Button on landing page) – to determine whether the product falls under the scope of the CRA
- **Questionnaire Logic** (based on CRA – XLS Sheet CL_Exclusion) – users are guided through a structured set of questions evaluating product applicability
- **Outcome Path:**
 - product is eligible or not,
 - eligible product classification: Critical, Important – Class I, Important – Class II, Other
- **User session data persistence** (product details and result).

CRA Compliance Assessment for a Product Version

See detailed information in: Annex 3, Chapter 5

- Automatically initiated CRA compliance self-assessment, when a new product version is created.
- Self-Assessment supports a structured self-evaluation process aligned with CRA requirements
- Hierarchical level of questionnaire: Area or requirements / Requirement / Question
- Organization role-specific questionnaires references

Administration of a Product Assessment Questionnaire Template

See detailed information in: Annex 3, Chapter 6

- Compliance self-assessment questionnaires are not hardcoded.
- Define a questionnaire template in a structured (JSON) format (based on the CRA Requirements Spreadsheet)

- Modify questionnaire template (template can be updated over time via an import mechanism)
- Mechanism to upload/import new questionnaires

Product Assessment Dashboard, Visualization, PDF Export

See detailed information in: Annex 3, Chapter 7

- A dynamic dashboard summarizing compliance progress for each product assessment
- Dashboard includes assessment status tables, product assessment charts, progress bar/indicators
- Export Conformity Assessment Report (pdf document)

Administration of an Organization Assessment Questionnaire Template

See detailed information in: Annex 3, Chapter 8

- Compliance self-assessment questionnaires did not hardcode.
- Define a questionnaire template in a structured (JSON) format (based on the CRA Requirements Spreadsheet)
- Modify questionnaire template (template can be updated over time via an import mechanism)
- Mechanism to upload/import new questionnaires
- CRA Process Assessment for an Organization
- See detailed information in: Annex 3, Chapter 9
- Automatically initiated CRA organizational process self-assessment, when a new organization is created.
- Hierarchical level of questionnaire: Area or requirements / Requirement / Question
- Organization Role-Specific Questionnaires references

Organization Assessment Dashboard, Visualization, Export

See detailed information in: Annex 3, Chapter 10

- A dynamic dashboard summarizing compliance progress for organizational assessment
- Dashboard includes assessment status tables, product assessment charts, progress bar/indicators
- Export Conformity Assessment Report (pdf document)

Automatic Task Generation

See detailed information in: Annex 3, Chapter 21

- Automatic task creation based on requirement-level self-assessment results (Not Compliant / Partially Compliant / Compliant / Not Applicable).
- Tasks include predefined fields and product version association.
- Additional logic for marking assessments as completed when all requirements are Compliant or Not Applicable.

8.2 SBOM

SBOM Management

See detailed information in: Annex 3, Chapter 20

- Display a list of all SBOMs associated with the selected product version
- Generate SBOMs directly within the system
- Import externally generated SBOMs
- Download existing SBOMs
- Scan SBOMs for vulnerabilities, resulting in a generated Vulnerability Report
- Review the Vulnerability Report and selectively add identified vulnerabilities to the Vulnerability Module
- Configuration of the project path and access data to generate SBOM

8.3 Vulnerability

Add New Vulnerability

See detailed information in: Annex 3, Chapter 16

- Create a new vulnerability record
- Associate vulnerability with a specific product and version
- Input key details such as name, status, severity, date of discovery, etc.
- Attach supporting documents related to vulnerability

Edit Vulnerability

See detailed information in: Annex 3, Chapter 18

- Modify existing vulnerability records
- View read-only fields and update editable information
- Attach or manage related documents

Vulnerability Details Page

See detailed information in: Annex 3, Chapter 13

- View complete vulnerability details
- Access an attachment section showing all associated files

8.4 Incident

Add New Incident

See detailed information in: Annex 3, Chapter 17

- Create a new incident record
- Associate the incident with a specific product and version
- Input details such as: ID, status, classification, attack type, asset details, reporter, etc.
- Attach supporting documents related to the incident

Edit Incident

See detailed information in: Annex 3, Chapter 19

- Modify existing incident records
- View read-only fields and update editable information
- Attach or manage related documents

Incident Details Page

See detailed information in: Annex 3, Chapter 14

- View complete incident details
- Access an attachment section showing all associated files

8.5 Documentation

Incident template – see detailed information in Annex 10

Vulnerability template – see detailed information in Annex 11

General description

See detailed information in: Annex 3, Chapters: 4, 7, 11, 12, 15

- Open text sections to describe products, versions.
- Adding images, uploading related documents.
- Support period determination of the product version
- Data saved per product version and automatically included in the published report.

Specification, description of the design & development processes of the product

See detailed information in: Annex 3, Chapters: 4, 11, 12, 15

- Open text sections, description fields to allow users to describe how design principles ensure CRA compliance.
- Adding images, related documents (diagrams, files).

Vulnerability handling process

See detailed information in: Annex 3, Chapter 20

- Documents' templates for vulnerability handling process available for the users
- Users can adjust the pre-filled (templates) content.
- SBOM files management (generating, uploading, downloading).
- Reports generation from the vulnerability scan.
- Possibility to publish vulnerability disclosure policy, selected product documentation.

Production & monitoring processes documentation

See detailed information in: Annex 3, Chapters: 6, 7, 8, 10, 11, 12

- Questionnaires for the self-assessment of the organization documentation elements and content (to check missing documents).
- Uploading evidence documents for the self-assessment activities, documentation related to the processes production within the organization, monitoring processes related to the production activities,
- Reports for the organization's compliance self-assessment

Cybersecurity Risk Assessment

See detailed information in: Annex 3, Chapters: 13, 14, 16, 17, 18, 19

- Risk assessment template available, including information how the essential cybersecurity requirements (CRA Annex I) are applicable - (users can modify predefined sections, see Annex 13).

Conformity Verification

See detailed information in: Annex 3, Chapters: 7, 10, 12, 20

- For the product with self-assessment - support in preparation of Declaration of Conformity (DoC) document for the product - document template available.
- For the product assessed by 3rd party – upload of the assessment report and signed DoC.
- DoC available in the tool, can be downloaded
- Evidence of conformity files available in the OSC RAT tool (SBOM files, vulnerability scan reports, self-assessment reports).

8.6 General Functionalities of OSC RAT Platform

Account Creation flow for unregistered users

See detailed information in: Annex 3, Chapter 2

- Navigation (landing page) - unregistered users can create an account directly from the landing page
- Users provide:
 - Personal details (Name, Email, Password)
 - Organization type (Natural Person or Legal Person)

- Organization details (Name, Role such as Manufacturer, Authorized Representative, OSS Steward, Importer, Distributor)
-

Organization Creation – logged-in users

See detailed information in: Annex 3, Chapter 3

- Logged-in users can create additional organizations.
- Users select the organization type (Natural Person or Legal Person) and enter organization details.
- The creator is automatically added as a member of the newly created organization.

Add New Product

See detailed information in: Annex 3, Chapter 4

- Users can create new products under their organization (from scratch, data taken from cache – from the last applicability check, based on existing product data).
- Users enter product information such as Name, Version, and Description.
- Applicability check is integrated into the product creation flow.
- System guidance ensures that only products appropriate for the organization's role are added.

Product Details Page

See detailed information in: Annex 3, Chapter 11

- Full view of product information and properties:
 - Name
 - Category
 - Organization Role
 - Incidents Count
 - Vulnerabilities Count
 - External Reporting
 - Assessment Type
 - Description
- Users can Edit, Withdraw, or Delete the product.
- Users can view or edit the Applicability Survey.

- Product versions section fields and buttons
- Product versions are grouped into two tabs:
 - Supported
 - Not Supported

Add New Product Version

See detailed information in: Annex 3, Chapter 15

- Users can create new product versions.
- Users can define version-specific fields such as Name, Description, and Supported / Not Supported status.

Product Version Details Page

See detailed information in: Annex 3, Chapter 12

- Comprehensive view of all Product Version details.
- Displays key properties such as:
 - Name
 - Status
 - Open Incidents Count
 - Open Vulnerabilities Count
 - Open Tasks Count
- Provides access to:
 - CRA Compliance Assessment - View and Edit CRA compliance assessment of the product version
 - Declaration of Conformity - View and Download “Declaration of conformity”
 - Related Information via multiple tabs (Tasks, Files, SBOM, Vulnerabilities, Incidents, Version Logs, Repositories)

9. Stakeholder Alignment and Project refinement (T2.5)

The task involves aligning stakeholders' expectations and refining project requirements within the OSCRAT initiative. It includes seeking approval from stakeholders or the steering committee for key decisions, strategies, or deliverables, ensuring alignment with OSCRAT objectives. Additionally, it entails refining project requirements to accurately reflect stakeholder needs and project goals, facilitating effective decision-making and enhancing project outcomes.

9.1. Stakeholders training and workshops results

The stakeholders' survey (version 2.2) was released, and 30 complete responses have been received so far, with additional feedback still being collected. The **updated version of the survey features improved consistency and refined wording of the questions**, making it easier for stakeholders to understand and complete.

During the reporting period, **four introductory training sessions** were planned to be conducted with stakeholder groups representing SMEs, public-sector cybersecurity professionals, and software development teams.

These sessions, three of which completed by Nov. 10th, 2025, focused on the conceptual understanding of the Cyber Resilience Act (CRA), the structure of CRA obligations, and the intended role of the OSCRAT platform in supporting organizations along the pre-market and post-market compliance lifecycle.

Although the hands-on pilot use of the OSCRAT platform will begin in the series of practical workshops scheduled from January 2026 onward, the initial training activities already contributed to the validation of the user-facing logic and core workflow assumptions. Specifically, during these sessions, partners presented:

- Mock-up interface screens (FIGMA prototypes) representing the core modules (Checklist, SBOM handling, Vulnerabilities, Incidents, and Documentation).
- Walkthroughs of user journeys for both pre-market (product classification, conformity assessment) and post-market (vulnerability and incident handling) phases.
- Illustrative examples of CRA task generation and the supporting role of the platform in structuring compliance activities.

Participants provided feedback on expected usability, terminology clarity, and the level of required automation versus user-controlled decision-making.

This input has been used to refine how guidance text, instructional tooltips, and requirement interpretations are presented within the interface. While the actual software was not demonstrated live at this stage, this early engagement

ensured that upcoming hands-on workshops will be aligned with stakeholder expectations and real operational workflows.

Ensuring a Meaningful and Compliant Pilot Phase

The early-stage training played a preparatory and alignment role for the pilot phase. By introducing participants to the CRA framework and the OSCRAT process logic in advance of platform access, the consortium ensured that stakeholders will be able to engage meaningfully with the tool once hands-on testing begins. This approach supports a progressive onboarding model, where:

- Awareness and conceptual alignment are established first (completed in current reporting period),
- Hands-on interaction and feedback cycles follow once the tool interfaces reach a stable test-ready form (starting January 2024).
- This staged training strategy contributes directly to the compliance and effectiveness of the pilot phase, as users will enter it with:
 - A shared understanding of CRA requirements and terminology,
 - A clear expectation of how OSCRAT supports compliance steps,
 - Familiarity with the planned modular workflow of the tool,
 - The ability to provide informed and structured feedback during live tool testing.

As a result, **the pilot phase will not function merely as a technical demonstration but as an evidence-based validation cycle**, enabling iterative refinement of both functionality and usability in alignment with CRA compliance goals and SME operational practices.

9.2. Project Requirements Refinement

Project requirements refinement focused on ensuring that the OSCRAT platform's design, scope, and functional requirements remained fully aligned with stakeholder expectations and the evolving regulatory context of the Cyber Resilience Act (CRA). The activity served as a bridge between early requirements definition (WP2) and the implementation phase (WP3), providing validation, refinement, and confirmation of the project's direction.

Stakeholder alignment was achieved through continuous engagement with SMEs, and project partners. A revised version of the stakeholder survey (v2.2) was developed and deployed, offering clearer wording, improved structure, and additional questions to capture more accurate insights into user needs which are planned to be implemented in the tool (see chapter 6.4 Integration of user needs).

In parallel, project requirements were refined through systematic review meetings, analysis of survey results, as well as inputs from trainings, workshops, and planned use cases involving the OSCRAT platform tools. This process ensures full traceability of all requirements—from CRA provisions to platform functionalities—and supports the preparation of complete implementation tasks for WP3 developers.

10. Conclusions

This deliverable, **D2.1 – Comprehensive Project Requirements Document**, consolidates the results of WP2 activities, which focused on defining, analysing, and refining the requirements for the OSCRAT tools supporting platform. The work done within WP2 provided an input material for the design and implementation phases planned in WP3.

The **requirements identification process** was based on multiple complementary sources, including the project proposal, a state-of-the-art review of existing R&D initiatives and commercial tools, stakeholder surveys, and the domain expertise of project partners. This multi-source approach ensured both CRA regulatory accuracy and practical applicability of the defined functionalities.

Within **Task 2.1 – Scope Definition**, the project team developed detailed CRA conformance flow diagrams covering product classification, assessment, and pre-market and post-market functionalities. User story and use case diagrams provided a structured overview of the OSCRAT tools: Checklist (CL), Software Bill of Materials (SBOM), Vulnerabilities (VUL), Incidents (INC), and Documentation (DOC). The scope definition presents the comprehensive overview of tools' functionalities and limitations.

In **Task 2.2 – CRA-Specific Requirements Identification**, a comprehensive analysis of the Cyber Resilience Act (CRA) was conducted. The analysis identified and mapped all obligations and references from the Regulation, aligning them with international standards such as ISO/IEC 27035, ISO/IEC 29147, and ISO/IEC 30111. The outcomes were implemented as structured checklists within the Checklist (CL) tool and documented in the ESR_TechDoc_Requirements.xlsx file, ensuring full traceability and coverage of CRA provisions and articles.

The user needs analysis (Task 2.3) confirmed a strong interest in CRA compliance support solutions. Most respondents considered CRA-related tools important or very important, with 67% declaring willingness to participate in future validation processes. Feedback from the first survey led to the release of an improved version (v2.2), which received 30 complete responses and will inform further refinement of requirements and functionalities in subsequent project stages.

In **Task 2.4 – Data Analysis to Inform the Development Process**, the results from user stories, use cases, and Figma mock-up screens were translated into precise implementation tasks for WP3 developers. This ensured a seamless transition from conceptual, high-level abstraction, requirements to actionable technical specifications. Weekly coordination meetings enabled continuous validation of assumptions and consensus-building among project partners.

Finally, **Task 2.5 – Stakeholder Alignment and Project Requirements Refinement** is planned to ensure that all key requirements remain aligned with stakeholder expectations and evolving ENISA guidelines. The feedback loop established through surveys, workshops, and upcoming tool testing will continue to guide refinements during later stages of the project, ensuring that OSCRAT tools remain compliant, robust, and up to date.

In conclusion, **WP2 has successfully delivered a coherent and comprehensive set of requirements that integrate CRA compliance obligations, user needs, and technical feasibility**. The outputs of this work package — including CRA workflows, user stories, use cases, the “*ESR_TechDoc_Requirements.xlsx*” dataset file, and validated stakeholder feedback — provide a complete and reliable input to the design and implementation phase in WP3.

11. Conclusions

Following this deliverable, project activities will advance to WP3, focusing on the implementation, integration, and validation of the OSCRAT tools.

Testing and feedback will be obtained through training sessions, workshops, and real uses cases. The consortium will update the tools and specifications also in case when new guidelines and harmonized standards are published to ensure full CRA compliance.

The revised stakeholder survey (v2.2) is still ongoing, and its analysis will inform final requirements, needs and expectations. Updated and compliant OSCRAT tools will then be provided to industrial partners for validation under WP4, ensuring technical and regulatory alignment with the newest conformity assessment methodologies of harmonized standards.

12. References

- [1] Grant Agreement, Project 101190180 – OSCRAT
- [2] Deliverable D1.1 Develop a Project Plan, Project 101190180 – OSCRAT

13. Annexes

13.1 Annex 1 – State of the art no. 1

See external file D2.1-Annex_1

A comparison of the functional scope of the identified tools and projects in relation to the planned elements of the OSCAT tool is presented in a summary table at the end of Annex 1.

13.2 Annex 2 – State of the art no. 2

See external file D2.1-Annex_2

Annex 2 includes the results of the analysis of incident and vulnerability handling aspects that should be considered when planning the functionality of the OSCAT tool.

13.3 Annex 3 – Implementation Tasks

See external file D2.1-Annex_3

13.4 Annex 4 – ESR_TechDoc_Requirements

See external file D2.1-Annex 4-ESR_TechDoc_Requirements.xlsx

13.5 Annex 5 – Questionnaire User Guide

See external file D2.1-Annex_5

13.6 Annex 6 – Use Cases Diagrams

See external file D2.1-Annex_6

13.7 Annex 7 – Stakeholder Questionnaire

See external file D2.1-Annex_7

13.8 Annex 8 – Revised Stakeholder Questionnaire

See external file D2.1-Annex_8

13.9 Annex 9 - Documentation Pillar for OSCRAT

Technical Specification: OSCRAT – CRA Annex VII Technical Documentation

13.10 Annex 10 – Incident Template

See external file D2.1-Annex_10

13.11 Annex 11 – Vulnerability Template

See external file D2.1-Annex_11

13.12 Annex 12 – CRA Conformity Assessment Guide

See external file D2.1-Annex_12

13.13 Annex 13 – Risk Assessment Template

See external file D2.1-Annex_13

13.14 Annex 14 – CRA-specific requirements mapping

See external file D2.1-Annex_14

13.15 Annex 15 – Vulnerability Disclosure Policy Template

See external file D2.1-Annex_14



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – Comprehensive Project Requirements Document



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

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 1

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 1
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

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 describes the state-of-the-art (part 1) in the field of OSCRAT project.
Keywords
State-of-the-art

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.

Table of contents

1. Introduction	5
2. OSCRAT toolkit functionality and properties based on the project assumption	5
3. EU initiatives supporting CRA implementation	8
3.1. CRAcoWi – Cyber Resilience Act Compliance Wizard	8
3.2. TrustBoost – Unifying & Upgrading Certification.....	9
3.3. CRACY – CRA made easy	9
3.4. OCCTET – EU Project Open Source Compliance Comprehensive Tools and Resources	10
3.5. CYBERFORT – Strengthening cyber defenses of SMEs for Cyber Resilience Act (CRA) compliance	11
3.6. CONFIRMATE – CONFormity assessment, metRics and compliance autoMATION for the cyberresilience act.....	12
3.7. CURIUM.....	12
3.8. CRA-AI – Cyber Resilience Act Artificial Intelligence	13
4. Examples of commercial tools.....	15
4.1. CRA Readiness Assessment – Cyber Resilience Act Readiness Assessment web application	15
4.2. The Product Security Platform	16
4.3. Finite State's platform	17
4.4. Application Security Posture Management Platform (ASPM).....	18
4.5. The Embedded Kit.....	19
5. Background of OSCRAT research and development.....	21

Figures

<i>Figure 1: Screenshot from the Cyber Cert Labs web site</i> <i>[https://www.cybercertlabs.com/]</i>	15

List of Tables

<i>Table 1: The basic functionality of OSCRAT toolkit.....</i>	7
<i>Table 2: Identifying the scope he CRA automation tools, outlining its functionalities and limitations. OSCRAT as the reference tool.....</i>	22

1. Introduction

The deliverable D2.1 encompasses a detailed overview of the CRA automation tools, including their scope, functionalities, and limitations. Additionally, it embraces the identified CRA-specific requirements for each tool, user needs analysis, and data collection.

The research works are preceded by the review of running projects focused on similar tools. The objective of the survey is to identify the background of research and development works focusing on the CRA related tools developed in OSCRAT.

The survey embraces on EU projects related CRA and indicates some examples of existing commercial tools.

2. OSCRAT toolkit functionality and properties based on the project assumption

The OSCRAT toolkit is developed to support CRA compliance procedures for European SMEs, which provide digital products to the market. It embraces five tools focused on different aspects of the development, manufacturing and maintaining of digital products.

The OSCRAT toolkit offers:

- Checklist automation,
- SBOM support,
- Vulnerability management support,
- Incident handling process,
- Documentation CRA compliance support and management.

The general OSCRAT toolkit properties are:

- Risk centred,
- Product life-cycle support,
- CRA focused,

Available free - implemented on the open-source Unicis Platform Community Edition.

More details are shown in the Table 1.

OSCRAT supports indirectly security awareness, trainings, knowledge sharing, etc.

Limitation:

- Not AI-based,

- Range of automatic support seems to be considerable comparing to other tools, though is still limited.

Functionality				
Checklists automation	SBOM support	Vulnerability management support	Incident handling process	Documentation CRA compliance support and management
- Checklists are very detailed and controlled by the tool - To identify the digital product category with respect to the CRA - To provide self-assessment checklists - To provide third-party assessment checklists - To support users in conducting self-assessment with the generated checklist - To produce conformity assessment reports for SMEs - Checklists embrace CRA, ISO/IEC 30111, ISO/IEC 29147, ISO/IEC 27035 - Possibility of the product reassessment - Guiding users how to achieve the CRA conformity (detailed tasks for users)	- To collect SBOM manifests - To parse the project description files - To generate SBOM reports compliant with SPDX/CycloneDX standards on this basis - To download CVE data and produce final scan reports - Integration with the external SBOM verification tools	- To provide SMEs with a structured, OVAL-based, approach to manage vulnerabilities according to the to the ISO/IEC 29147 (vulnerabilities disclosure) and ISO/IEC 30111 (vulnerabilities handling) - To provide the reporting channel to relevant EU agencies, such as ENISA - Simple communication channels (email, form) to external organizations coordinating security	- To identify the severity of incidents - To support the incident handling process (preparation, detection, severity assessment, reporting, response, lessons learnt) - To report significant incidents to key cybersecurity entities such as ENISA, EU-CyCLONe, and CSIRTs - It is based on the ISO/IEC27035 - Simple communication channels (email, form) to external organizations coordinating security	- To provide a centralized repository for digital product documentation, including Conformity Assessment Reports, SBOM reports, Vulnerability Disclosure Policies, Incident Reports, and Certifications of Conformity - Simple digital repository for documentation

Table 1: The basic functionality of OSCRAT toolkit.

3. EU initiatives supporting CRA implementation

The section embraces EU projects presented on the Annual Impact event, Brussels, 19 June 2025 organized by CYBERSTAND.eu project members:

<https://cyberstand.eu/events/impacting-cra-defining-standards-future>

<https://cyberstand.eu/sites/default/files/2025-06/Mini%20panels.pdf>

Most of the CRA-related EU-Co-founded projects are supported by ECCC (European Cybersecurity Competence Centre and Network) [https://cybersecurity-centre.europa.eu/about-us_en]. Most of these projects are in the initial state currently – first deliverables have been elaborated, usually they concern identification of user needs and product requirements. This section uses very general information placed on the above-mentioned websites and related.

3.1. CRACoWi – Cyber Resilience Act Compliance Wizard

DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION (2024-2027)

The IoT Security Foundation (IoTSF), non-profit organization,

The CRACoWi project is supported by a consortium of 14 stakeholders from four EU countries, including industrial end-users and technology partners.

<https://www.cracowi.eu/>

<https://www.tiko-pro.eu/success-stories/details/cracowi-digital-europe-project>

Webinar:

<https://iotsecurityfoundation.org/iotsf-webinar-series-cyber-resilience-act-cra-compliance-tool-cracowi/>

The CRACoWi embraces:

- Automated Tools to aid in compliance, reducing the burden on manufacturers,
- Firmware Scanning Tool allowing to generate SBOMs based on binary firmware scan,
- Tools for Vulnerability Assessment helping identification of known vulnerabilities in their digital products,
- Certification Support assisting in the preparing the necessary documentation for certification.
- The CRACoWi supports:

- Secure by Design concept in the product development – products are designed with security as a priority,
- Lifecycle Security concepts in the product development – continuous updates and maintenance are implied to adapt to the changes in the threat environment,
- Compliance Assessments – the rigorous assessment of the product allows to verify compliance with established cybersecurity standards and CRA requirements – difficult and also important especially for SMEs.
- The CRAcoWi tool is able to perform:
- Initial Assessments, i.e. a quick health check on a product's readiness for CRA compliance,
- Documentation Generation, i.e. compiling the required documentation, making the certification process smoother, etc.,
- Continuous Monitoring, i.e. disclosing new vulnerabilities, alerts about potential risks in existing products offered by the manufacturer.

3.2.TrustBoost – Unifying & Upgrading Certification Capabilities Across Europe

EC project: DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION

36 months, 1 September 2024 – 31 August 2027

Co-ordinated by National Standards Authority of Ireland (NSAI)

<https://www.trustboost.eu/>

The TrustBoost (CyberBoost) Platform manages the certification and conformity status of digital products throughout their lifecycle. It is SaaS based and equipped with real-time dashboards aligning with EU regulations like CRA and NIS2.

The TrustBoost project objectives are:

- To improve the overall cybersecurity posture within the EU,
- To align with EU legislation to ensure digital products meet stringent cybersecurity standards.
- To foster a resilient digital ecosystem capable of withstanding cyber threats.

Project members declare that TrustBoost platform “ensures:

- Transparent Evaluations: Clear and open cybersecurity evaluations.
- Streamlined Processes: Simplified certification processes.
- Unified Approach: Bridging gaps between diverse standards and compliance metrics.”

3.3. CRACY – CRA made easy

CRACY is a group of 12 leading European cybersecurity experts, helping SMEs implement CRA.

LSEC – Leaders in Security

<https://cra-cy.eu/>

<https://www.digitalsecuritycatalyst.com/colibri-wp/cracy-cra-made-easy/>

Security tools: sase.cra-cy.eu, test, repo

Compliance tools H2/2025

Guidance: risk management, controls, tooling

CRACY is a group of 12 leading European cybersecurity experts, supporting SMEs in the CRA implementation.

Project team declare CRACY objectives: “Aiming to lower the barriers for small and medium European (SME) engineering companies to be able to facilitate the necessary security requirements for their products with digital elements (PDEs). By making the Cyber Resilience Act (CRA) easy (eACY) to comply with (CRACY), we strive towards reaching a best practice, if not a standard, to which these technology development companies can adopt and obtain a new series of qualified, more secure products and digital services.”

3.4. OCCTET – EU Project Open-Source Compliance Comprehensive Tools and Resources

DIGITAL-ECCC—2024-DEPLOY-CYBER-06

24 months, start date November 2024

<https://occtet.eu/>

The project objective is to develop an open-source toolkit to automate the compliance process for Free and Open-Source Software (FOSS) used in digital products. It is related to the EU initiative aimed at improving cybersecurity and compliance with the CRA for SMEs.

- The developed toolkit is addressed to SMEs and embraces:
- Compliance Checklist
- Conformity Assessment Specifications
- Automated Evaluation Method and Tool
- Federated Database platform for publishing the results of OSS component assessments allowing contributions from various stakeholders
- Inventory of Automatic Dependency Analysis Tools
- Reporting tool.

The OCCTET toolkit helps SMEs to assess cybersecurity risks, manage software dependencies, and generate the required compliance documentation.

Additionally, the project products include:

- Guidance and best practices - to help businesses understand the CRA compliance issue and integrate security into their products and workflows,
- Community and collaboration platform where SMEs, developers, and cybersecurity experts can share knowledge, exchange best practices, and develop common solutions,
- Training and awareness activities, such as webinars, workshops, and guides designed to empower SMEs with the knowledge they need to implement cybersecurity measures efficiently.

Project features:

- Risk based approach,
- Life-cycle consideration,
- Vulnerability management (SBOMs generation and management, vulnerabilities triage - no known vulnerabilities in the product, due diligence when integrating third party open-source components).

3.5. CYBERFORT – Strengthening cyber defences of SMEs for Cyber Resilience Act (CRA) compliance

EC project: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA

Started: 1 December 2024

Co-ordinated by I-ENERGYLINK, partners from Romania and Cyprus

https://www.i-energylink.eu/wp-content/uploads/2025/01/241220_I-LINK-REPRESENTATIVES-ARE-THRILLED-TO-ANNOUNCE-THE-COORDINATION-OF-A-NEW-EUROPEAN-PROJECT-%E2%80%93-CYBERFORT_V01.2.pdf

On the project web site is placed the condensed description of CYBERFORT:

“Key Features and Activities:

Automated Compliance Tools:

CYBERFORT develops free, open-source tools to simplify and automate the process of CRA compliance for SMEs.

Streamlined Documentation:

The project focuses on enhancing the efficiency of compliance documentation processes through automation, reducing the administrative burden on SMEs.

Support Framework:

CYBERFORT establishes a robust support framework, including cascading financing mechanisms, a platform for CRA-related resources, and extensive training and upskilling programs.

Knowledge Sharing:

The project promotes knowledge sharing, standardization, and the exchange of cybersecurity best practices through workshops, hackathons, and conferences.

Financial Support:

CYBERFORT provides financial assistance to SMEs through cascade financing mechanisms, offering targeted support to those implementing the project's recommendations”

3.6. CONFIRMATE – CONFormity assessment, metRics and compliance autoMATion for the cyberresilience act

January 2025 – July 2026

<https://itkam.org/de/projects/confirmate/>

CONFIRMATE project is focused on the work out of a suite of open-source tools supported by additional instruments to automate compliance with CRA, embracing:

- Automation tool for CRA based on open source Clouditor, [<https://www.aisec.fraunhofer.de/en/fields-of-expertise/SAS/Clouditor.html>] to assess essential requirements conformity,
- CRA compliance guide,
- Pen-testing methodology.

The Clouditor is an assurance tool that checks whether cloud-based services and applications are securely configured [<https://www.aisec.fraunhofer.de/en/fields-of-expertise/SAS/Clouditor.html>].

3.7. CURIUM

<https://curium-project.eu/>

The project page presents a vision:

“CURIUM introduces a novel Compliance Continuum – a suite of cybersecurity-oriented tools and services designed to provide information, guidance, trustworthy security testing, and streamlined compliance with the Cyber Resilience Act (CRA).

By simplifying and automating compliance, CURIUM empowers European SMEs – especially micro and small enterprises – to conduct self-assessments, prepare for third-party certification, and reduce costs while accelerating time to market.”

The project team plan to establish a harmonized regulatory framework to enhance cybersecurity across ICT products, services, and processes addressing both: the European Cybersecurity Act (EUCSA) and the Cyber Resilience Act (CRA) requirements.

The Compliance Continuum platform integrates cybersecurity assessment framework that evaluates digital products both individually and within their broader system-wide interconnections (as a part of system).

- The Compliance Continuum provides the following cybersecurity services:
- Cyber Resilience Assessment (CyReA) – Identifies whether a digital product falls under the CRA and determines the required conformity assessment process.
- Digital Product Risk Management (DPRA) – Supports manufacturers in assessing cybersecurity risks across the product lifecycle to proactively minimize security threats.
- Digital Product Maturity Assessment (DPMA) – Offers a structured risk mitigation framework based on product maturity, helping manufacturers implement effective security measures.
- Conformity Assessment & Compliance (CAC) – Provides a guided approach to technical documentation and self-gap analysis, ensuring alignment with CRA requirements.
- Penetration Self-Testing & Vulnerability Assessment (PSTVA) – Equips users with tools for vulnerability assessment, code review, and penetration testing, reinforcing compliance efforts.

3.8. CRA-AI – Cyber Resilience Act Artificial Intelligence

EC project: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA

24 months, start date January 1, 2025

<https://www.cybercertlabs.com/cra-ai/>

<https://www.dnsc.ro/pages/proiect-cra-ai>

Aim: “Highly automated AI-based software platform to support SMEs and micro-enterprises at every stage of their journey to ensure conformity with the provisions of the Cyber Resilience Act.”

The platform will guide these small organisations through the process of obtaining and maintaining the CE Mark, in line with the requirements of the Cyber Resilience Act (CRA).

Manufacturers of digital products should meet cyber security standards, including the essential requirements in Annex 1 and the obligations in Annex 2 of the CRA. Dealing with documentation.

According to the contents of the [<https://www.dnsc.ro/pages/proiect-cra-ai>] the software platform will include features:

- **Product Inventory:** Establishing an inventory of all products, components and/or modules of a product or software, considering the Software Bill of Materials (SBOM). Users may define a Target of Evaluation (ToE) presenting the scope of the CRA assessment.
- **Risk Assessment:** Performing risk assessments considering vulnerabilities.
- **Testing:** User is able to define a full set of test criteria for the product or service. This can include penetration testing, vulnerability management, and secure code reviews.
- **Documentation:** The tool can generate “Information and instructions to the user” as defined in Annex 2 of the CRA. This includes contact information for the manufacturer or distributor, details of the intended use, and a user-friendly explanation of security issues.
- **Assessment:** The software will align to the EUCC scheme and any associated standards that are defined by the scheme. There are two forms of assessment, self-assessment, and conformity assessment. The software will prepare and generate relevant documentation. Also, where a conformity assessment is required, this documentation provides the Conformity Assessment Body (CAB) with all the necessary information to assess the product or service.
- **Monitoring:** The tool is able to monitor the product or service for any vulnerabilities that are discovered after the product or service has been placed on the market.
- **Vulnerability Disclosure:** When vulnerabilities or flaws are discovered in a product or piece of software, other software or product vendors and other parties are alerted to take appropriate action.

There is no clear information about the range of AI implementations yet. There is mentioned that “ ... CRA-AI project will help enterprises ensure that they can do this in a cost effective and robust manner, leveraging the automation capabilities of AI technology to keep costs in check but also to ensure rigor in the process. “

4. Examples of commercial tools

4.1. CRA Readiness Assessment – Cyber Resilience Act Readiness Assessment web application

Cyber Cert Labs, Dublin, Ireland

<https://www.cybercertlabs.com/>

“Our 30-minute Cyber Resilience Act readiness assessment will help your get ahead of the curve.

Price: €199”

The Cyber Cert Labs participates in the EU CRA-AI Cyber Resilience Act Artificial Intelligence project.

The CRA Readiness Assessment is the questionnaires-based tool. It embraces the key questions based on the CRA essential requirements. The tool allows to obtain:

- a comprehensive report for a given digital products strengths and areas of improvement,
- actionable recommendations to enhance CRA preparedness.

Additionally, customers receive a copy of the CRA Guide based on the product development lifecycle elaborated by Cyber Cert Labs.

Figure 1: Screenshot from the Cyber Cert Labs web site

[<https://www.cybercertlabs.com/>]

Some remarks on the tool based on information placed on the Cyber Cert labs web site (demo and documentation are not available to see details):

- There is no detailed information about organization of questionnaires. They are hierarchical ones, or only flat as shown in the picture? Comparing to the

OSCRAT approach they are less detailed. It is important, because the preciseness degree of questionnaires implies the preciseness of reports offered for customers. Diagrams showing progress seems to be hard to interpret unless diagrams are supplemented by detailed reports. OSCRAAT represents a more detailed approach.

- There is no detailed information whether the tool actively supports: SBOMs, vulnerability management, incident handling, documentation management, or does the tool ask the customers how they do this?
- Cyber Cert Labs claims the assessment of the true cost of meeting CRA requirements, which is crucial for product planning. We do not know how the tool support cost analysis. This issue is omitted in the OSCRAAT tool.
- The tool envisages the product life cycle embracing set of manageable actions implied by the CRA. The similar approach is in the OSCRAAT tool implemented.
- The web site offers several articles for developers, manufacturers and distributors as the package of domain knowledge. It should be considered in OSCRAAT as well.

The scope of the support for SMEs is limited to the CRA conformity assessment, providing related knowledge and rising security awareness.

The tool is focused on SMEs needs, especially for smaller entities, helping them to overcome some questions:

- Many SMEs don't have dedicated cybersecurity or compliance specialists – the tool is helpful in this range,
- Assessing the true cost of meeting CRA requirements is crucial for product planning.

The tool facilitates SMEs to place their digital products on the market. Demand on CRA-compliant products will grow.

4.2. The Product Security Platform

Cybellum

Tel Aviv, Israel

<https://cybellum.com/platform/>

<https://cybellum.com/blog/understanding-the-eu-cyber-resilience-act-cra-an-overview/#:~:text=Dedicated%20Product%20Security%20Manager%20Assign%20a%20dedicated,all%20security%20measures%20are%20up%20to%20date.>

The Product Security Platform (demo available on request) includes components:

- Risk Management – to uncover the reality of your product security posture with a centralized dashboard
- Cyber Compliance – to manage and automate the creation of compliance evidence for regulatory requirements such as the FDA PMA (medical devices), ISO 21434 (automotive cybersecurity), EU CRA, own policies and others,
- Assurance & Vulnerability Management
 - to manage risks and vulnerabilities in the product context,
 - to aggregate threat models, fuzz tests, pen tests and vulnerabilities into one unified risk data system,
 - to use AI to triage risks,
- Incident Response – to identify and manage new risks affecting products (postproduction phase),
- Software Licensing – to validate and to enforce of open-source software licensing, minimizing legal risk,
- Asset & SBOM Management (AI supported) – to create and to manage SBOMs and assets for products and their components.

The platform is able to manage assets and risks throughout the entire product lifecycle – from threat models and SBOMs during design and development, to vulnerability management and incident response in pre- and post-production. The triage of risks is supported by AI.

Apart from the Product Security Platform, Cybellum offers the Cyber Digital Twins TTM, allowing to create digital replicas of the product's software used for its analysis.

The Cybellum tools go beyond the CRA compliance checking. They embrace advanced functionalities aiding the digital product development, production and maintenance with respect to cybersecurity.

4.3. Finite State's platform

Columbus, OH, USA

<https://finitestate.io/blog/eu-cra-sbom-technical-documentation-guide>

The American Finite State Company offers the product the Finite State platform and cybersecurity services aligned to the EU CRA.

They focus on:

- the deep analysis of software components (SCA - software composition analysis) and their mutual dependencies on the binary and source code levels, to discover vulnerabilities, licencing problems, outdated versions, etc.,

- the binary, static application security testing (SAST), to uncover additional weaknesses.

The CRA compliance requires generating and maintaining accurate Software Bill of Materials (SBOM) and technical documentation that reflects current vulnerability data. This critical issue is very difficult, especially for SMEs. Finite State company offers its platform to solve this problem.

4.4. Application Security Posture Management Platform (ASPM)

Legit Security

Boston, MA, USA

<https://www.legitsecurity.com/blog/strengthening-software-security-under-eu-cra>

Legit Security offers the Application Security Posture Management (ASPM) platform, which have the following features:

- Software Discovery and Inventory – identification of all aspects of software manufacturer and its security controls to reduce the risk of overlooked vulnerabilities and unprotected assets,
- Prioritization of Security Testing Findings – integration of findings provided by different testing tools, like SAST (static application security testing), SCA (software composition analysis), and DAST (dynamic application security testing),
- Remediation Guidance – removing from finding some issues to fix them,
- Dependency Analysis – mapping dependencies and data flows in software ecosystem to identify potential weak points in application structure, to enforce holistic approach to risks, and to build and maintain a security posture,
- Continuous Monitoring – to detect vulnerabilities, configuration issues, and other risks as they arise.

The ASPM software is focused on the application security and offers the following capabilities:

- Integration with third-party tools – ASPM integrates seamlessly with existing CI/CD pipelines, development tools, and security platforms; it allows to quickly identify how and where applications are being developed as well as security coverage gaps; a CI/CD pipeline is understood as an automated process that streamlines software development by integrating code changes frequently and deploying them reliably; this process consists of the continuous integration (CI) and continuous delivery/deployment (CD); this

approach allows to accelerate software delivery, to improve quality, and to reduce manual errors;

- Sensitive data identification – thanks to the secrets scanning, the ASPM detects exposed secrets across the development environment, reducing the risk of data breaches and unauthorized access;
- Risk-based scoring – thanks to the vulnerabilities' prioritization based on context and potential impact, ASPM helps developers to solve the most critical risks first;
- Compliance reporting – the tool can generate detailed reports tailored to various regulatory standards; it allows to demonstrate compliance and to pass audits;
- Real-time alerts – thanks to the continuous monitoring, the ASPM can provide instant notifications when risks or vulnerabilities are detected; developers can respond quickly and mitigate potential damage;
- Root cause identification and remediation – developers can trace the cause of a vulnerability (or vulnerabilities) to its source, allowing one action to address multiple findings.

American Legit Security recognize an importance of the European CRA preparing its ASPM platform to better support teams in the product development to the European market. The ASPM offers not only the mentioned Compliance reporting tool, but also a unified view of the product security posture. It helps to integrate seamlessly existing tools supporting development process and delivers the automation and AI-driven insights to be resist to threats.

The Legit Security tools allow to be aligned with evolving EU cybersecurity frameworks, like CRA, NIS2 and RED.

4.5. The Embedded Kit

Witekio

The Embedded Kit is a spin off brand of Witekio with development teams in the US, in the UK, France, and Germany.

<https://theembeddedkit.io/blog/cyber-resilience-act-conformity-assessment/>

[Home | Witekio](#)

The Embedded Kit: ready-to-use solutions for Linux devices embracing:

- Welma Yocto Linux for embedded developments,
- Kamea IoT device management,
- Pluma embedded testing,
- CVE Scan vulnerability monitoring.

The Embedded Kit includes this wide range of solutions for developers, very useful in reaching the CRA conformance. The Witekio organization notices the importance of the CRA and provides the CRA-related knowledge and services, e.g. risk analysis, secure by design development, consulting, selecting security solutions, product integration, vulnerability monitoring and patching during the product lifecycle.

5. Background of OSCRAT research and development

The section presents a review summary using the OSCRAT functionality and properties as a reference point for review other tools.

The Table 2 summarizes tools developed within nine EC projects and five selected examples of commercial tools.

The European projects are focused on the CRA and related regulations, i.e. EC members' needs. They embrace conformance assessment tools and minimal support to SBOMs-, vulnerabilities-, incidents- and documentation management. Some tools offer extended possibilities towards the certification process, e.g. CSA-related. The developers' support is limited to the CRA range.

The second group embraces commercial tools broadly supporting developers of digital products – life cycle, security by design, integration CI/CD, testing, services, knowledge, etc. They have no specialized checklists-based tools to assess the CRA conformance, but they offer related services.

First AI-based solutions are met (CRA-AI, ASPM).

Remarks regarding OSCRAT project requirements the following conclusions may be formulated:

1. OSCRAT covers digital products developers' needs with respect to the CRA. The conformance checking tool is very precise and support developers. For discovered non-conformities developers obtain remedy task and hints.
2. Vulnerabilities and incidents are managed according to world-wide standards
3. SBOMs are considered at minimal required level.
4. Identified potential for OSCRAT future development: AI implementation, integration with commercial tools for testing, product integration, risk prioritization, life-cycle management, certification, etc.
5. The most like OSCRAT are: CRAcoWi and CRA-AI projec

Table 2: Identifying the scope of CRA automation tools, outlining its functionalities and limitations. OSC RAT as the reference tool.

Project/tool	Toolkit functionality comparing the OSC RAT tool functionality					Extra functionality and specific features
	Checklists automation	SBOM support	Vulnerability management support	Incident handling process	Documentation on CRA compliance support and management	
OSCRAT	Yes	Yes	Yes	Yes	Yes	Knowledge and best practices for SMEs
CRACoWi	Automated Tools to aid in compliance, including initial assessment	Firmware Scanning Tool allowing to generate SBOMs	Tools for Vulnerability Assessment (known vulnerabilities)	Continuous Monitoring, i.e. disclosing new vulnerabilities, alerts about potential risks in existing products offered by the manufacturer	Certification Support assisting in the preparing the necessary documentation for certification (CRA readiness)	- Secure by Design concept support - Lifecycle Security concepts support - By leveraging artificial intelligence, CRACoWi simplifies the self-assessment and

						certification process for digital products
TrustBoost	- The framework for the accurate identification and categorization of digital products, processes, and services - Real-time dashboards aligning with EU regulations like CRA and NIS2, i.e. CyberBoost SaaS platform					- SaaS platform to manage cybersecurity certification CRA, RED-DA, NIS2, and CSA and interact with stakeholders involved in conformity assessment and certification processes, including NCCAs, CABs (CB and Labs), NABs, ENISA, vendors, CSIRTs, buyers, and companies

					within the scope of NIS2. - Knowledge exchange
CRACY	Compliance tools	Security tools: sase.cra-cy.eu, test, repo			Guidance: risk management, controls, tooling - SMEs support, best practices
OCCTET	- Compliance Checklist - Conformity Assessment Specifications - Automated Evaluation Method and Tool	SBOMs generation and management	Vulnerability management (vulnerabilities triage - no known vulnerabilities in the product, due diligence when integrating third party open-source components)	Reporting tool	- Federated Database platform for publishing the results of OSS component assessments allowing contributions from various stakeholders, - Inventory of Automatic Dependency Analysis Tools - Guidance and best practices

							- Community and collaboration platform for SMEs, developers and experts - Training and awareness activities - Risk based approach, - Life-cycle consideration
CYBERFORT	Compliance Management Software (CMS)					Streamlined Documentation	- Support framework, incl. cascading financing mechanisms, a platform for CRA-related resources, and extensive training and upskilling programs

						- Knowledge Sharing - Financial Support
CONFIRMATE	Automation tool for CRA based on open source Clouditor					- CRA compliance guide - Pen-testing methodology - Trainings modules
CURIUM	- Cyber Resilience Assessment (CyReA) – whether the product falls within the scope of the CRA - Conformity Assessment & Compliance (CAC) – a guided approach to technical documentatio		Digital Product Risk Management (DPRA) - Penetration Self-Testing & Vulnerability Assessment (PSTVA)			It addresses the European Cybersecurity Act (EUCSA) and the Cyber Resilience Act (CRA) requirements - Digital Product Maturity Assessment (DPMA)

	n and self-gap analysis, ensuring alignment with CRA requirements					
CRA-AI		Product Inventory, embracing components, modules and SBOMs where they needed	- Risk Assessment (vulnerabilities , threats, threats modelling) - Monitoring vulnerabilities that are discovered after the product or service has been placed on the market - Vulnerability Disclosure – alerting interested parties about discovered vulnerabilities		Documentation, which generate the required “Information and instructions to the user” (Annex 2 of the CRA).	- Testing - penetration testing, vulnerability management, and secure code reviews - Assessment – aligning to the EUCC scheme and related, allowing the self-assessment and conformity assessment, as well as the information exchange with the CAB

						- Training platform
Examples of commercial projects						
CRA Readiness Assessment of Cyber Cert Labs, Ireland	The CRA Readiness Assessment, a questionnaire s-based tool, embraces the key questions based on the CRA essential requirements				- Comprehensive report for a given digital products strengths and areas of improvement - Actionable recommendations to enhance CRA preparedness	CRA Guide based on the product development lifecycle elaborated by Cyber Cert Labs
Product Security Platform of Cybellum	Cyber Compliance – to manage and automate the creation of compliance evidence for regulatory requirements such as the FDA PMA (medical	Asset & SBOM Management (AI supported) – to create and to manage SBOMs and assets for products and their components	Assurance & Vulnerability Management – integrated, AI-based risk- and vulnerability management,	Incident Response – to identify and manage new risks affecting products (postproduction phase)		- Software Licensing – to validate and to enforce of open-source software licensing, minimizing legal risk - Cybersecurity services

	devices), ISO 21434 (automotive cybersecurity), EU CRA, own policies and others					
Finite State, OH, USA		Advanced tool for the SBOM generating and maintaining	- Advanced tool for a deep software components analysis (SCA) - Advanced tool for the binary, static application security testing (SAST)			Cybersecurity services focused on IoT
Application Security Posture Management Platform (ASPM) of Legit Security, USA	The ASPM includes the Compliance reporting tool to generate detailed reports tailored to various regulatory	Integration with third party tools (CI/CD pipeline)	Risk-based scoring tool allows to prioritize of vulnerabilities –the most critical risks are solved first	The ASPM includes Real-time alerts tool based on a continuous monitoring – instant notifications when risks or	Compliance reporting tool allows to demonstrate compliance and facilitates audits	- Software Discovery and Inventory - Dependency Analysis - Sensitive data identification - Broad range of

	standards, e.g. CRA			vulnerabilities are detected		cybersecurity services
The Embedded Kit, international initiative, Witekio	Services, no dedicated tool	Mainly Kamea IoT device management and Pluma embedded testing	Mainly CVE Scan vulnerability monitoring			- Broad range of cybersecurity services



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 1



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 2

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 2
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

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
State of the art (part 2) provides an overview of the vulnerability and incident reporting methods and formats used by national cybersecurity incident response teams (CSIRTs) and the vulnerability description standard developed by ENISA. The document also presents sample solutions that can be used within the OSCRAT tool to generate SBOM (Software Bill of Material) files. The attached screenshots also show some test cases of these tools to demonstrate their potential use.
Keywords
Product with Digital Elements, SBOM, Software Bill of Materials generation, validation, Vulnerability report, Incident report

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.

Table of contents

1. Vulnerability and incident data preparation	5
1.1. National CERTs reporting forms.....	5
1.2. Incident description	9
1.3. ENISA EUVD – vulnerability description.....	9
1.4. Data required to score the vulnerability	10
2.1. SBOM file formats.....	10
2.2. SBOM generation tools.....	11
2.3. SBOM checking tools.....	14

Figures

<i>Figure 1 Results of SBOM generation command execution in Syft tool</i>	<i>12</i>
<i>Figure 2 Example of SBOM generation command execution in cdxgen (in a server mode on a local machine)</i>	<i>12</i>
<i>Figure 3 Fragment of an SBOM file generated using cdxgen</i>	<i>13</i>
<i>Figure 4 JSON file in SPDX format generated in GitHub.....</i>	<i>14</i>
<i>Figure 5 Sample of a Tirvy vulnerability check report for the SBOM file</i>	<i>15</i>
<i>Figure 6 Screenshot from the vulnerability scan execution in a Bomber tool.....</i>	<i>16</i>
<i>Figure 7 HTML vulnerability scan report performed for the SBOM with Bomber</i>	<i>17</i>
<i>Figure 8 Sample of vulnerability scan report in a text format, generated by gype</i>	<i>18</i>
<i>Figure 9 Sample of vulnerability scan report in a JSON format, generated by gype</i>	<i>18</i>
<i>Figure 10 Screenshot from the vulnerability scan execution in a dependency-check tool.....</i>	<i>19</i>
<i>Figure 11 Sample of HTML vulnerability scan report performed for the SBOM with dependency-check</i>	<i>20</i>

List of Tables

Table 1 Examples of vulnerability and incident description data ranges used by sample European CRISTs.....	6

1. Vulnerability and incident data preparation

1.1. National CERTs reporting forms

The list of available European CSIRTs can be found on a website

<https://github.com/enisaeu/CNW>.

As shown in several examples in the table below, the scope of information in the notification forms is very different in each of the national vulnerability and incident handling units. The main recurring elements are the time of detection and description of the vulnerability/incident, the name and version of the service system (in the case of a vulnerability), the estimated scope, the scope of losses (in the case of an incident), the data of the reporter (optionally for the vulnerability). Reporting does not have to be done via a form, but also via an email inbox, with basic information, which is then analysed by the CERT/CSIRT teams and (if contact details are provided) the whistleblower is contacted for further clarifications and findings.

Table 1 Examples of vulnerability and incident description data ranges used by sample European CRISTs

Country	Vulnerability reporting data	Incident reporting data
Finland www.viestintavirasto.fi	- time of detecting (DD:MM: YYYY, hh:mm) - Description of the vulnerability and its impact - Product version in which you detected the vulnerability - Instructions to reproduce vulnerability - Already contacted party's contact details - Attachments - Notes on the release schedule of the vulnerability and correction - Contact information (if not anonymous)	- Incident type (phishing, DoS attack, malware, data breach, ...), - The notifiers contact information (if not anonymous) - Target organization name - Industry (digital services, food supply, energy, finance, ICT and information security, ...) - The date (time) of notice, start/end time of incident - Description of the issue - What kind of impact did the incident have - Measures taken or planned - URL or other identifying information - Attachments - Has an external information security company been hired to investigate the case? - Has a police report been filed about the incident? - Exchange of information (can be confidentially exchanged with other authorities?) - Do you want a reply?
Estonia www.cert.ee		- Incident beginning (date/time) - What happened and when - Incident end (if not ended, what is the probable end time?) - Impact on information systems (Availability, Integrity, Confidentiality, None, Unknown) - Cause (System failures, Malicious actions, Human errors, Third-party failures, Other, Unknown) - Action plan description - Is help needed with resolving the incident? - Should other authorities notify (Police, Board Guard, Consumer protection and technical regulatory authority) - Attachments

Latvia www.cert.lv cvd.cert.lv	- The resource where the vulnerability has been found - Description of the vulnerability - Steps to re-exploit the vulnerability - the impact of vulnerability - recommended fix - attachments	- Incident's description (in any form) - Has the cause been determined (internal, external, or unknown)? - Services and operating system supported by affected devices - Preserving evidence before resuming operations - Other information that may help resolve or mitigate the incident
Lithuania www.nksc.lt	- System where the vulnerability has been found and/or the vulnerability scan has been performed - Contact data - IP address from which the vulnerability scan was performed - Information about the detected vulnerability and/or the performed vulnerability scan - Have you informed your manager about the discovered security vulnerability?	- Contact details - Incident time - Public key number - Incident's description
Poland www.cert.pl	- Reporter details (optional) - Have you tried contacting the system owner or vendor (what was the response)? - What is the nature of vulnerability? - Additional information (description, e.g. how was the vulnerability discovered, and was it observed during an attack? Is vulnerability publicly known? Are you planning to release vulnerability information publicly? Are you applying for a CVE number?)	- Reporting persons contact data - Contact data of person authorized to make a statement about the incident - Estimated or exact number of people affected by the incident - Estimated or exact time of the incident - Exact date and time of the incident detection - Estimated area affected by the incident - Did the incident impact an essential or digital service offered by another entity? - Established reason for the incident - Impact on information systems of the organization - Incident description in the most minute detail - Is the incident scope international (which EC members affected)? - Response: was there any preventive measure deployed? - What mitigations were deployed. - Attachments

Germany (www.bsi.bund.de)

- Purpose of the report (for BSI only, for mediation with manufacturer, ...)
- Was there an attempt to contact the vendor?
- Vendor name
- Multiple/One vendor is affected?
- Name and version of the product / service
- Does it have an IT security label / BSI certificate?
- Vulnerability category (based on OWASP Top 10)
- How vulnerability was exploited (description)
- Company's data (name, number of employees, industry)
- Reporter's data (name, mail, position in company, PGP key)
- Purpose of the report (notification and further use by BSI, request for a contact/support)
- Time and method of incident detection (system failure, log analysis, information from 3rd parties,)
- In case of many attacks – estimated number
- The method and manner of carrying out the attack
- Type of attack (accidental, targeted at a company/person) and suspected attackers
- The purpose of the attack and damage caused
- Data on the accusation filed, detection of the perpetrator, involvement of external authorities

1.2. Incident description

The incident classification - a manufacturer shall notify any severe incident having an impact on the security of the product

The incident is considered as severe, if any of following applies:

- it negatively affects or is capable of negatively affecting the ability of a product to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions;
- it has led or can lead to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

Information in the notification required within: 24h after detection, 72h after detection, one month after the submission of the incident notification.

- whether the incident is suspected of being caused by unlawful or malicious acts,
- indicate, where applicable, the Member States on the territory ("geographical coverage"?) of which the manufacturer is aware that their product has been made available.
- General information:
 - the nature of the incident,
 - an initial assessment of the incident,
 - any corrective or mitigating measures taken,
 - corrective or mitigating measures that users can take,
 - where applicable, how sensitive the notification information is for the manufacturer.
- detailed description of the incident
 - including its severity and impact,
 - the type of threat or root cause that is likely to have triggered the incident,
 - applied and ongoing mitigation measures.

1.3. ENISA EUVD – vulnerability description

Now, reports are made through national vulnerability reporting points (as mentioned in the previous point). The data in the notification (to be used by ENISA for further analysis) can be derived from the vulnerability description made available on the European Union Vulnerability Database (EUVD) pages and from the API description, made available for the purpose of searching and retrieving vulnerability data from the EUVD database.

The list of vulnerability description fields can be checked, for example, by calling the GET command to search for recent vulnerabilities or exploited vulnerabilities:

- <https://euvdservices.enisa.europa.eu/api/lastvulnerabilities>
- <https://euvdservices.enisa.europa.eu/api/exploitedvulnerabilities>

Extracted fields that could be filled in by the user when submitting a vulnerability to EUVD:

- description
- date of discovery (finding) of the vulnerability
- date of first known exploitation (if already exploited)
- product data
 - name
 - version
- vendor data
 - name

1.4. Data required to score the vulnerability

After reporting the basic vulnerabilities, it is further handled by CERT/CSIRT, where, after establishing contact with the manufacturer of a given product, the problem is analysed, severity is assessed, a unique number is assigned, if any, and publication in public vulnerability databases (such as EUVD). The severity assessment requires an in-depth analysis and is usually carried out according to a scale based on the Common Vulnerability Severity Scoring system.

CVSS (<https://www.first.org/cvss/>) is an open industry standard for assessing the severity level of vulnerabilities in computer systems. The quantitative model provided by CVSS provides a repeatable accurate measurement, allowing users to learn the basic characteristics of the vulnerabilities that were used to generate the results. Two common uses of CVSS are to prioritize remediation for vulnerabilities and to calculate the severity of the threat detected in systems. The standard was developed and is managed by FIRST (The Forum of Incident Response and Security Teams, a non-profit organization whose mission is to support Computer Security Incident Response Teams (CSIRT) around the world. The evaluation system distinguishes 3 groups of measures: Base and supplemental metrics, environmental and Threat metrics, each of which consists of several sets of measures. There is a calculator (<https://www.first.org/cvss/calculator/4-0>) that allows to familiarize yourself with the assessment model and adjust the baseline rating.

In OSCRAT system, the end user will not independently determine the severity of a vulnerability. This task is left to the CSIRT/ENISA, which conducts a thorough vulnerability analysis.

2. Vulnerability check

2.1. SBOM file formats

Software Bill of Material is a list of components, libraries (open-source and third-party) saved in a fixed, specified format. SBOM files contain information about component names and versions and support security management by enabling the analysis of known vulnerabilities of these components and facilitating assessment of the risk associated with the use of the software. The main, commonly used SBOM formats in use are as follows:

1. Software Package Data Exchange (SPDX®)

SPDX is an open-source machine-readable format. It comes from the Linux Foundation Project (<https://spdx.dev>) but was adopted and published as an ISO/IEC 5962 standard.

2. CycloneDX (CDX)

Is an open source machine-readable SBOM format (<https://cyclonedx.org>) developed by the OWASP community. The format is defined by the ECMA standard (European Computer Manufacturers Association) – ECMA-424 CycloneDX Bill of materials specification (<https://ecma-international.org/publications-and-standards/standards/ecma-424>).

There are also other formats for identifying installed software, software components, such as e.g. Software Identification Tagging (SWID). SWID is an older format for software inventory management described by the ISO standard ISO/IEC 19770-2 (<https://www.iso.org/standard/65666.html>). The tags describe installed software using metadata (product name, version, patch level, vendor), without dependency trees or support software supply chain analysis.

2.2. SBOM generation tools

There are some tools already available on the market for generating SBOM files, scanning and finding known vulnerabilities in a software project component. The next subchapter contains a list of several such tools, links to their websites and sources, as well as examples of command line usage that were performed to check and confirm working of these tools.

Syft

(<https://github.com/anchore/syft>)

Syft is a tool for generating a Software Bill of Materials (SBOM) from container images and filesystems. For a project available in a public repository, you can download project locally (e.g. using clone command for a GitHub project) and then generate the SBOM file.

Example of execution:

```
syft dir:. -o spdx-json > sbom.spdx.json
```

```

root@jbaginski:/usr/local/bin/unicis-platform-ce# git clone https://github.com/UnicisTech/unicis-platform-ce
Cloning into 'unicis-platform-ce'...
remote: Enumerating objects: 11110, done.
remote: Counting objects: 100% (3273/3273), done.
remote: Compressing objects: 100% (748/748), done.
remote: Total 11110 (delta 2581), reused 2917 (delta 2441), pack-reused 7837 (from 3)
Receiving objects: 100% (11110/11110), 8.23 MiB | 7.84 MiB/s, done.
Resolving deltas: 100% (7365/7365), done.
root@jbaginski:/usr/local/bin/unicis-platform-ce# syft dir:. -o sdx-json > sbom.sdx.json
✓ Indexed file system
✓ Cataloged contents          cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a8
├── ✓ Packages                [2,856 packages]
├── ✓ Executables             [0 executables]
├── ✓ File digests            [4 files]
└── ✓ File metadata           [4 locations]
[0000] WARN no explicit name and version provided for directory source, deriving artifact ID

```

Figure 1 Results of SBOM generation command execution in Syft tool

CycloneDX / cdxgen

(<https://cyclonedx.github.io/cdxgen/#/>, <https://github.com/CycloneDX/cdxgen>)

The tool for generating SBOMs in CycloneDX specification for most applications and container images, for Linux and Windows hosts.

It can be run in a server mode and listens to port configured port (default is 9090).

The local path scanning can be invoked or scanning a git repository.

```

curl
http://127.0.0.1:9090/sbom?url=https://github.com/UnicisTech/unicis-
platform-ce.git -o /home/jacek/Dokumenty/bom.json

```

```

root@jacek-VirtualBox:~# curl "http://127.0.0.1:9090/sbom?url=https://github.com/UnicisTech/
unicis-platform-ce.git" -o /home/jacek/Dokumenty/bom.json
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 1548k    0 1548k    0     0   358k      0  --:--:--  0:00:04  --:--:--  358k

```

Figure 2 Example of SBOM generation command execution in cdxgen (in a server mode on a local machine)

```

bomFormat: "CycloneDX"
specVersion: "1.6"
serialNumber: "urn:uuid:bc99e9a0-48bc-4297-8185-1c61c1a05ad5"
version: 1
▼ metadata:
  timestamp: "2025-05-26T19:59:05Z"
  ▼ tools:
    ▼ components:
      ▼ 0:
        group: "@cyclonedx"
        name: "cdxgen"
        version: "11.3.1"
        purl: "pkg:npm/%40cyclonedx/cdxgen@11.3.1"
        type: "application"
        bom-ref: "pkg:npm/@cyclonedx/cdxgen@11.3.1"
        publisher: "OWASP Foundation"
        ► authors: [...]
      ► authors: [...]
      ► lifecycles: [...]
    ▼ component:
      name: "unicis-platform"
      group: ""
      version: "0.2.1"
      purl: "pkg:npm/unicis-platform@0.2.1"
      bom-ref: "pkg:npm/unicis-platform@0.2.1"
      type: "application"
      ► properties: [...]
  ▼ components:
    ▼ 0:
      group: "@atlaskit"
      name: "app-provider"
      version: "1.6.1"
      scope: "optional"
      ▼ hashes:
        - A.

```

Figure 3 Fragment of an SBOM file generated using cdxgen

GitHub's SBOM gh CLI extension

(<https://github.com/advanced-security/gh-sbom>)

As it was announced 2 years ago on the GitHub Blog (<https://github.blog/enterprise-software/governance-and-compliance/introducing-self-service-sboms/>) introduction of a new GitHub cloud repository function. The SBOM export function “allows anyone with read access to a GitHub cloud repository to generate an [NTIA](#)-compliant SBOM with a single click. The resulting JSON file saves project dependencies and metadata, like versions and licenses in the industry standard SPDX format.”

Going to the “Insights” tab on a GitHub project’s web site, the user can find “Dependency graph and a button to “Export SBOM” file.

Developers can also generate SBOM using gh CLI extension to programmatically generate SBOMs from repository’s dependency graph. gh is command line interface extension, that helps generate JSON SBOM files in SPDX or CycloneDX format.

Example of execution (in a server mode on a local machine):


```
gh sbom -r "https://github.com/UnicisTech/unicis-platform-ce" >
/root/unicis-platform-ce/tests/gh_sbom2.spdx.json | jq
```

```
SPDXID: "SPDXRef-DOCUMENT"
  creationInfo:
    created: "2025-06-02T05:23:07Z"
    creators:
      0: "Tool: protobom-v0.0.0-20250530160405-7c0c18742702+dirty"
      1: "Tool: GitHub.com-Dependency-Graph"
    dataLicense: "CC0-1.0"
    documentNamespace: "https://spdx.org/spdxdocs/protobom/ae56b9d-2ee4-47a5-a86a-b3fc5a898a07"
    name: "com.github.UnicisTech/unicis-platform-ce"
  packages:
    0:
      SPDXID: "SPDXRef-npm-unist-util-remove-position-5.0.0-848eld"
      copyrightText: "(c) Titus Wormer, Copyright (c) 2016 Titus Wormer <tituswormer@gmail.com>"
      downloadLocation: "NOASSERTION"
      externalRefs:
        0:
          referenceCategory: "PACKAGE-MANAGER"
          referenceLocator: "pkg:npm/unist-util-remove-position@5.0.0"
          referenceType: "purl"
          filesAnalyzed: false
          licenseConcluded: "MIT"
          name: "unist-util-remove-position"
          versionInfo: "5.0.0"
      1: { SPDXID: "SPDXRef-npm-cookies-next-4.2.1-5f5617", copyrightText: "Copyright (c) 2019 Andrei Zanolvskii", downloadLocation: "NOASSERTION", ... }
      2: { SPDXID: "SPDXRef-npm-preact-10.22.0-6412be", copyrightText: "Copyright (c) 2015-present Jason Miller", downloadLocation: "NOASSERTION", ... }
      3: { SPDXID: "SPDXRef-npm-types-tough-cookie-4.0.5-3f1327", copyrightText: "Copyright (c) Microsoft Corporation", downloadLocation: "NOASSERTION", ... }
      4: { SPDXID: "SPDXRef-npm-neo-async-2.6.2-f098d9", copyrightText: "Copyright (c) 2014-2018 Suguru Motegi, Copyright Caolan McMahon", downloadLocation: "NOASSERTION", ... }
      5: { SPDXID: "SPDXRef-npm-types-webidl-conversions-7.0.3-1cdc24", copyrightText: "Copyright (c) Microsoft Corporation", downloadLocation: "NOASSERTION", ... }
      6: { SPDXID: "SPDXRef-npm-webassemblyjs-utf8-1.13.2-86e837", copyrightText: "Copyright (c) 2018 Sven Sauleau <sven@sauleau.com>", downloadLocation: "NOASSERTION", ... }
```

Figure 4 JSON file in SPDX format generated in GitHub

2.3. SBOM checking tools

This chapter presents examples of tools supporting vulnerability detection in a software project based on generated SBOM (Software Bill of Materials) files.

Details on how to use the tool (installation, execution) can be found on the project pages (in the GitHub repositories). However, the following are also examples of calls to each and examples of the results generated using them.

The EUVD database should ultimately be the main source of vulnerability information for use when scanning known vulnerabilities based on SBOM files. But since currently available SBOM scanning tools do not yet include EUVD, SBOM scanning function in OSCRAT may use existing vulnerability databases.

Scanning tools presents the results with different format that can be presented to the user (e.g. PDF, HTML) when the scan is finished.

The OSCRAT user should have the possibility to specify the path to the online repository or import the SBOM file to the OSCRAT and then, to call the scanning function.

Trivy

(<https://trivy.dev/latest/>, <https://github.com/aquasecurity/trivy>)

According to the information provided on ENISA's website (europa.europa.eu/faq), EUVD builds upon the OASIS Common Security Advisory Framework to support automation in the processing, production and distribution of security advisories.

CSAF, as stated on the website (www.csaf.io) is a language to exchange security advisories and allows stakeholders to automate the creation, consumption of security vulnerability information and remediation.

On the CSAF website, the Trivy tool is mentioned among the set of vulnerability handling tools,

Depending on the version of the operating system and software components, Trivy can use different sources of information about weaknesses, vulnerabilities, as listed on the project website: <https://trivy.dev/latest/docs/scanner/vulnerability/>.

The results are available in different formats, e.g. a table mode (formatted text), JSON file, Static Analysis Results Interchange Format (SARIF, <https://docs.oasis-open.org/sarif/sarif/v2.1.0/sarif-v2.1.0.html>), custom template that can be loaded from a file.

Example of execution:

```
trivy sbom "SBOM_Name.spdx.json" --output "Report_name.txt"
```

=====

Total: 16 (UNKNOWN: 0, LOW: 0, MEDIUM: 13, HIGH: 2, CRITICAL: 1)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
stdlib	CVE-2024-24790	CRITICAL	fixed	1.20.12	1.21.11, 1.22.4	golang: net/netip: Unexpected behavior from Is methods for IPv4-mapped IPv6 addresses https://avd.aquasec.com/nvd/cve-2024-24790
	CVE-2023-45288	HIGH			1.21.9, 1.22.2	golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS https://avd.aquasec.com/nvd/cve-2023-45288
	CVE-2024-34156				1.22.7, 1.23.1	encoding/gob: golang: Calling Decoder.Decode on a message which contains deeply nested structures... https://avd.aquasec.com/nvd/cve-2024-34156
	CVE-2023-45289	MEDIUM			1.21.8, 1.22.1	golang: net/http/cookiejar: incorrect forwarding of sensitive headers and cookies on HTTP redirect... https://avd.aquasec.com/nvd/cve-2023-45289
	CVE-2023-45290					golang: net/http: golang: mime/multipart: golang: net/textproto: memory exhaustion in Request.ParseMultipartForm https://avd.aquasec.com/nvd/cve-2023-45290
	CVE-2024-24783					golang: crypto/x509: Verify panics on certificates with an unknown public key algorithm... https://avd.aquasec.com/nvd/cve-2024-24783
	CVE-2024-24784					golang: net/mail: comments in display names are incorrectly handled https://avd.aquasec.com/nvd/cve-2024-24784
	CVE-2024-24785					golang: html/template: errors returned from MarshalJSON

Figure 5 Sample of a Trivy vulnerability check report for the SBOM file

Bomber

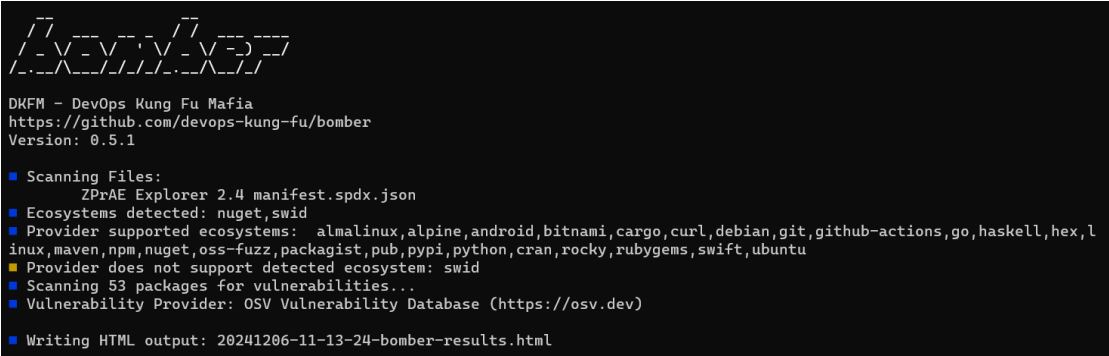
(<https://github.com/devops-kung-fu/bomber>)

The tool includes [OSV](#) database as default vulnerabilities' information provider to scan, but declares that also other databases can be used, such as [Github Advisory Database](#), [Sonatype OSS Index](#), or [Snyk](#).

In addition to standard output (stdout), the tool also provides results in HTML and JSON formats.

Example of execution:

```
bomber.exe scan --output html "SBOM_Name.json"
```



```

  /--V-V-V-V-V--/
 /--X--X--X--X--X--/

DKFM - DevOps Kung Fu Mafia
https://github.com/devops-kung-fu/bomber
Version: 0.5.1

■ Scanning Files:
  ZPrAE Explorer 2.4 manifest.spdx.json
■ Ecosystems detected: nuget,swid
■ Provider supported ecosystems: almalinux,alpine,android,bitnami,cargo,curl,debian,git,github-actions,go,haskell,hex,l
  inux,maven,npm,nuget,oss-fuzz,packagist,pub,pypi,python,cran,rocky,rubygems,swift,ubuntu
■ Provider does not support detected ecosystem: swid
■ Scanning 53 packages for vulnerabilities...
■ Vulnerability Provider: OSV Vulnerability Database (https://osv.dev)

■ Writing HTML output: 20241206-11-13-24-bomber-results.html
```

Figure 6 Screenshot from the vulnerability scan execution in a Bomber tool



The following results were detected by `bomber 0.5.1` on 2024-12-06 11:03:44.3242714 +0100 CET m=+1.722158401 using the osv provider.

Vulnerabilities displayed may differ from provider to provider. This list may not contain all possible vulnerabilities. Please try the other providers that `bomber` supports (osv, github, ossindex, snyk). There is no guarantee that the next time you scan for vulnerabilities that there won't be more, or less of them. Threats are continuous.

EPSS Percentage indicates the % chance that the vulnerability will be exploited. This value will assist in prioritizing remediation. For more information on EPSS, refer to <https://www.first.org/epss/>.

Scanned Files

ZPrAE Explorer 2.4 manifest.spdx.json (sha256:8615d482a92ba54f89919f10aaa989363e44dbaac0c49c6c03b63bbeea5dd571)

No license information detected.

Vulnerability Summary

Critical: 1

Vulnerability Details

pkg:nuget/log4net@2.0.5

Vulnerabilities

XML External Entity attack in log4net

Severity: **CRITICAL**

[Reference Documentation](#)

Apache log4net before 2.0.10 does not disable XML external entities when parsing log4net configuration files. This could allow for XXE-based attacks in applications that accept arbitrary configuration files from users.



Powered by the [DevOps Kung Fu Mafia](#)

Figure 7 HTML vulnerability scan report performed for the SBOM with Bomber

Grype

(<https://github.com/anchore/grype>)

Grype performs vulnerability scanning using a vulnerability database. The database is prepared by pulling data from a variety of publicly available vulnerability data sources. These sources include Amazon Linux (ALAS), GitHub Security Advisories (GHSAs), National Vulnerability Database (NVD), Oracle Linux (OVAL), and others, as listed on the Grype project's GitHub website.

The output format includes table, XML, JSON, Static Analysis Results Interchange Format (SARIF), user specified custom templates.

Example of execution:

```
grype sbom:sbom-spdx.json -o table --file "sbom-check-result.txt"
```

✓ Scanned for vulnerabilities [43 vulnerability matches]

by severity: 6 critical, 13 high, 18 medium, 6 low, 0 negligible
 by status: 42 fixed, 1 not-fixed, 0 ignored

NAME	INSTALLED	FIXED-IN	TYPE	VULNERABILITY	SEVERITY
@babel/helpers	7.24.7	7.26.10	npm	GHSA-968p-4wvh-cqc8	Medium
@babel/runtime	7.24.7	7.26.10	npm	GHSA-968p-4wvh-cqc8	Medium
@babel/runtime-corejs2	7.24.7	7.26.10	npm	GHSA-968p-4wvh-cqc8	Medium
axios	1.7.2	1.8.2	npm	GHSA-jr5f-v2jv-69x6	High
axios	1.7.2	1.7.4	npm	GHSA-8hc4-vh64-cxmj	High
axios	1.7.9	1.8.2	npm	GHSA-jr5f-v2jv-69x6	High
cookie	0.4.2	0.7.0	npm	GHSA-pxg6-pf52-xh8x	Low
cookie	0.5.0	0.7.0	npm	GHSA-pxg6-pf52-xh8x	Low
cookie	0.6.0	0.7.0	npm	GHSA-pxg6-pf52-xh8x	Low
esbuild	0.19.11	0.25.0	npm	GHSA-67mh-4wv8-2f99	Medium
formidable	3.5.1	3.5.3	npm	GHSA-75v8-2h7p-7m2m	Low
multer	1.4.5-lts.1	2.0.0	npm	GHSA-4pg4-qvpc-4q3h	High
multer	1.4.5-lts.1	2.0.0	npm	GHSA-44fp-w29j-9vj5	High
next	14.1.4	14.2.25	npm	GHSA-f82v-jwr5-mffw	Critical
next	14.1.4	14.2.10	npm	GHSA-gp8f-8m3g-qvj9	High
next	14.1.4	14.2.15	npm	GHSA-7gfc-8cq8-jh5f	High
next	14.1.4	14.2.7	npm	GHSA-g77x-44xx-532m	Medium
next	14.1.4	14.2.21	npm	GHSA-7m27-7ghc-44w9	Medium
next	14.1.4	14.2.24	npm	GHSA-qpjv-v59x-3qc4	Low
next	14.2.25	14.2.26	npm	GHSA-223j-4rm8-mrmf	Low
prismjs	1.29.0	1.30.0	npm	GHSA-x7hr-w5r2-h6wg	Medium
quill	1.3.7		npm	GHSA-4943-9vgg-gr5r	Medium

Figure 8 Sample of vulnerability scan report in a text format, generated by gype

```
{
  "matches": [
    {
      "vulnerability": {
        "id": "GHSA-968p-4wvh-cqc8",
        "dataSource": "https://github.com/advisories/GHSA-968p-4wvh-cqc8",
        "namespace": "github:language:javascript",
        "severity": "Medium",
        "urls": [
          "https://github.com/advisories/GHSA-968p-4wvh-cqc8"
        ]
      },
      "description": "Babel has inefficient RegExp complexity in generated code with .replace when transpiling named capturing groups",
      "cvss": {
        {
          "version": "3.1",
          "vector": "CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
          "metrics": {
            "baseScore": 6.2,
            "exploitabilityScore": 2.5,
            "impactScore": 3.6
          },
          "vendorMetadata": {
            "base_severity": "Medium",
            "status": "N/A"
          }
        }
      },
      "fix": {
        "versions": [
          "7.26.10"
        ],
        "state": "fixed"
      },
      "advisories": []
    },
    {
      "relatedVulnerabilities": [
        {
          "id": "CVE-2025-27789",
          "dataSource": "https://nvd.nist.gov/vuln/detail/CVE-2025-27789",
          "namespace": "nvd:cpe",
          "severity": "Medium",
          "urls": [
            "https://github.com/babel/babel/pull/17173",
            "https://github.com/babel/babel/security/advisories/GHSA-968p-4wvh-cqc8"
          ]
        }
      ]
    }
  ]
}
```

Figure 9 Sample of vulnerability scan report in a JSON format, generated by gype

OWASP Dependency-check

(<https://github.com/dependency-check/DependencyCheck>)

The tool uses the NVD API. Users are encouraged to obtain an NVD API Key, otherwise NVD API Key dependency-check's updates will be very slow. The tool requires access to externally hosted resources like NVD Database, CISA Known Exploited Vulnerabilities, Retire JS Repository, and others (listed on a GitHub website (<https://dependency-check.github.io/DependencyCheck/data/index.html>)).

The report is presented as an HTML file.

Command line execution:

```
./bin/dependency-check.sh --scan "SBOM_Name.json" --format HTML --out /mnt/share/
```

Results:

Lack of identified dependencies and vulnerabilities. The problem may be that the tool does not correctly recognize the file format that was not generated by the tool..

```
root@jbaginski:/home/jbaginski/OWASP/dependency-check/dependency-check# ./bin/dependency-check.sh --scan "/mnt/share/ZPrAE Explorer 2.4 manifest.spdx.json" --format HTML --o
ut /mnt/share/
[INFO] Checking for updates
[WARN] An NVD API Key was not provided - it is highly recommended to use an NVD API key as the update can take a VERY long time without an API Key
[INFO] NVD API has 34 records in this update
[INFO] Downloaded 34/34 (100%)
[INFO] Completed processing batch 1/1 (100%) in 319ms
[INFO] Skipping Known Exploited Vulnerabilities update check since last check was within 24 hours.
[INFO] Begin database defrag
[INFO] End database defrag (11747 ms)
[INFO] Check for updates complete (19823 ms)
[INFO]

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed
by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard
to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any dama
ges whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

About ODC: https://jeremylong.github.io/DependencyCheck/general/internals.html
False Positives: https://jeremylong.github.io/DependencyCheck/general/suppression.html

♥ Sponsor: https://github.com/sponsors/jeremylong

[INFO] Analysis Started
[INFO] Finished File Name Analyzer (0 seconds)
[INFO] Finished Dependency Merging Analyzer (0 seconds)
[INFO] Finished Hint Analyzer (0 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
[INFO] Created CPE Index (3 seconds)
[INFO] Finished CPE Analyzer (3 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[INFO] Finished Sonatype OSS Index Analyzer (0 seconds)
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
[INFO] Finished Known Exploited Vulnerability Analyzer (0 seconds)
[INFO] Finished Dependency Bundling Analyzer (0 seconds)
[INFO] Finished Unused Suppression Rule Analyzer (0 seconds)
[INFO] Analysis Complete (3 seconds)
[INFO] Writing HTML report to: /mnt/share/dependency-check-report.html
root@jbaginski:/home/jbaginski/OWASP/dependency-check/dependency-check#
```

Figure 10 Screenshot from the vulnerability scan execution in a dependency-check tool



DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

 [Sponsor](#)

Project:

Scan Information ([show all](#)):

- *dependency-check version*: 11.1.1
- *Report Generated On*: Sun, 8 Dec 2024 18:33:02 +0100
- *Dependencies Scanned*: 0 (0 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count

Dependencies (vulnerable)

This report contains data retrieved from the [National Vulnerability Database](#).
 This report may contain data retrieved from the [CISA Known Exploited Vulnerability Catalog](#).
 This report may contain data retrieved from the [Github Advisory Database \(via NPM Audit API\)](#).
 This report may contain data retrieved from [RetireJS](#).
 This report may contain data retrieved from the [Sonatype OSS Index](#).

Figure 11 *Sample of HTML vulnerability scan report performed for the SBOM with dependency-check*



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 2



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 3

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 3
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

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
Tasks from scrum platform - system functionality details for developers
Keywords
system functionality, incident management, vulnerability management, tasks, workflow, users' management, product management, organization management, assessment process, documentation, workflow, SBOM, development

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.

Table of contents

1.	Task #307 - Implement Applicability Check for CRA (Unregistered User)	5
2.	Task #309 - Implement Account Creation Flow for Unregistered Users.....	6
3.	Task #310 - Enable Logged-In Users to Create a New Organization	7
4.	Task #311 - Enable Users to Add a New Product	8
5.	Task #312 - CRA Compliance Assessment for a Product Version.....	10
6.	Task #314 - Product CRA Compliance Assessment Questionnaire Template Administration & Import Mechanism.....	11
7.	Task #315 - Product CRA Compliance Dashboard, Visualization & PDF Export.....	11
8.	Task #316 - Organization CRA Compliance Assessment Questionnaire Template Administration & Import Mechanism	12
9.	Task #317 - CRA Process Assessment for an Organization.....	13
10.	Task #318 - Organization CRA Compliance Dashboard, Visualization & PDF Export.....	13
11.	Task #319 - Product Details Page.....	15
12.	Task #320 - Product Version Details Page.....	15
13.	Task #321 - Vulnerability Details Page	16
14.	Task #322 - Incident Details Page.....	17
15.	Task #323 - Add New Product Version	19
16.	Task #324 - Add New Vulnerability.....	19
17.	Task #325 - Add New Incident	20
18.	Task #326 - Edit Vulnerability.....	21
19.	Task #327 - Edit Incident	22
20.	Task #328 - SBOM Management	24
21.	Task #336 - Requirements Evaluation – Automatic Task Generation new....	26

1. Task #307 - Implement Applicability Check for CRA (Unregistered User)

Overview

From the landing page, unregistered users should be able to perform an applicability check to determine whether their product falls under the scope of the **Cyber Resilience Act (CRA)**.

UI Design References

- **Landing Page UI:** [Figma - Landing Page](#)
- **Applicability Check Flow UI:** [Figma - CRA Applicability Check](#) (Two of the columns - *Hint for the user* and *Reference* - are currently not applied in the mockups. They should be added as static text for the hint and url link for the reference.)
- Relevant mockups: *CRA_Applicability_1.1* to *CRA_Applicability_1.15*

Functionality Description

1. Accessing the Applicability Check

- From the landing page, clicking the “**Applicability Check**” button should open the **CRA Applicability Check** page.
- Users are guided through a series of questions designed to assess product applicability under the CRA.

2. Questionnaire Logic

- The content of the questions and answers is defined in the Excel file [Source File](#) (Sheet: *CL_Exclusion*, Columns: *Question* and *Answer*):

3. Outcome Paths

Based on the user’s responses, the flow ends in one of two outcomes:

- **Product is Eligible**
 - UI Reference: [Figma - CRA Applicability Check](#) mockup *CRA_Applicability_2.1*
 - Additionally, if the product is eligible, a classification is applied:
 - **Critical**
 - **Important – Class I**
 - **Important – Class II**
 - **Other**
 - This classification is displayed on the eligibility result page.
 - Logic reference: [Source File](#) (Sheet: *CL_Exclusion*, Column: *Scope of CRA application*)
- **Product is Not Eligible**
 - UI Reference: [Figma - CRA Applicability Check](#) *CRA_Applicability_2.2*
 - If a specific answer determines ineligibility, the questionnaire is interrupted, and the user is redirected to the ineligible outcome page.

- Logic reference: [Source File](#) (Sheet: *CL_Exclusion*, Column: *OSCRAT tool reaction depending on the answer*)

User Session and Registration Handling

- Once an unregistered user completes a **positive applicability check**, they can proceed to **register and log in** to the platform.
- The product data gathered from the questionnaire should be retained and made accessible to the user postlogin.
- **Session management** must be implemented to temporarily store this data.
- If multiple applicability checks are performed before registration, **only the latest eligible result** should be saved and accessible after login.

2. Task #309 - Implement Account Creation Flow for Unregistered Users

Overview

Unregistered users should be able to create an account directly from the landing page in order to gain access to the platform.

Design Reference

- **Landing Page UI:** [Figma - Landing Page](#)

Functionality Description

1. Navigation

- From the landing page, clicking the **“Create a free account”** link should open the **“Create a new account”** page.

2. User Input Fields

On the **“Create a new account”** page, users must provide the following basic information:

- **First Name** – User’s first name
- **Last Name** – User’s last name
- **Email** – User’s email address
- **Password** – User’s chosen password

3. Organization Type Selection

- Users must choose between two types of registrants:
- **Natural Person**
- **Legal Person**
- Presented as two radio buttons
- Source: [Reference File](#), Sheet: *2_CL_Organization*, Question 2.1

4. Conditional Fields Based on Selection

- If **“Legal Person”** is selected, the following additional fields must be displayed:
- **Organization Name** – Required
- **Organization Role** – radio button selection: Manufacturer, Authorized representative, Open-source software steward, Importer, Distributor

Source: [Reference File](#), Sheet [2_CL_Organization](#), Question 2.3

- **Tax ID** – Optional field
- **Organization Size** – Four radio buttons: *Micro, Small, Medium, Other*

Source: [Reference File](#), Sheet [2_CL_Organization](#), Question 2.2

- **Contact Data** – Three separate fields: *Postal Address, Email, Phone*
- **Additional Information / Notes** – A large free-text field
- If **"Natural Person"** is selected:
- **Organization Name** – Required

- **Organization Role** – radio button selection: Manufacturer, Authorized representative, Open-source software steward, Importer, Distributor

Source: [Reference File](#), Sheet [2_CL_Organization](#), Question 2.3

- **Contact Data** - Three input fields: *Postal Address, Email, Phone*
- **Additional Information / Notes** - One large free-text field

Notes for Implementation

- Form validation should ensure all required fields are completed before submission.
- Conditional rendering of fields must work dynamically based on the user's selection of registrant type.

3. Task #310 - Enable Logged-In Users to Create a New Organization

Overview

A logged-in user should be able to create a new organization within the platform. Upon creation, the user is automatically added as a member of that organization.

Design Reference

- **UI Reference:** [Figma - Organization Selector](#)

Functionality Description

1. Accessing the Feature

- From the **Organization dropdown** located in the upper-left corner of the application, the user selects **"Create a new Organization."**
- This action opens the **"Create a New Organization"** page.

2. Organization Type Selection

- Users must select the type of organization:
- **Natural Person**
- **Legal Person**
- Displayed as two radio buttons.
- Source: [Reference File](#), Sheet: [2_CL_Organization](#), Question 2.1

3. Conditional Fields Based on Type

- If **"Legal Person"** is selected, the following fields are displayed:
 - i. **Organization Name** – Required

ii. **Organization Role** – radio button selection: Manufacturer, Authorized representative, Open-source software steward, Importer, Distributor

Source: [Reference File](#), Sheet [2_CL_Organization](#), Question 2.3

iii. **Tax ID** – Optional

iv. **Organization Size** – Four radio buttons: *Micro*, *Small*, *Medium*, *Other*

Source: [Reference File](#) Sheet [2_CL_Organization](#), Question 2.2

v. **Contact Data** – Three input fields: *Postal Address*, *Email*, *Phone*

vi. **Additional Information / Notes** – One large free-text field

- If "Natural Person" is selected:

- **Organization Name** – Required

- **Organization Role** – radio button selection: Manufacturer, Authorized representative, Open-source software steward, Importer, Distributor

Source: [Reference File](#), Sheet [2_CL_Organization](#), Question 2.3

- **Contact Data** - Three input fields: *Postal Address*, *Email*, *Phone*

- **Additional Information / Notes** - One large free-text field

4. Post-Creation Behavior

- Once the form is submitted successfully, the user is automatically:

- Added as a **member** of the new organization.

- Switched to the context of the newly created organization (if applicable in UI flow).

Notes for Implementation

- The organization creation form must validate all required fields before submission.

- The UI must dynamically render additional fields based on the selected organization type.

4. Task #311 - Enable Users to Add a New Product

Overview

From the **Products** page, a logged-in user should be able to add a new product to their current organization.

The “**Add new product**” button opens a dialog that allows the user to choose one of three ways to add a product:

1. From Scratch

2. From Cache (Applicability Check results)

3. From Existing Product

1. Add a New Product from Scratch

- The user selects “**Add a new product from scratch**”.

- The system displays an empty form with:

- applicability check

- product fields

- The user fills in the fields and clicks “**Save**”.

- There is no hard constraint for the product in regards to the **current organization's role**. However, there should be a text warning / hint, which helps the user to add only appropriate products into the current organization. If the product is not applicable for the **current organization's role**, the user should be advised to switch to or create another organization and then add the desired product.

Fields:

- Product Acronym / Short Name (*required, short text*)
- Product Full Name (*required, short text*)
- Product Version (*required, short text*)
- Product Short Description (*optional, long text*)

2. Add a New Product from Cache

- The user selects **"Add a new product from the cache"**.
- The system displays a form pre-populated with data retained from the **CRA**

Applicability Check for unregistered users.

- The user reviews the fields and clicks **"Save"**.
- There is no hard constraint for the product in regards to the **current organization's role**. However, there should be a text warning / hint, which helps the user to add only appropriate products into the current organization. If the product is not applicable for the **current organization's role**, the user should be advised to switch to or create another organization and then add the desired product.

Fields:

- Product Acronym / Short Name (*required, short text*)
- Product Full Name (*required, short text*)
- Product Version (*required, short text*)
- Product Short Description (*optional, long text*)

3. Add a New Product from an Existing Product

- The user selects **"Add a new product by loading an existing product"**.
- The system displays a form pre-populated with:
 - data from the a previously created product's applicability check
 - data from a previously created product.
- The user reviews and optionally edits the fields, then clicks **"Save"**.
- There is no hard constraint for the product in regards to the **current organization's role**. However, there should be a text warning / hint, which helps the user to add only appropriate products into the current organization. If the product is not applicable for the **current organization's role**, the user should be advised to switch to or create another organization and then add the desired product.

Fields:

- Product Acronym / Short Name (*required, short text*)
- Product Full Name (*required, short text*)
- Product Version (*required, short text*)
- Product Short Description (*optional, long text*)

Notes for Implementation

- Use consistent **form validation** and error handling (required fields must be completed).
- Cache data should only be available if the user has previously completed an **Applicability Check**.
- In all three cases, an obligatory **Applicability Check** should be in place.
- When cloning an existing product, ensure that unique identifiers (like acronym/version) can be modified to avoid duplicates.

5. Task #312 - CRA Compliance Assessment for a Product Version

Overview

When a new product version is added or when a new product is added (and applicability check is passed), the system should automatically initiate a CRA Compliance Assessment questionnaire. This ensures that the product version undergoes a structured self-assessment process to determine its compliance with the Cyber Resilience Act (CRA).

Structure

- **Area of Requirements** (top level)
- **Requirement** (per area)
- **Question** (per requirement)

Organization Role-Specific Questionnaires

- Manufacturer → Sheet 3b_ESR – product assessment
- Importer → Sheet 4b_cl - product assessment
- Distributor → Sheet 5b_CL - product assessment
- Open-source steward → no questionnaire
- Authorized representative → Sheet 7b_CL - product assessment

Self-Assessment Flow

For each Requirement, the user must perform a self-assessment by answering related questions. At the end of each requirement, the user selects one of four compliance statuses:

Status Action

Fully Compliant Requirement task closed — no further action

Partially Compliant User may create a new manual follow-up task

Status Action

Not Compliant

An automatic task is generated by the platform; the user can accept or reject it (with option to create manual task)

Not Applicable Requirement excluded

References:

- Source spreadsheet: [CRA Requirements Spreadsheet](#)
- Reference diagram: [Organization Role Mapping](#)
- Reference diagram: [Compliance Flow](#)

6. Task #314 - Product CRA Compliance Assessment Questionnaire Template Administration & Import Mechanism

Overview

Questionnaires must not be hardcoded; they should be updatable over time via an import mechanism. A template definition and import process must be developed to allow for updates without code changes.

Requirements

- Define a **questionnaire template** (JSON or another standard structured format).
- Template structure should mirror the CRA Requirements Spreadsheet.
- Provide an **admin-friendly mechanism** to upload/import new questionnaires.
- Do not support **version control** for questionnaires (track changes over time).
- Ensure the platform correctly loads role-based questionnaires at runtime.

References:

- CRA Requirements Spreadsheet: [CRA Requirements Spreadsheet](#)
- Organization Role Mapping diagram: [Organization Role Mapping](#)

7. Task #315 - Product CRA Compliance Dashboard, Visualization & PDF Export

Overview

The system must provide a dynamic dashboard view summarizing compliance progress for each product assessment. This dashboard must include a status table, charts, a progress bar, and export to PDF.

Dashboard Components

1. Status Table

A table listing all requirements, their evaluation status, and conformity results.

Columns:

- Requirement Identifier
- Requirement Name
- Requirement Status → Evaluated / Not Evaluated
- Conformity Status → Compliant, Partially Compliant, Not Compliant, In Evaluation (e.g., 33%), or Not Applicable

Sample Table:

Security Requirement Requirement Status Conformity Status

ES01 Secure Product Design Evaluated Partially Compliant

ES02 Secure Development Practices Evaluated Not Compliant

ES03 Outsourced Development Evaluated Compliant

ES04 Security Testing and Vulnerability Remediation Not Evaluated In Evaluation [33%]

ES05 Third-party Component and Supply Chain Management Evaluated Not Applicable

Progress computation formula: average of answered questions for the requirement (e.g., 1 of 3 answered → 33%).

2. Pie Charts

• Chart A:

- Evaluated vs. Not Evaluated (count of requirements)
- Breakdown of Compliant / Partially Compliant / Not Compliant / Not Applicable

• Chart B:

- Task distribution by type & status (e.g., auto-generated, manual, closed)

3. Progress Bar

- Computed as the arithmetic average of all requirements:
- *Evaluated requirements* → 100%
- *Not Evaluated requirements* → use their completion percentage (e.g., 33%).

4. Export Conformity Assessment Report

- The **dashboard must be exportable as a PDF file**, including:
- Product and organization identifiers
- Status table, questions and given answers (with rationales if added)
- Charts
- Progress bar
- Timestamp of export

Reference: [Dashboard Status Section](#)

8. Task #316 - Organization CRA Compliance Assessment Questionnaire Template Administration & Import Mechanism

Overview

Questionnaires must not be hardcoded; they should be updatable over time via an import mechanism. A template definition and import process must be developed to allow for updates without code changes.

Requirements

- Define a **questionnaire template** (JSON or another standard structured format).
- Template structure should mirror the CRA Requirements Spreadsheet.
- Provide an **admin-friendly mechanism** to upload/import new questionnaires.
- Do not support **version control** for questionnaires (track changes over time).
- Ensure the platform correctly loads role-based questionnaires at runtime.

References:

- CRA Requirements Spreadsheet: [CRA Requirements Spreadsheet](#)
- Organization Role Mapping diagram: [Organization Role Mapping](#)

9. Task #317 - CRA Process Assessment for an Organization

Overview

When a new organization is added, the system should automatically initiate a CRA Organizational Process Assessment questionnaire. This ensures that the organization undergoes a structured self-assessment process to determine its compliance with the Cyber Resilience Act (CRA).

Structure

- **Area of Requirements** (top level)
- **Requirement** (per area)
- **Question** (per requirement)

Organization Role-Specific Questionnaires

- Manufacturer → Sheet 3a_ESR - organization assessment
- Importer → Sheet 4a_cl - organization assessment
- Distributor → Sheet 5a_CL - organization assessment
- Open-source steward → Sheet 6a_CL - organization assessment
- Authorized representative → Sheet 7a_CL - organization assessment

Self-Assessment Flow

For each Requirement, the user must perform a self-assessment by answering related questions. At the end of each requirement, the user selects one of four compliance statuses:

Status Action

Fully Compliant Requirement task closed — no further action

Partially Compliant User may create a new manual follow-up task

Not Compliant

An automatic task is generated by the platform; the user can accept or reject it (with option to create manual task)

Status Action

Not Applicable Requirement excluded

References:

- Source spreadsheet: [CRA Requirements Spreadsheet](#)
- Reference diagram: [Organization Role Mapping](#)
- Reference diagram: [Compliance Flow](#)

10. Task #318 - Organization CRA Compliance Dashboard, Visualization & PDF Export

Overview

The system must provide a dynamic dashboard view summarizing compliance progress for each organization assessment. This dashboard must include a status table, charts, a progress bar, and export to PDF.

Dashboard Components

1. Status Table

A table listing all requirements, their evaluation status, and conformity results.

Columns:

- Requirement Identifier
- Requirement Name
- Requirement Status → Evaluated / Not Evaluated
- Conformity Status → Compliant, Partially Compliant, Not Compliant, In Evaluation (e.g., 33%), or Not Applicable

Sample Table:

Security Requirement Requirement Status Conformity Status

ES01 Secure Product Design Evaluated Partially Compliant

ES02 Secure Development Practices Evaluated Not Compliant

ES03 Outsourced Development Evaluated Compliant

ES04 Security Testing and Vulnerability Remediation Not Evaluated In Evaluation [33%]

ES05 Third-party Component and Supply Chain Management Evaluated Not Applicable

Progress computation formula: average of answered questions for the requirement (e.g., 1 of 3 answered → 33%).

2. Pie Charts

• Chart A:

- Evaluated vs. Not Evaluated (count of requirements)
- Breakdown of Compliant / Partially Compliant / Not Compliant / Not Applicable

• Chart B:

- Task distribution by type & status (e.g., auto-generated, manual, closed)

3. Progress Bar

- Computed as the arithmetic average of all requirements:
- *Evaluated requirements* → 100%
- *Not Evaluated requirements* → use their completion percentage (e.g., 33%).

4. Export Conformity Assessment Report

- The **dashboard must be exportable as a PDF file**, including:
- Organization identifier
- Status table, questions and given answers (with rationales if added)
- Charts
- Progress bar
- Timestamp of export

Reference: [Dashboard Status Section](#)

11. Task #319 - Product Details Page

Overview

When a user selects a specific product, the system should display a dedicated **Product Details Page**. This page provides an overview of the product's properties and its associated versions.

Page Structure

The Product Details Page is divided into **three main sections**:

1. Product Properties Section

Displays key information about the selected product, including:

- Product Name
- Category
- Organization Role
- Incidents Count
- Vulnerabilities Count
- External Reporting
- Assessment Type
- Description

Actions (buttons):

- **Delete** – remove the product
- **Withdraw** – mark the product as withdrawn
- **Edit** – update product details

2. Applicability Survey Section

- **2.1 View** button - allows viewing the applicability survey.
- **2.2 Edit / Retake** button - allows editing / retaking the applicability survey.

3. Product Versions Section

Displays all versions of the product grouped into two tabs:

- **Active / Supported** – lists active or supported product versions
- **Not Supported** – lists product versions that are no longer supported

Available Actions:

- **New Assessment / New Product Version** – creates a new version and triggers a new assessment

Each version entry displays:

- Version Name
- Status
- Open Incidents Count
- Open Vulnerabilities Count
- Open Tasks Count
- **Show More** button – opens a detailed view of the product version

12.Task #320 - Product Version Details Page

Overview

When a user selects a specific **product version**, the system should display a **Version Details Page**. This page provides comprehensive information about the selected version, including its properties, conformity assessment status, and related records.

Page Structure

The Version Details Page is divided into **three main sections**:

1. Product Version Properties Section

Displays key information about the selected version:

- Product Version Name
- Status
- Release Date: By default: product version creation date; Editable
- Open Incidents Count
- Open Vulnerabilities Count
- Open Tasks Count
- Supported Period: Date value

2. CRA Compliance Assessment Section

This section has **two sub-sections**:

• 2.1 CRA Compliance Assessment

- Buttons: **View** and **Edit** – allows viewing or editing the compliance assessment.

• 2.2 Declaration of Conformity

- Buttons: **View** and **Download** – allows viewing or downloading the declaration of conformity.

3. Related Information Section

Displays additional data linked to the selected version via **tabs**:

- Tasks
- Files
- SBOM
- Vulnerabilities
- Incidents
- Version Logs
- Repositories

Tab Behavior:

- Clicking a tab displays a list of corresponding items.
- Each list should include buttons for **filtering**, **adding**, and **viewing details**.

13.Task #321 - Vulnerability Details Page

Overview

When a user selects a specific **vulnerability**, the system should display a **Vulnerability Details Page**. This page provides detailed information about the vulnerability, related metadata, and associated documents.

Page Structure

The Vulnerability Details Page is divided into **three main sections**:

1. Basic Vulnerability Information Section

Displays key properties of the selected vulnerability:

- Vulnerability Name
- Status
- Severity
- Affected Vendor
- Affected Product
- Affected Version

Actions (buttons):

- **Edit** – update vulnerability details
- **Close** – mark the vulnerability as closed

2. Extended Vulnerability Data Section

Displays additional metadata and references:

- Summary
- Advisory IDs
- Published Date
- Updated Date
- Assigner Name
- References

3. Attachments Section

Displays all files associated with the vulnerability.

Features:

- **Add Document** button – attach a new file to the vulnerability
- Table listing attached files with the following columns:
 - Name
 - Type
 - Version
 - Date Added
 - Added By
 - Last Edited
 - Edited By

Each row includes:

- **More** button – access additional file details or actions

14. Task #322 - Incident Details Page

Overview

When a user selects a specific **incident**, the system should display an **Incident Details Page**. This page provides comprehensive information about the incident, related metadata, and attached documents.

Page Structure

The Incident Details Page is divided into **three main sections**:

1. Basic Incident Information Section

Displays key properties of the selected incident:

- Incident Name
- Classification
- Attack Type
- Asset Details

Actions (buttons):

- **Edit** – update incident details
- **Close** – mark the incident as closed

2. Extended Incident Data Section

Displays additional metadata and investigative details:

- Reporter
- Date of Detection
- Published Date
- Severity
- Handling Date
- Description
- Corrective Actions
- Root Cause
- Scope
- Preventive Actions

3. Attachments Section

Displays all files associated with the incident.

Features:

- **Add Document** button – attach a new file to the incident
- Table listing attached files with the following columns:
 - Name
 - Type
 - Version
 - Date Added
 - Added By
 - Last Edited
 - Edited By

Each row includes:

- **More** button – access additional file details or actions

15.Task #323 - Add New Product Version

Overview

From the **Product Details Page**, the user can create a new product version by clicking on the “**New Assessment / New Product Version**” button. This action opens the **Add New Product Version Page**, where details for the new version can be entered.

Page Structure

The **Add New Product Version Page** consists of the following elements:

1. Product Information (Read-Only Fields)

- Product Acronym / Short Name
- Product Full Name

2. New Version Information (Input Fields)

- New Product Version (text field)
- New Product Version Short Description (text area)
- Supported / Not Supported: checkbox

3. Actions (Buttons)

- **Back** – return to the previous page
- **Create Product Version** – saves the new product version and associates it with the product **Expected Behavior**
 - Read-only fields must be pre-filled with existing product data.
 - Input fields must be validated before allowing creation of the new product version.
 - On success, the user is redirected back to the **Product Details Page** where the new version is listed under the appropriate tab (Active/Supported or Not Supported).

16. Task #324 - Add New Vulnerability

Overview

From the **Product Version Details Page**, the user can create a new vulnerability by clicking on the “**New Vulnerability**” button. This action opens the **Add New Vulnerability Page**, where details for the new vulnerability can be entered.

Page Structure

The **Add New Vulnerability Page** consists of the following sections:

1. Context Information (Read-Only Fields)

- Version
- Product

2. Vulnerability Information (Input Fields)

- Name
- Status (*Pending, Preparation, Receipt, Verification, Remediation Development, Release, Post-Release*); The values should not be in alphabetical order, but like in the list provided.
- Severity

- Affected Product **required*
- Affected Version **required*
- Date of Discovery **required*
- Summary **required*
- Advisory IDs
- Assigner
- Checkbox: “Has the product been made available on the territory of other Member States?”
- If selected “Yes,” an additional optional text field appears for the user to provide details (a list of those Member States).

3. Attachments Section

- **Add Document** button – allows uploading and attaching files related to the vulnerability

4. Actions (Buttons)

- **Cancel** – discard and return to the Product Version Details Page
- **Add** – save the new vulnerability and associate it with the selected product version

Expected Behavior

- Read-only fields must be pre-filled with the relevant product and version context.
- Input fields must be validated before the vulnerability can be added.
- On success, the new vulnerability is listed under the **Vulnerabilities tab** in the

Product Version Details

Page.

17.Task #325 - Add New Incident

Overview

From the **Product Version Details Page**, the user can create a new incident by clicking on the “**New Incident**” button. This action opens the **Add New Incident Page**, where details for the new incident can be entered.

Page Structure

The **Add New Incident Page** consists of the following sections:

1. Context Information (Read-Only Fields)

- Version
- Product

2. Incident Information (Input Fields)

- ID
- Status (*Pending, Start, Declared, Stable, Active, Resolved, Completed*); The values should not be in alphabetical order, but like in the list provided.
- Classification (select one of the predefined values):
- General
- Confidentiality

- Integrity
- Availability
- Access Control
- Vulnerabilities
- Technical Failure
- Theft or Loss of Equipment
- Attack Type (select one of the predefined values):
- Denial of Service
- Unauthorised Access
- Malware
- Abuse
- Others
- Asset Details
- Reporter
- Date of Detection **required*
- Severity
- Handling Date
- Description **required*
- Corrective Actions
- Root Cause
- Scope **required*
- Preventive Actions
- Checkbox: “Is the incident suspected of being caused by unlawful or malicious acts?”
- If selected Yes, an optional text field appears where the user can describe the situation.
- Checkbox: “May the incident have a cross-border impact?”
- If selected “Yes,” an additional optional text field appears for the user to provide details.

3. Attachments Section

- **Add Document** button – allows uploading and attaching files related to the incident

4. Actions (Buttons)

- **Cancel** – discard and return to the Product Version Details Page
- **Add** – save the new incident and associate it with the selected product version

Expected Behavior

- Read-only fields must be pre-filled with the relevant product and version context.
- Input fields must be validated before the incident can be added.
- On success, the new incident is listed under the **Incidents tab** in the **Product Version Details Page**.

18. Task #326 - Edit Vulnerability

Description

From the "Product Version Details" page and with the *Vulnerabilities* tab selected, the user can click the "Show More" button for a specific vulnerability, which opens the

Edit Vulnerability page.

Page Structure

The page consists of three main sections:

1. Basic details (read-only fields)
2. Editable vulnerability information
3. Attachments

1. Read-Only Fields

- Version
- Product

2. Editable Fields

- Name
- Status (*Pending, Preparation, Receipt, Verification, Remediation Development, Release, Post-Release*); The values should not be in alphabetical order, but like in the list provided.
- Severity
- Affected Product
- Affected Version
- Summary
- Advisory ID(s)
- Assigner
- Checkbox: "Has the product been made available on the territory of other Member States?"
- If selected "Yes," an additional optional text field appears for the user to provide details (a list of those Member States).

3. Attachments

- A button "**Add Document**" allowing the user to attach supporting files.

Buttons

- **Cancel**
- **Save**

Status Management Considerations

1. The user manually changes the vulnerability phase (status).
2. There is no fixed order for changing states.
3. Status changes are independent — no constraints are applied based on other actions or properties of the vulnerability.

19. Task #327 - Edit Incident

From the "**Product Version Details**" page, with the **Incidents** tab selected, the user can click the "**Show More**" button for a specific incident, which opens the "**Edit Incident**" page.

Page Structure

The **Edit Incident** page consists of three sections:

1. Read-Only Fields

- Version
- Product

2. Editable Fields

- ID
- Status (*Pending, Start, Declared, Stable, Active, Resolved, Completed*); The values should not be in alphabetical order, but like in the list provided.
- Classification (*General, Confidentiality, Integrity, Availability, Access Control, Vulnerabilities, Technical Failure, Theft or Loss of Equipment*)
- Attack Type (*Denial of Service, Unauthorised Access, Malware, Abuse, Others*)
- Asset Details
- Reporter
- Date of Detection
- Severity
- Handling Date
- Description
- Corrective Actions
- Root Cause
- 14.11.2025 OSCRAT 1
- Scope
- Preventive Action
- Checkbox*: "Is the incident suspected of being caused by unlawful or malicious acts?"
- If selected **Yes**, an optional text field appears where the user can describe the situation.

- Checkbox: "May the incident have a cross-border impact?"

- If selected "Yes," an additional optional text field appears for the user to provide details.

3. Attachments

- A list of attached files
- Button: **Add Document**

Page Actions

Buttons at the bottom:

- **Cancel**
- **Save Changes**

Status Management

1. The user manually changes the incident status (phase).
2. There is no specific order in which statuses must be changed.
3. There are no constraints linked to other actions or properties of the incident.

20. Task #328 - SBOM Management

Overview

The Software Bill of Materials (SBOM) functionality allows users to generate, import, scan, and manage SBOMs for a specific **Product Version**. It can be accessed by navigating to the **Product Version Details** page and selecting the **SBOM** tab. The SBOM tab provides two main actions — **Import** and **Generate** — and displays a list of all SBOMs associated with the product version.

SBOM List View

Each SBOM entry in the list displays the following information:

Text fields:

1. **Name**
2. **Status** – one of the following: *Processing, Ready, Failed, Scanning, Archived*
3. **Date Added**
4. **Added By** – user's first and last name
5. **Vulnerabilities Scan Status** - Not scanned or Last scan date

Buttons (for each SBOM on the list):

1. **Scan**
2. **Download**
3. **View Scans**

Actions

1. Generate SBOM

- The user clicks the **Generate** button to create a new SBOM.
- When clicking the **Generate** button, the user should be prompted to select the desired SBOM format. The available options are: **SPDX** and **CycloneDX**. Multiple format selection should be supported.
- The generation process is executed using the external tool **Syft**.

Preconditions:

- A repository path must be defined for the current product version.

This is configured under the **Repositories** tab in the **Product Version Details** page.

- If no repository is defined, the **Generate** button is **inactive**, and a warning message appears: *"To generate an SBOM, first define a repository in the Repository tab."*
- If a generation process is already in progress, the button remains **inactive** with the warning message: *"Wait until the last SBOM attached is done processing before generating a new one."*

Business Rules:

- One product version can have multiple software versions.
- Only **one SBOM** can exist per software version.

Before generating a new one, the system checks whether an SBOM already exists.

If so, an informational message is displayed: *“An SBOM already exists for this software version.”*

- Once generated, the SBOM is **read-only**.
- The SBOM name must follow a defined naming convention that includes the **software version identifier**.

2. Import SBOM

- The user can import an SBOM that was previously generated outside the platform.
- Upon clicking **Import**, the user uploads a file in an acceptable SBOM format (to be specified). Supported formats are expected to include:

- **SPDX**

- **CycloneDX**

- (Additional formats may be defined by authorities later.)

Note: By the end of the year, official guidance will specify the required SBOM detail level and accepted standards.

3. Scan SBOM

- Clicking **Scan** (for selected SBOM) initiates a vulnerability scan using the external tool **Grype**.
- Scanning results are written down in a **Vulnerability Report**, linked to the specific SBOM.
- The user can review the report and select vulnerabilities to add to the **Vulnerabilities** module (Product Version Details page, Vulnerabilities tab).

Conditions:

- Scans can only be performed on SBOMs with **Status: Ready**.
- Multiple scans may be run for the same SBOM over time.

4. Download SBOM

- Users can download any existing SBOM.
- Each download action must be logged, including:
 - User performing the action
 - Timestamp of the download

5. View Scans (Scans Overview)

The **View Scans** action opens a dedicated **SBOM Scans Overview** page or window that lists all scans performed for a specific SBOM.

Each entry includes:

- **Scan ID**
- **Execution Date**
- **Triggered By**
- **Status** – *Processing, Completed, Failed*
- **Result Summary** (e.g., number of vulnerabilities detected)

Status Workflow

Status Description

Processing SBOM generation in progress

Ready SBOM generation completed successfully

Failed SBOM generation failed

Archived SBOM no longer active, kept for historical reference

Implementation Notes

- Integrate Syft and Grype as external services for SBOM generation and vulnerability scanning.
- Ensure proper error handling and user feedback during generation/import/scan operations.
- Maintain audit logs for generation, import, scan, and download actions.
- Future-proof the implementation to accommodate new SBOM standards and formats.

21.Task #336 - Requirements Evaluation – Automatic Task Generation new

The system automatically evaluates the results of the CRA Compliance Self Assessment for each requirement

and performs actions based on the user's selected compliance outcome.

Each requirement can result in one of four possible statuses:

1. Not Compliant
2. Partially Compliant
3. Compliant
4. Not Applicable

The logic defined below determines whether the system should automatically create follow-up tasks or update the overall assessment status.

1. Not Compliant

When a requirement is marked as Not Compliant:

- The system automatically generates a new task linked to the product version.
- The following task fields are pre-filled automatically:
 - Name – derived from the requirement identifier and name (e.g., “[REQ-ID] Requirement Remediation”).
 - Description – from the excel file - suggestions column.
 - Product Version – linked to the product version where the assessment was made.
- The user is presented with a confirmation dialog asking whether to accept the automatically generated task:
 - Yes → The task is created and added to the task list.
 - No → The task is discarded, and no new entry is created.

2. Partially Compliant

114.11.2025 OSC RAT

When a requirement is marked as Partially Compliant:

- The system does not automatically generate a task.
- The user can manually create a task, if corrective actions are needed.

3. Compliant & Not Applicable

When a requirement is marked as Compliant or Not Applicable:

- No new tasks are generated.
- Once all requirements are evaluated and all are either Compliant or Not Applicable, the system automatically marks the entire assessment as Finished.

Task Object – Additions and Updates

To support the automatic task generation mechanism, the following updates to the Task object are required:

1. Product Version

- New optional property linking the task to a specific product version.
- Enables filtering and reporting by version.

2. Status

- Possible values:
- To Do
- Planned
- In Progress
- Done

3. Origin Type (Automatic / Manual)

- Boolean field indicating whether the task was automatically generated by the system or manually

created by the user.

- UI Representation: Displayed via an icon or visual marker (e.g., ⚙️ for automatic tasks, 🖐️ for manual).

Task List – Filtering

Enhance the Tasks page with an additional filter:

- Filter by Product Version → Displays all tasks associated with the selected product version.
- The filter should support multi-selection if needed.

Implementation Notes

- Automatic task generation should trigger instantly upon requirement evaluation submission.
- All auto-created tasks must be logged in the system's audit log with their origin and timestamp.

214.11.2025 OSC RAT.



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 3



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.

#	Question	Answer
No.		
1.1	Is the product commercially supplied?	
1.1.1		Yes
1.1.2		No
1.2	Is the product made available only for a limited period required for testing purposes	
1.2.1		Yes
1.2.2		No
1.3	Does the product with digital elements was developed as a spare part to replace identical components on the market?	
1.3.1		Yes
1.3.2		No

1.4	Is this a new solution or a modification of an existing product?	
1.4.1		New solution
1.4.2		Modification of an existing product
1.5	Is this a substantial modification?	
1.5.1		Yes
1.5.2		No
1.6	Does the product contain digital elements?	
1.6.1		The product is a software solution, which is part of an electronic information system, in form of of computer code;
1.6.2		The product is a hardware solution in form of physical electronic information system, capable of processing, storing or transmitting digital data
1.6.3		The product does not contain digital elements.

1.7	Does the product with digital elements has the nature of a medical device?	
1.7.1		Yes, in accordance with EU Regulation 2017/745,
1.7.2		No
1.8	Does the product with digital elements has the nature of a medical device for in vitro diagnostics?	
1.8.1		Yes, in accordance with EU Regulation 2017/746,
1.8.2		No

1.9	Does the product with digital elements is build for vehicles, where a product is a component for: - protection and safety of vehicle occupants and vulnerable road users or, - pressure monitoring systems or, - fuel efficiency or, - CO2 emissions or, - tyres.	
1.9.1		Yes, in accordance with EU Regulation 2019/2144,
1.9.2		No
1.10	Is the product with digital elements: - products, parts and equipment for remote control of aircraft or, - products for aircraft maintenance and operation or, - products/equipment for operation of airports or, - products related to the protection of the airport environment or, - components used in ATM/ANS.	
1.10.1		Yes, it is certfyied in accordance with Regulation (EU) 2018/1139,
1.10.2		No
1.11	Does the product with digital elements has a nature of marine equipment intended to be placed on board EU ships?	
1.11.1		Yes, in accordance with EU Regulation 2014/90/UE,
1.11.2		No
1.12	Does the product with digital elements is developed or modified exclusively for national security, defense, or specifically designed to process classified information?	

1.12.1		Yes
1.12.2		No
1.13	Does your product fall into any of the following categories?	
1.13.1		Hardware Devices with Security Boxes?
1.13.2		Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing
1.13.3		Smartcards or similar devices, including secure elements

1.13.4		Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
1.13.5		Firewalls, intrusion detection and prevention systems
1.13.6		Tamper-resistant microprocessors
1.13.7		Tamper-resistant microcontrollers
1.13.8		Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

1.13.9		Standalone and embedded browsers
1.13.10		Password managers
1.13.11		Software that searches for, removes, or quarantines malicious software
1.13.12		Products with digital elements with the function of virtual private network (VPN)
1.13.13		Network management systems

1.13.14		Security information and event management (SIEM) systems
1.13.15		Boot managers
1.13.16		Public key infrastructure and digital certificate issuance software
1.13.17		Physical and virtual network interfaces
1.13.18		Operating systems

1.13.19		Routers, modems intended for the connection to the internet, and switches
1.13.20		Microprocessors with security-related functionalities
1.13.21		Microcontrollers with security-related functionalities
1.13.22		Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities

1.13.23		Smart home general purpose virtual assistants
1.13.24		Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems

1.13.25		Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council (1) that have social interactive features (e.g. speaking or filming) or that have location tracking features
1.13.26		Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children

1.13.27

Other

Hint for the user

This Regulation applies to economic operators only in relation to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity.

Including through sales, monetization, paid support, or data processing beyond security purposes excluding cases where the product is solely cost-recovery based or developed/used exclusively by public administration without market availability

The unfinished software which does not comply with CRA can be made available on the market, provided that the software is made available only for a limited period required for testing purposes with a visible sign clearly indicating that it does not comply with this Regulation and that it will not be available on the market for purposes other than testing.

This Regulation does not apply to spare parts that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace.

In order to ensure that products with digital elements made available on the market can be repaired effectively and their durability extended, an exemption cover both spare parts that have the purpose of repairing legacy products made available before the date of application of CRA and spare parts that have already undergone a conformity assessment procedure pursuant to CRA.

Determining whether it is a “significant modification” and requires reassessment – a significant modification, if the product is being assessed by a third party, must also be reported to that party.

‘substantial modification’ means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I or which results in a modification to the intended purpose for which the product with digital elements has been assessed.

"Product with digital elements" means a software or hardware product, where:

- "software" means the part of an electronic information system which consists of computer code;
- "hardware" means a physical electronic information system, or parts capable of processing, storing or transmitting digital data;
- "electronic information system" means a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data;

and its remote data processing solutions, including software or hardware components being placed on the market separately, where:

- "component" means software or hardware intended for integration into an electronic information system;
- "remote data processing" means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

If the product is subject to the requirements set out in the Regulation (EU) 2017/745, it is a medical device.

"Medical device" means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
 - diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
 - investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
 - providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,
- and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

The following products shall also be deemed to be medical devices:

- devices for the control or support of conception;
- products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point.

If the product is subject to the requirements set out in the Regulation (EU) 2017/746, it is a vitro diagnostic medical device.

"In vitro diagnostic medical device" means any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following:

- concerning a physiological or pathological process or state;
- concerning congenital physical or mental impairments;
- concerning the predisposition to a medical condition or a disease;
- to determine the safety and compatibility with potential recipients;
- to predict treatment response or reactions;
- to define or monitoring therapeutic measures.

Specimen receptacles shall also be deemed to be in vitro diagnostic medical devices;

If the product is subject to the requirements set out in the Regulation (EU) 2019/2144, it is a product for protection and safety of vehicle occupants and vulnerable road users, pressure monitoring systems, fuel efficiency and CO2 emissions, tyres.

A product certified and in the scope of Regulation (EU) 2018/1139 does not apply to CRA.

A product in the scope of Regulation 2014/90/UE does not apply to CRA.

Products with digital elements that are developed or modified exclusively for national security or defence purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation.

Hint: This category of products includes: payment terminals, tachograph vehicle units, smart meters, access control terminals and Hardware Security Modules where significant portions of the required security functionality depend upon a hardware physical envelope (referred to as a 'Security Box') that is designed to resist direct attacks. [Ref. extras from COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)]
Hint: "‘smart metering system’ means an electronic system that is capable of measuring electricity fed into the grid or electricity consumed from the grid, providing more information than a conventional meter, and that is capable of transmitting and receiving data for information, monitoring and control purposes, using a form of electronic communication This category of products includes: - Smart Metering Gateway - Device or unit within smart metering systems responsible for collecting Meter Data, processing Meter Data, providing communication capabilities for devices in the Local Metering Network, protecting devices in the Local Area Network, and providing cryptographic primitives (in cooperation with a Security Module). [Ref. Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), BSI CC PP 0073] - Components which can be used in the environment of smart metering systems by various types of users to support their tasks and communication activities in a secure operating environment [Ref. BSI Technische Richtlinie BSI TR-03109-2.B]
Hint: This category of products includes: smart card hardware/ICs, smart card composite products, TPMs used in Trusted Computing, digital tachograph cards, etc. – are devices where significant portions of the required security functionality depending upon hardware features at a chip level. NOTE: Smart card holder and issuer generally execute operations through communication with Smart Card terminal. The Smart Card terminals that have a physical protected envelope shall be considered as hardware with Security Boxes.

Hint: This category of products includes:

- Hypervisor-based operating system virtualization: focuses on the virtualization of the entire operating system, which each virtualized environment instance being designated as virtual machine (VM).

- Container-based operating system virtualization, includes two types of containers: application containers, which package a single process or application; and system containers, which simulate a full operating system and tend to execute multiple processes simultaneously.

NOTE: The virtualisation environment includes: BIOS, firmware, Operating Systems (OS) and drivers.

Hint: This products family includes:

- Firewalls - An internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall).

Source: RFC 4949 Internet Security Glossary, Version 2

- Intrusion Detection system - information systems used to identify that an intrusion has been attempted, is occurring, or has occurred [Source: ISO 27039:2015], and

- Intrusion Prevention System is variant on intrusion detection systems that are specifically designed to provide an active response capability [Source: ISO 27039:2015]

Hint: This category of products includes: Microprocessors that implement security mechanisms against tampering of the device. Such mechanisms deter unauthorized use, malicious modification of the module (including substitution of hardware and software), or exposure of security information, such as cryptographic keys and secrets. Depending on the level of protection, anti-tamper mechanisms may include: tamper resistance, tamper detection, tamper response, and tamper evidence (see table below).

[Ref. FIPS 140-3: Security Areas, Chapter 5: Physical security]

Hint: This category of products includes:

- Microcontrollers, that is, a small computer on a single integrated circuit (System on Chip – SoC). In modern terminology, a microcontroller is similar to, but less sophisticated than, a system on a chip (SoC). A SoC may include a microcontroller as one of its components, but usually integrates it with advanced peripherals like a graphics processing unit (GPU), a Wi-Fi module, or one or more coprocessors.

- Microcontrollers are used in most cases for embedded applications, in contrast to (general purpose) microprocessors consisting of a variety of chips and peripherals.

Hint: This category of products includes a variety of products that implement Identity and Access Management functions (locally or remotely). Identity management systems typically include software platforms that manage user identities and credentials, such as usernames, passwords, digital certificates, and multi-factor authentication tokens. They often integrate with directory services like Active Directory or LDAP and provide features such as single sign-on (SSO), role-based access control (RBAC), identity federation, and lifecycle management for user accounts. These systems help ensure that employees, partners, or clients can access appropriate systems based on their roles while preventing unauthorized access. Privileged access management software specifically targets accounts that have elevated permissions, such as system administrators or database managers. These tools secure, monitor, and audit the use of privileged credentials to reduce the risk of misuse or credential theft. PAM solutions typically include secure credential vaults, session recording, just-in-time access provisioning, and alerting mechanisms for suspicious behavior.

Hint: This category of products includes:

- Standalone web browsers and
- Embedded browsers,

Standalone and embedded browsers are software components used for web access, with standalone browsers functioning as independent applications and embedded browsers integrated into other software or hardware systems to provide web-based interfaces or display web content. Standalone browsers offer full-featured browsing capabilities, user interaction, and security controls, while embedded browsers are often used in applications, kiosks, or devices where web content needs to be displayed within a controlled environment. Both types play key roles in enabling web access, but they differ in functionality, user interaction, and integration with other systems.

Hint: Password managers are software tools designed to securely store, generate, and manage passwords and other sensitive credentials for users. They help individuals and organizations maintain strong, unique passwords for each account or service, reducing the risk of security breaches caused by reused or weak passwords. These tools typically encrypt stored data and require a master password or biometric authentication to access the vault. Advanced password managers may also support features like autofill, secure sharing, multi-factor authentication integration, and monitoring for compromised credentials. They enhance both security and convenience by simplifying the management of complex credentials across multiple platforms and devices.

Hint: This category of products includes software that monitors a mobile device/ computer or network to identify malware, prevent it from infecting devices and clean infected devices. Antivirus and anti-malware software are security tools designed to detect, block, and remove malicious software such as viruses, ransomware, trojans, and spyware. They scan systems using signature databases and behavioral analysis to identify threats, then remove or quarantine infected files to prevent damage.

Hint: This category of products includes any mechanism for overlaying a cryptographically secured network over distributed wide-area networks. [Ref: PP-Module for Virtual Private Network (VPN) Gateways; PP-Module for VPN Client Version 2.1; NIST 800-113 - Guide to SSL VPNs] Products with digital elements that provide Virtual Private Network (VPN) functionality are software or hardware solutions designed to create secure, encrypted connections over public or untrusted networks. These products mask users' IP addresses, protect data in transit, and enable private access to internet resources or internal networks.

Hint: This category of products includes:

- NMS/EMS consists of systems and applications for control and monitoring of network elements (NE) on the network (such as hosts, gateways and terminal servers) and offers Fault, Configuration, Accounting, Performance, Security [FCAPS functionality] for the whole network.
- includes network management system (NMS)/ equipment management system (EMS) which is used for the management of network elements / devices.

[Ref. The FCAPS management categories and TMN management functions are also specified in ITU-T: Recs M.3010, X.700 and X.701 and ISO/IEC 10040. Configuration management system ISO/IEC 7184:2024; Fault Management – ETSI-TR 32.111 – series]

Hint: SIEM solutions are a combination of the formerly disparate product categories of SIM (security information management) and SEM (security event management). SEM deals with real-time monitoring, correlation of events, notifications and console views. SIM provides long-term storage, analysis and reporting of log data. [Ref. ETSI GS ISI 002 V1.2.1 (2015-11) Information Security Indicators (ISI); Event Model A security event classification model and taxonomy]

Hint: Boot managers are software tools that control the startup process of a computer, allowing users to choose which operating system or environment to load when the system powers on. They are essential in multi-boot setups where multiple operating systems. This category of products includes: Boot manager, boot loader, bootstrap loader (used synonymously), used during start-up process for data processing devices. They are responsible for (securely) loading the operating system of the device.

Hint: Public Key Infrastructure (PKI) and digital certificate issuance software are security solutions used to manage the creation, distribution, validation, and revocation of digital certificates. These systems support secure communications, authentication, and data integrity by enabling encryption and digital signatures based on asymmetric cryptography. PKI solutions include components such as certificate authorities (CAs), registration authorities (RAs), and certificate management tools.

Hint: The category refers to the components—either hardware or software-based—that allow a product with digital elements to connect to and communicate over a network. These interfaces serve as the points of entry and exit for data transmission, enabling interaction with external systems or services.

This category of products includes:

- Physical network interfaces that are based on network hardware platforms
- Virtual network interfaces that created a software version (i.e., emulation) of physical network interfaces

Hint: This category of products includes software that controls the execution of programs and that may provide services such as resource allocation, scheduling, input-output control, and data management.

[Ref. ISO/IEC 2382:2015 Information technology — Vocabulary]

Hint: The category encompasses network infrastructure devices that manage and direct data traffic between local and external networks. These products typically perform core networking functions such as routing, signal modulation/demodulation, and switching of data packets. As they often serve as gateways to the internet or other network segments, their exposure to potential threats is high, making it essential that they are developed with robust cybersecurity features to ensure secure configuration, data integrity, access control, and resilience against malicious exploitation.

This category of products includes:

- Routers are devices that direct traffic between different networks. They operate at OSI Layer 3: Network Layer, as are designed to route packets between different networks based on logical addressing (IP addresses).
- Network switches are networking devices that connect devices on a computer network by using packet switching to receive, process, and forward data to the destination device. Switches work primarily at Switches work at the OSI Layer 2 – data link – by using MAC addresses to forward data between devices on the same network. Some switches are designed to operate at both layer 2 and layer 3, being able to perform routing functions.
- Modems function at the physical layer of the OSI model, converting digital data from a computer into analogue signals suitable for sending over various transmission media, and vice versa. Modems used to connect to internet usually provide integrate functionality of router/modem, and sometimes switching.

Hint: This category of products includes microprocessors that implement security mechanisms against tampering of the device. Such mechanisms deter unauthorized use, malicious modification of the module (including substitution of hardware and software), or exposure of security information, such as cryptographic keys and secrets. Depending on the level of protection, anti-tamper mechanisms may include: tamper resistance, tamper detection, tamper response, and tamper evidence (see table below).

[Ref. FIPS 140-3: Security Areas, Chapter 5: Physical security]

Hint: This category of products includes microcontrollers that implement security mechanisms against tampering of the device. Such mechanisms deter unauthorized use, malicious modification of the module (including substitution of hardware and software), or exposure of security information, such as cryptographic keys and secrets. Depending on the required level of protection, anti-tamper mechanisms may include: tamper resistance, tamper detection, tamper response, and tamper evidence (see table below). [Ref. FIPS 140-3: Security Areas, Chapter 5: Physical security]

Hint: This products with security-related functionalities refers to specialized hardware components designed to perform dedicated security functions, such as cryptographic operations, secure boot, or hardware-based access control. These components are integral to the trustworthiness of a product's security architecture, as they often handle sensitive processes at the hardware level. Due to their low-level operation and influence on overall system integrity, ensuring their secure design, configuration, and update mechanisms is critical to mitigating vulnerabilities and supporting secure product lifecycles.

This category of products includes application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) are two forms of components used in consumer electronics.

Hint: This category includes voice-activated or text-activated devices designed to perform a wide range of functions within a domestic environment, such as controlling connected appliances, managing user preferences, or providing information services. These assistants typically integrate microphones, speakers, network interfaces, and cloud connectivity, making them continuously exposed to user input and internet-based communication. Given their access to personal data and their central role in smart home ecosystems, strong cybersecurity measures are essential to protect privacy, authenticate users, prevent unauthorized access, and ensure secure data handling.

This category of products includes:

- Any software system designed to help users interact with and control smart home devices directly from their smartphones or tablets based on voice commands, text, gesture or other interfaces, acting as centralized hubs for smart home automation and personal assistance.
- Any smart home device that has integrated virtual assistants such as Smart Voice-controlled Devices (SVD), consumer IoT device with integrated voice-controlled virtual assistant logic that responds to prompts and commands from users.
- Smart devices embedding multi-modal virtual assistants (i.e., interacting with users via a variety of channels, such as sound, images, text, etc.).

Hint: This category covers connected devices specifically designed to safeguard residential environments. These products typically involve real-time monitoring, remote access, and automated responses to potential threats, often processing sensitive audio, video, or biometric data. Due to their role in protecting physical spaces and personal safety, they require stringent cybersecurity controls to ensure data confidentiality, prevent tampering or unauthorized access, and maintain the reliability and integrity of their security functions.

This category of products includes consumer IoT devices that implement functions of physical security, including alarms, door locks, detectors (e.g., fire), surveillance, etc, such as:

- connected smoke detectors, door locks and window sensors
- smart cameras
- baby monitors
- connected home automation and alarm systems
- IoT gateways, base stations and hubs to which multiple devices connect.

Hint: This category of products includes toys that have all the three following characteristics:

- being internet-connected (in other words have the ability to connect to the internet); AND
- having social interactive features (e.g. speaking or filming) or location tracking features; AND
- being covered by Directive 2009/48/EC.

The Directive 2009/48/EC applies to “to products designed or intended, whether or not exclusively, for use in play by children under 14 years of age (hereinafter referred to as toys)” (see Art. 2 par. 1 Directive 2009/48/EC).

The following toys, among others, are excluded from this category since they are not considered as toys within the meaning of Directive 2009/48/EC (see Art. 2 par. 1 and Annex I Directive 2009/48/EC):

- “Products intended for use for educational purposes in schools and other pedagogical contexts under the surveillance of an adult instructor, such as science equipment”;
- “Functional educational products, such as electric ovens, irons or other functional products operated at a nominal voltage exceeding 24 volts which are sold exclusively for teaching purposes under adult supervision”;
- “Electronic equipment, such as personal computers and game consoles, used to access interactive software and their associated peripherals, unless the electronic equipment or the associated peripherals are specifically designed for and targeted at children and have a play value on their own, such as specially designed personal computers, key boards, joy sticks or steering wheels”;
- “Interactive software, intended for leisure and entertainment, such as computer games, and their storage media, such as CDs”;
- “Child-appealing luminaires”; and
- “Electrical transformers for toys”.

Also, the following toys are excluded from this category since the Directive 2009/48/EC does not apply to them (see Art. 2 par 2 Directive 2009/48/EC):

- “playground equipment intended for public use”;
- “automatic playing machines, whether coin operated or not, intended for public use”;
- “toy vehicles equipped with combustion engines”;
- “toy steam engines”; and
- “slings and catapults”.

Hint: This category of products includes:

Near-body wearable electronic device - wearable electronic device intended to be located near a human body but which does not make direct contact with its external surface; (see) excluded is equipment that is not wearable (e.g., that operates in close proximity to the human body) is not considered to be near-body wearable electronics. [Ref: IEC 63203-101-1:2021]

On-body wearable electronic device - wearable electronic device intended to be located on the external surface of a human body and which makes direct contact with it [Ref: IEC 63203-101-1:2021]

This relates to products that include software or hardware performing data processing or computation, but other than the above on the list. The category may include e.g.:

- products containing embedded software, firmware, or an operating system that can receive updates (e.g., security updates, firmware updates),
- products that connect to the internet or any other device via wired or wireless communication? (e.g., Wi-Fi, Bluetooth, USB, network cable, NFC, RFID, etc.),
- products that require a cloud service or remote data processing to perform one of their functions (i.e., would the product fail to function without cloud/remote software support?) - if the product requires access to a database, an API, or another data processing service provided by the manufacturer, such processing falls under the CRA regulations. At the same time, the regulation does not cover general security measures for the manufacturer's entire IT infrastructure,

Reference	OSCRAT tool reaction depending on the answer
Recital (15) Recital (16) Article 1 Article 2 Article 3 (22)	
	Skip next question and proceed with question 1.3.
	If the answer is no, proceed to the next question.
Article 4(3)	
	If the answer is Yes , OSCRAT should display a notice to the user that their product is not subject to the CRA , if it is marked with a visible sign clearly indicating that it does not comply with CRA regulations , and it is marked as a version made available for a limited period of time for testing purposes only . Then user exits the OSCRAT tool.
	If the answer is no, proceed to the next question.
Recital (29), article 2 (6)	
	If the answer is yes, exit OSCRAT, CRA does not apply to such a product.
	Proceed to next question

Recital (38), Recital (39) Article 3 (30) Article 13 (10) Article 21, Article 22	
	Skip the next question and proceed to question 1.6.
	Proceed to next question
Recital (41), Article 3(30), Article 13 (10) Article 21, Article 22	
	Proceed to next question
	If the answer is no, give the information about the product status in terms of CRA, exit OSC RAT (CRA does not apply to such a product).
Article 2(1), Article 3(1)	
	Proceed to next question
	Proceed to next question
	If the answer is that a product does not contain digital elements, exit OSC RAT - CRA does not apply to such a product.

Recital (25), Article 2(2)(a)	
	If the answer is yes, exit OSC RAT, CRA does not apply to such a product.
	Proceed to next question
Recital (25), Article 2(2)(b)	
	If the answer is yes, exit OSC RAT, CRA does not apply to such a product.
	Proceed to next question

Recital (27), Article 2(2)(c)	
	If the answer is yes, exit OSC RAT, CRA does not apply to such a product.
	Proceed to next question
Recital (27), Article 2(3)	
	If the answer is yes, exit OSC RAT, CRA does not apply to such a product.
	Proceed to next question
Article 2(4)	
	If the answer is yes, exit OSC RAT, CRA does not apply to such a product.
	Proceed to next question
Recital (26), Article 2(7)	

	If the answer is yes, exit OSCRAT, CRA does not apply to such a product.
	Proceed to next question
Annex III, Annex IV	Exit OSCRAT when the on of the options is selected - CRA applies to that product with class specified in column H..
Annex IV point (1)	Checkbox to select
Annex IV point (2)	Checkbox to select
Annex IV point (3)	Checkbox to select

Annex III part II point (1)	Checkbox to select
Annex III part II point (2)	Checkbox to select
Annex III part II point (3)	Checkbox to select
Annex III part II point (4)	Checkbox to select
Annex III part I point (1)	Checkbox to select

Annex III part I point (2)	Checkbox to select
Annex III part I point (3)	Checkbox to select
Annex III part I point (4)	Checkbox to select
Annex III part I point (5)	Checkbox to select
Annex III part I point (6)	Checkbox to select

Annex III part I point (7)	Checkbox to select
Annex III part I point (8)	Checkbox to select
Annex III part I point (9)	Checkbox to select
Annex III part I point (10)	Checkbox to select
Annex III part I point (11)	Checkbox to select

Annex III part I point (12)	Checkbox to select
Annex III part I point (13)	Checkbox to select
Annex III part I point (14)	Checkbox to select
Annex III part I point (15)	Checkbox to select

Annex III part I point (16)	Checkbox to select
Annex III part I point (17)	Checkbox to select

Annex III part I point (18)	Checkbox to select
Annex III part I point (19)	Checkbox to select

Recital (9), (11), (12), (34), (39),
(40), (56), (64)
Article 2(1),
Article 3(1)(2), 3(8), 3(9), 3(10)
Article 6(a)

Checkbox to select

Comments, remarks	Scope of CRA application
	Do the CRA requirements apply to the product?
Will the product be made available on the market as part of commercial activities?	

[illegible]

a product with the nature of a medical device for use in humans and accessories for such devices (Article 1, paragraph 1), including clinical trials on products (Article 1, paragraph 2) or separate groups of products with no intended medical purpose – Annex XVI (Article 1, paragraph 2).	
	Not applicable
a product with the nature of a medical device for in vitro diagnostics used by humans and accessories for such products (Article 1, paragraph 1j).	
	Not applicable

a product built for vehicles, with regard to their general characteristics, safety and the protection and safety of vehicle occupants and vulnerable road users; in the scope of type-approval (Article 1): • of vehicles and systems, components and separate technical units, and, • of tyre pressure monitoring systems, with regard to their safety, fuel efficiency and CO2 emissions; and, • of newly manufactured tyres, with regard to their safety and environmental performance.	
	Not applicable
the product has been certified in accordance with Regulation (EU) 2018/1139, i.e. a product of the nature (Article 1): • products, parts and equipment for remote control of aircraft; • aircraft maintenance and operation; • equipment and operation of airports; • related to the protection of the airport environment; • components used in ATM/ANS.	
	Not applicable
a product of the nature of marine equipment intended to be placed on board EU ships (Article 1).	
	Not applicable

	Not applicable
	Applicable. Qualifies as a CRITICAL product
	Applicable. Qqualifies as a CRITICAL product
	Applicable. Qqualifies as a CRITICAL product

	Applicable. Qualifies as an IMPORTANT product Class II
	Applicable. Qualifies as an IMPORTANT product Class II
	Applicable. Qualifies as an IMPORTANT product Class II
	Applicable. Qualifies as an IMPORTANT product Class II
	Applicable. Qualifies as an IMPORTANT product Class I

	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I

	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I

	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I

	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I

	Applicable. Qualifies as an IMPORTANT product Class I
	Applicable. Qualifies as an IMPORTANT product Class I

	Applicable - PDE Other than IMPORTANT or CRITICAL (standard product with digital elements)

Go to
Recitals
from CRA

Go to
Articles
from CRA

Go to
Articles
13-
15,19,20
from CRA

Go to
Annex
from CRA



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 5

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 5
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

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
Guide for the OSCRAT questionnaire
Keywords
Users' needs, Users' expectations, Inventory/labelling, Risk management, Vulnerability management, Incident management, Security management, Documentation, Workflow

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.

Table of contents

1. Guide for the OSCRAT questionnaire.....	5

1. Guide for the OSCRAT questionnaire

The purpose of this guide is to explain what the OSCRAT tool's response is to the answers provided by the user when completing a questionnaire.

What is a questionnaire in OSCRAT tool?

It is a set of questions formulated so that the questions allow for the assessment of compliance with CRA requirements.

Type of questionnaires - In OSCRAT tool you will find several questionnaires:

<i>Name of the questionnaire</i>	<i>Purpose of the questionnaire</i>
1_CL_Exclusion	The purpose of this questionnaire is to identify whether the analysed product falls under the CRA regulation. If the product is subject to CRA, then it is identified which category the product falls into.
2_CL_Organization	The purpose of this questionnaire is to identify the context in which the organization is located: manufacturer, importer, distributor, open-source steward
a. Manufacturer 3a_ESR - organization evaluation	Applicable only if the organization was classified as a manufacturer through the "2_CL Organization" questionnaire. Contains the assessment of minimum-security requirements related to organization.
a. Manufacturer 3b_ESR - products assessment	Applicable only if the organization was classified as a manufacturer through the "2_CL Organization" questionnaire. Contains the assessment of minimum-security requirements of the product. One assessment for each product!
a. Manufacturer 3c_Tech.Doc. of the product	Applicable only if the organization was classified as a manufacturer through the "2_CL Organization" questionnaire. The goal is to verify that the technical documentation is complete. A checklist will be applied for each product.
b. CL_Importers	Applicable only if the organization was classified as a Importer through the "2_CL Organization" questionnaire.

c. CL_Distributors	Applicable only if the organization was classified as a Distributor through the "2_CL Organization" questionnaire.
d. CL_OpenSourceStewards	Applicable only if the organization was classified as Open-source steward through the "2_CL Organization" questionnaire.
e. CL_Representatives	Applicable only if the organization was classified as Authorised representatives through the "2_CL Organization" questionnaire.
ESR - products assessment	The purpose of this questionnaire is to assess product conformity. It applies only to organizations that are manufacturers .
Tech.Doc. of the product	The purpose of this questionnaire is to validate that the product's technical documentation is prepared with the rigor required by CRA legislation.

Order of questionnaires

1. 1_CL_Exclusions
2. 2_CL_Organization (classification) - If organization is:
 - a. Manufacturer
 - i. 3a_ESR organization evaluation
 - ii. 3b_ESR - products assessment
 - iii. 3c_Tech.Doc. of the product
 - b. Importer: 4_CL_Importers
 - c. Distributor: 5_CL_Distributors
 - d. Open-source steward: 6_CL_OpenSourceStewards
 - e. Authorized representatives: 7_CL_Representatives

Checklist & Questionnaire structure:

1. Questionnaires :1, 2

- All questions are closed questions (only one options can be choose)
- Structure of the questions:
 - o Question
 - o Hint for the user - An explanatory text that helps the user understand the security requirement and prepares them for the questions section
 - o CRA References
 - o Answer (one option)
 - o Additional notes [text field]

2. Questionnaires: 3a, 3b, 4, 5, 6, 7

- A questionnaire will contain several questions, grouped into several sections, called "security areas"
- Each "security area" can have one or more "security requirements"
- To evaluate a security requirement "security requirement", several questions are needed. The questions can be of two types:
 - o **Closed questions**, to which the user must answer YES or NO (in some cases not applicable) and
 - o **Open questions**, to which the user must explain, to tell how the respective activity is carried out.

- Each "security requirement" will have the following structure:

<i>Requirement name</i>	Name of the security requirement
<i>CRA/ISO references</i>	Legislation references
<i>Hint for the user</i>	An explanatory text that helps the user understand the security requirement and prepares them for the questions section
<i>Questions</i>	A section with several mixed questions (closed and open questions)
<i>Answers</i>	The section where the user answers. It can be a radio button, for closed questions, it can be a text field (up to 1000 characters) or it can be an upload files section (where office files or print-screens are uploaded as attachments). In some cases, there may be an Evidence Hint text, which helps the user understand what they need to provide as an answer.
<i>Additional information</i>	The section collects any other information - answers to questions that were not asked, explanations that did not find their place in the answers to questions, particular situations related to the product or organization, etc.
<i>Compliance assessment</i>	Security requirement compliance assessment. This can only be done after all the questions related to "security requirements" are answered. Only one option can be chosen from the following: ○ Compliant ○ Partially Compliant ○ Not compliant ○ Not applicable
<i>Rationale</i>	A text for justification for compliance assessment.
<i>Action to be performed [optional]</i>	If the "security requirement" is not compliant (non-compliant or partially compliant) then the user will be subjected to a GENERIC TASK (the resolution of which will bring compliance with the security requirement). The user has the right to accept the task or to reject it. If it is accepted, will be created a link between "security requirements" and "generic task". After the task is closed, the security requirement will be reassessed (the user must answer again to all questions related to this requirement – versioning is per security requirements, not per question and include also the compliance assessment)

- **Tags:** each question can have multiple tags:
 - Pre and/or Post market (applicability) - the questions will be formulated depending on the context of the product (before launch or after launch)
 - Mandatory question – the questions that cannot be “Not applicable”

- Mandatory upload – is mandatory for user to upload a file in order to demonstrate the compliance
 - Technical file tag - Questions whose answers or attachments are part of the information package called "CONTENT OF THE TECHNICAL DOCUMENTATION" will be marked.
- When a field is marked with a star * - the text field or upload is mandatory (the user must respond or upload)
- The tool's response depending on the user's action (per question):
 - unanswered question - The status score of "question" is considered 0%. "Security requirements" cannot be evaluated and has status **"Not evaluated"**
 - answered question - The status score of "question" is considered 100%.
 - attachment is required and not provided - The status score of "question" is considered 50%.
- When all questions have a status of 100% (they have been answered) then the "security requirements" can be evaluated. After evaluation, it receives the status **"Evaluated"**.

3. Checklist: 3c_Tech.Doc. [Optional]

- comprehensive, practical checklist, well-structured so the user can tick off each item for compliance verification.

VERSIONING RULES:

- Of the questions: Questions may change over time, so the question database will be updated. To avoid confusion, each update of the question database must be uniquely versioned. Only one version can be active during an assessment.
- Of the answers: Each time an assessment is made, a new version is active, the remaining versions are archived and marked "read only"
 - For PRODUCT (3a questionnaire): a new questionnaire is triggered for each new product and for each major product update (new version of the product). When a new product is launched (premarket) will be triggered a new "generic task" for the assessment of the organization (questionnaire 3a). The user can decline the task (see next point).
 - For ORGANIZATION (only for Manufacturer - 3b questionnaire): manually triggered by the organization. If the last assessment is older than 365 days, a warning message will appear as a notification / an automatic reassessment task will be proposed. If the user declines the task, confirms that there are no changes in the organization, the warning message disappears, and the counter is reset (the 365 days). At any time, the user can decide to reassess the organization, due to changes in: internal processes, reorganizations, merge & acquisition, new business line, etc.
- For other role (Importer, Distributor, Open-source steward, authorised representatives) no versioning is needed, because the questionnaires applied one time.

DASHBOARD STATUS

- Status table - the user will see a list with all security requirements listed and status. Sample:

#	Security requirement	Requirement Status	Conformity Status
ES01	Secure Product Design	Evaluated	Partial-Compliant
ES02	Secure Development Practices	Evaluated	Not Compliant
ES03	Outsourced Development	Evaluated	Compliant
ES04	Security Testing and Vulnerability Remediation	Not evaluated	In evaluation [Progress* 33%]
ES05	Third-party Component and Supply Chain Management	Evaluated	Not applicable

** Progress computation is a mathematical formula that takes the arithmetic average of all questions related to the respective control (in this example, the security requirement had 3 questions, the user answered only one question)*

- One Pie chart:
 - o Evaluated / Not evaluated [how many of each] and
 - o Compliant / Partially Compliant / Not compliant / Not applicable [how many of each]
- One Pie chart related to task and status [how many of each]
- Progress bar: mathematical formula that takes the arithmetic average of all security requirements (for the "Evaluated" ones it is considered 100%, for the "Not evaluated" ones the completion percentage is taken – e.g. 33%)
- Export Report on PDF



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 5



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 6

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 6
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

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 presents a detailed system design at the use case level.
Keywords
Use cases, diagrams, flow

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.

Table of contents

1.	Introduction	8
2.	Main functions of OSC RAT tool.....	8
2.1.	Use case - Add new product.....	10
2.2.	Use case - Add new product as copy of existing	10
2.3.	Use case - Add new product with data stored in cache	10
2.4.	Use case - Answer question	10
2.4.1.	Answer question details	11
2.4.2.	Use case - Add rationale.....	12
2.4.3.	Use case - Analyse answer	13
2.4.4.	Use case - Attach document.....	13
2.4.5.	Use case - End checklist (not CRA applicable).....	13
2.4.6.	Use case - Establish product classification.....	13
2.4.7.	Use case - Generate task.....	13
2.4.8.	Use case - Go to next question.....	13
2.4.9.	Use case - Store user answer.....	14
2.5.	Use case - Applicability Check.....	14
2.6.	Use case - Delete selected product.....	14
2.7.	Use case - Edit selected product.....	15
2.7.1.	Edit selected product details.....	15
2.7.2.	Use case - Add product activity	16
2.7.2.1.	Add product activity details.....	16
2.7.2.2.	Use case - Add document.....	16
2.7.2.3.	Use case - Add (report) incident.....	17
2.7.2.4.	Use case - Add (report) vulnerability	18
2.7.2.5.	Use case - Send notification.....	18
2.7.2.6.	Use case - Send to CSIRT incident notification.....	18
2.7.2.7.	Use case - Send to CSIRT vulnerability notification	18
2.7.3.	Use case - Add vulnerability to product	18
2.7.4.	Use case - Attach file to product.....	18
2.7.4.1.	Attach file to product details.....	19
2.7.4.2.	Use case - Add CAB assessment.....	19
2.7.4.3.	Use case - Add SBOM.....	20

2.7.4.4.	Use case - Add user manual	20
2.7.4.5.	Use case - Technical documentation.....	20
2.7.5.	Use case - Edit selected product version.....	20
2.7.6.	Use case - Generate SBOM file.....	20
2.7.7.	Use case - Review product incidents.....	20
2.7.7.1.	Review product incidents details.....	20
2.7.7.2.	Use case - Add document.....	21
2.7.7.3.	Use case - Edit selected product incident.....	21
2.7.7.4.	Use case - Save.....	22
2.7.8.	Use case - Review product vulnerabilities.....	22
2.7.8.1.	Review product vulnerabilities diagram.....	22
2.7.8.2.	Use case - Add document.....	23
2.7.8.3.	Use case - Edit selected product vulnerability.....	23
2.7.8.4.	Use case - Save.....	24
2.7.9.	Use case - Save product details.....	24
2.7.10.	Use case - Select product version	24
2.7.11.	Use case - View product log.....	24
2.7.11.1.	View product log diagram	24
2.7.11.2.	Use case - View incident activity log.....	24
2.7.11.3.	Use case - View vulnerability activity log.....	24
2.7.12.	Use case - Vulnerability scan of the SBOM file	25
2.7.13.	Use case - Withdraw product	25
2.8.	Use case - Fill organisation questionnaire.....	25
2.9.	Use case - Fill product questionnaire.....	25
2.10.	Use case - Fill questionnaire	26
2.11.	Use case - Finish questionnaire	26
2.11.1.	Finish questionnaire details.....	26
2.11.2.	Use case - Establish product classification.....	27
2.11.3.	Use case - Generate tasks (to fill the gaps).....	27
2.12.	Use case - Initialise questionnaire.....	27
2.13.	Use case - Load questionnaire state.....	28
2.14.	Use case - Login to OSC RAT.....	28
2.15.	Use case - Recover password	29
2.16.	Use case - Register in OSC RAT.....	29
2.17.	Use case - Reuse questionnaire data	29

2.18.	Use case - Review application main page	29
2.19.	Use case - Review organisation details.....	30
2.19.1.	Review organisation details	30
2.19.2.	Use case - Add organisation document.....	30
2.19.3.	Use case - Configure notifications	31
2.19.4.	Use case - CSIRT Management.....	31
2.19.5.	Use case - ENISA Management.....	31
2.19.6.	Use case - Manage external reporting organisation.....	31
2.19.6.1.	Manage external reporting organisation details	32
2.19.6.2.	Use case - Add reporting organisation.....	32
2.19.6.3.	Use case - Assign reporting organisation to product.....	32
2.19.6.4.	Use case - Edit reporting organisation.....	33
2.19.6.5.	Use case - Remove reporting organisation	33
2.19.7.	Use case - Review organisation users.....	33
2.19.8.	Use case - Save organisation details.....	33
2.20.	Use case - Review organisation products	33
2.21.	Use case - Review organization dashboard	34
2.22.	Use case - Review product dashboard.....	35
2.23.	Use case - Review reports.....	36
2.23.1.	Review reports details.....	36
2.23.2.	Use case - Add report template.....	36
2.23.3.	Use case - Generate conformity assessment report.....	36
2.23.4.	Use case - Generate incidents report.....	37
2.23.5.	Use case - Generate report.....	37
2.23.6.	Use case - Generate vulnerability report	37
2.23.7.	Use case - Remove report template.....	37
2.23.8.	Use case - Review reports templates.....	37
2.23.9.	Use case - Show warning.....	37
2.23.10.	Use case - View selected report	37
2.24.	Use case - Review user organisations.....	37
2.24.1.	Review user organisations details.....	38
2.24.2.	Use case - Add organisation	38
2.24.3.	Use case - Delete organisation.....	39
2.24.4.	Use case - Generate task "Fill organisation questionnaire"	39
2.25.	Use case - Review user profile.....	39

2.25.1.	Review user profile details	40
2.25.2.	Use case - Change password	40
2.25.3.	Use case - Save user profile details.....	40
2.26.	Use case - Review user tasks	40
2.26.1.	Review user tasks details	40
2.26.2.	Use case - Attach file.....	41
2.26.3.	Use case - Edit selected task	41
2.26.4.	Use case - Review task related rationale	41
2.26.5.	Use case - Save task details	42
2.26.6.	Use case - Set task as done.....	42
2.27.	Use case - Save questionnaire state	42
2.28.	Use case - Select organisation	42
2.29.	Use case - Show OSC RAT suggestion based on applicability check result	42

Figures

Figure 1	Main functions of OSC RAT tool.....	8
Figure 2	Answer question details.....	12
Figure 3	Edit selected product details	16
Figure 4	Add product activity details.....	16
Figure 5	Attach file to product details.....	19
Figure 6	Review product incidents details.....	21
Figure 7	Review product vulnerabilities details.....	23
Figure 8	View product log details	24
Figure 9	Finish questionnaire details.....	27
Figure 10	Review organisation details.....	30
Figure 11	Manage external reporting organisation details.....	32
Figure 12	Review reports details.....	36
Figure 13	Review user organisation details	38
Figure 14	Review user profile details	40
Figure 15	Review user tasks details	41

1. Introduction

This appendix forms an integral part of document D2.1 Comprehensive Project Requirements Document. This document presents a detailed system design at the use case level.

2. Main functions of OSCRAT tool

The diagram presents a Use Case model of the OSCRAT system, it reflects the interactions between users and system functionalities. It presents definitions of relationships user type -> functionality and functionality -> functionality, helping to understand what action (or sequence of actions) can be performed by a specific user.

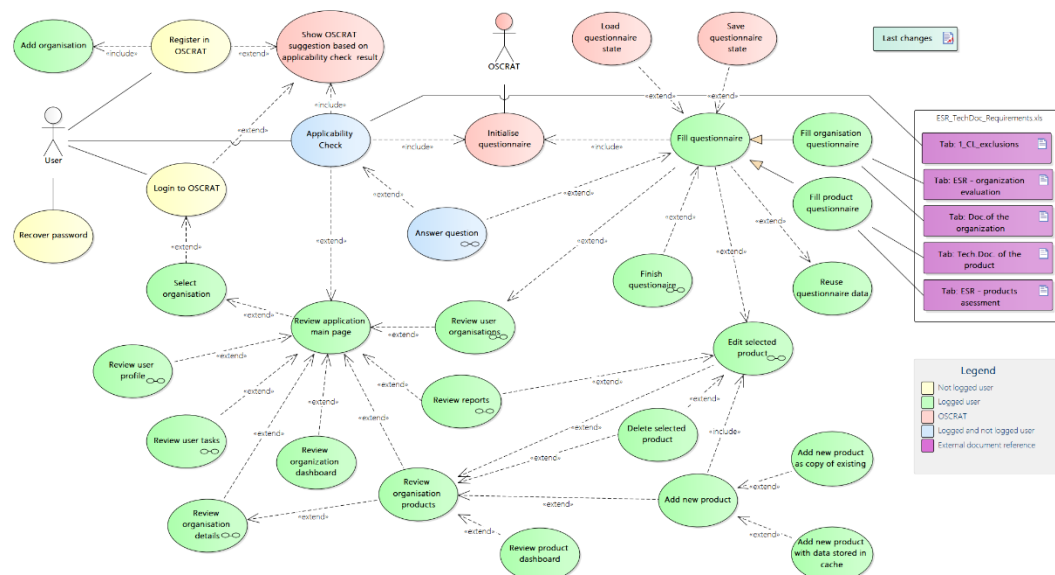


Figure 1 Main functions of OSCRAT tool

The diagram in its upper right corner shows elements grouped under the name ESR_TechDoc_Requirements.xls. It is important to note that this document is a spreadsheet with multiple tabs, which contains all the detailed product requirements resulting from the CRA document. These are not direct requirements for the OSCRAT tool, but in a way they partially enforce a specific functional scope. However, these requirements directly affect the content of the surveys available in the tool.

Actors defined in the diagram:

- User and sub-roles (logged/not logged/logged and not logged) – organization

- OSC RAT – system entity responsible for automatic actions related to questionnaire.

As an unregistered user, you can only perform a limited number of actions in the system. These actions are related to two separate areas: the user and their account, and quick verification of the need to apply CRA requirements. Within the account, an unregistered user can:

- UC: register in the system;
- UC: log in to the system;
- UC: recover the password to their account.

Regardless of whether the user has an account in the OSC RAT system, they can verify the need to apply CRA requirements (UC: Applicability check) at any time by completing a specially prepared questionnaire (UC: answer question).

Quick verification of the need to apply CRA requirements ends in two ways (UC: show OSC RAT suggestion based on pre-questionnaire result):

- no such need and no further action;
- the possibility to log in to the system and perform further support activities offered by the OSC RAT tool.

The functions available to logged-in users include:

- UCs: add, select, edit, and review organization (and details);
- UCs: edit and review user profile;
- UCs: review user tasks;
- UCs: add, edit, delete, and review product;
- UCs: review organization and product dashboards;
- UCs: review reports (i.e. for product);
- UCs: fill additional questionnaires.

It is worth noting here that the user has the option of using previously provided information (when completing the first questionnaire) when adding a product (UC: add new product with data stored in cache). However, when completing the same questionnaire again, it is pre-filled with the previously provided answers (UC: reuse questionnaire data).

Completing each questionnaire is supported by actions performed by the OSC RAT system in the background, which cause: initialization of the questionnaire (UC: initialize questionnaire), saving its status after each answer provided by the user (UC: save questionnaire state), and restoring it to its previous status in the event of interruption (UC: load questionnaire state).

At any time, from the main application window, the user has access to the most important functions and views of the tool:

- products;
- organization;
- dashboards;
- reports;
- tasks;
- user profile.

2.1. Use case - Add new product

The user selects the "Add new product" option. The system displays a window with fields for the new product. The user fills in the fields and selects the "save" option. The system adds the new product in the context of the organization and displays the updated list of organization products.

Fields (* required):

- product acronym/short name (short text)*
- product full name (short text)*
- product version (short text)*
- product short description (long text)

On successful add: Generate task "fill pre-questionnaire for product" -> determining the class of the product

2.2. Use case - Add new product as copy of existing

The system displays a window with list of existing products User edit/adds required data and saves changes.

2.3. Use case - Add new product with data stored in cache

The user selected the "Add new product" command. The system displays a window with option to add new product with data stored in cache. User selects this option. System displays form for adding new product partially fulfilled with data from cache (from applicability check questionnaire). User adds required data and saves changes.

2.4. Use case - Answer question

During filling questionnaire user answers for questions. Question is served by system one by one. After answer system can take actions according to the answer

(list of possible actions below). Possible actions depend on question, questionnaire type or previously answers.

For each answer user can add rationale (test) or attach one or more files as evidence or rationale.

Input:

- Database, XML, JSON or other data source with questionnaire.
- Questionnaire - list of questions and list of required/possible actions for each possible answer (based on .xls set of questions).

Condition:

- questionnaire started (initialized)

Possible types of answers:

- single answer
- multiple answers

For each question system should provide:

- content of the question - (short text)
- hints - detailed description (explanations, definitions) to help applicant to answer - long text
- reference to source of question (e.g. "CRA Article 14(2)" - (short text)

The actions can be involved during questionnaire filling or later during answer analysis for the report (depending on question or system designer decision)

- CRA Not applicable - only during pre-questionnaire, ending questionnaire for not CRA applicable product
- Create related task - the answer can be implicit to take some activity for applicant (e.g. implicit requirement to third party assessment, prepare documents like security policy or some establish procedures or other activities to fill detected gaps)
- Go to question - go to specified question (to maintain workflow or skip a not related block of other questions)
- Mark not applicable questions - given answer can make some questions from current or other questionnaire not applicable (pointless), the system should mark them to ask them for the applicant
- Implicit product classification - the result of the answer can establish the product type.

2.4.1. Answer question details

When answering survey questions, users can supplement their answers by adding additional information in the form of external program files (UC: attach document). Users can also add a justification (UC: add rationale) at any time. Users can move on to the next question at any time (UC: go to next question).

In the background, the OSCRAT tool performs several tasks. First, it saves the user's answer (UC: store user answer). If this is the last question, the system ends the survey and displays a recommendation (UC: end checklist). In some cases, the system analyses the answer provided (UC: analyse answer) and performs additional tasks that may make it easier for the user to work with the tool in the future (UCs: establish product classification, generate task).

To establish product classification, there is a diagram (product classification workflow), which could be helpful.

To generate right task - there is the technical document with additional information (ESR_Tech_Doc_Requirements.xls).

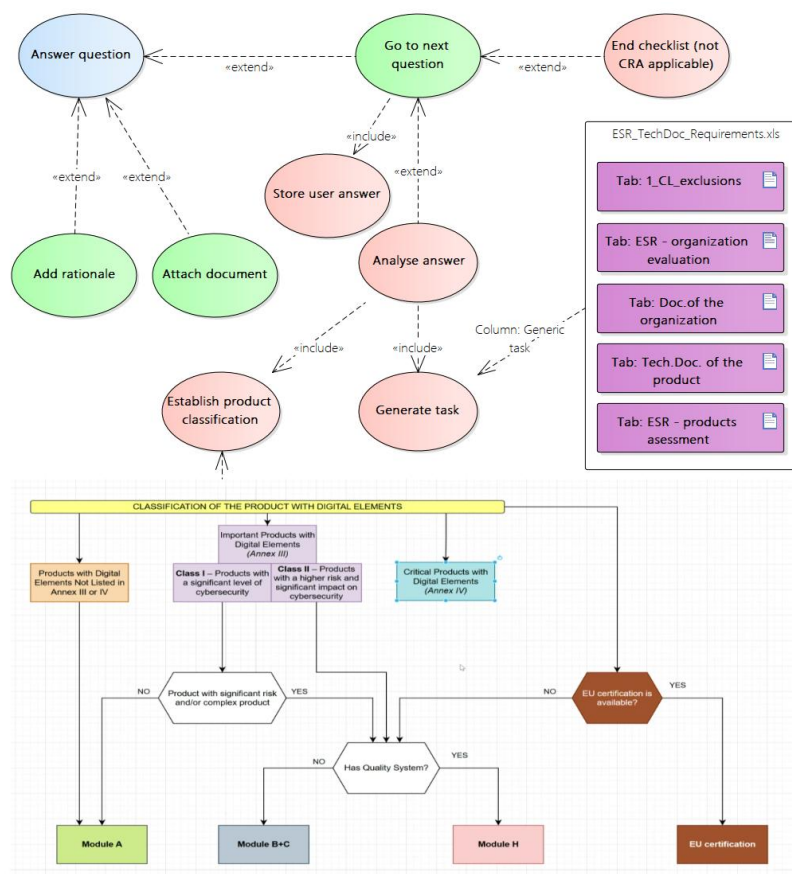


Figure 2 Answer question details

2.4.2. Use case - Add rationale

For each answer system delivers possibility to add rationale via large text field. User adds rationale. System saves changes.

2.4.3. Use case - Analyse answer

Possible action taken on answer:

- Establish product classification (Only during applicability check)
- generate task (Only during assessment)

2.4.4. Use case - Attach document

For each answer system delivers possibility to add document. User adds external file. System delivers possibility to add file with information:

- document identifier or label
- document version
- short description
- document type (e.g. procedure, policy)

System saves changes.

2.4.5. Use case - End checklist (not CRA applicable)

CRA Not applicable (only during applicability check) - ending questionnaire for not CRA applicable product (system shows appropriate message with no following action needed "Product not CRA applicable - no OSC RAT tool needed")

2.4.6. Use case - Establish product classification

Only during applicability check. Classification is based on CRA

2.4.7. Use case - Generate task

Only for assessment questionnaire. Generate OSC RAT task for user based on column: Generic task.

2.4.8. Use case - Go to next question

After answer system should:

- store answer,
- take appropriate action (if applicable),
- go to next or specified question (if no finish)
- or finish questionnaire (when end of questions or product not CRA eligible).

In any time user can stop work with the questionnaire and go back later in any time and system should restore questionnaire state to allow user to resume filling.

Obligatory system action:

- store user answer

Possible action taken after choosing to answer and clicking "Next question" (depending on question):

- End questionnaire (when not CRA applicable)
- Go to specified question (to continue or skip some questions)
- Exclude not applicable questions (from current and/or another questionnaire).

2.4.9. Use case - Store user answer

For not logged in users (during pre-questionnaire) system stores user session and given answers. System delivers possibility to allow users to take a break and get back later. Saving questionnaire state is done on the fly after each answer.

2.5. Use case - Applicability Check

Applicability Check (Fill pre-questionnaire)

On system web page unregistered user can start prequestionnaire to estimate CRA applicability for product.

This questionnaire contains a limited set of questions necessary to estimate CRA applicability for product (ref. document: CRA_oblig_req.xlsx, worksheet "1_CL_exclusions").

Results of this questionnaire:

- end of activity - if product is not CRA eligible (present the information to the user that the product is not a subject to CRA requirements),
- suggestion of using the OSC RAT tool - if a product is CRA applicable:
 - present the information that the product is CRA eligible,
 - the class of the product (critical/important class I/II/ other PDE);
 - the user can register or login to complete the assessment and e.g. a link, redirection to the login/registration page).

System delivers possibility to allow users to take a break and get back later. Saving questionnaire state is done on the fly after each answer.

2.6. Use case - Delete selected product

The user has selected the product removal item. The system asks for confirmation of the action. If the user confirms, the system deletes all information related to the product and the product itself. If the user does not confirm, the system returns to displaying the product list without changes.

2.7. Use case - Edit selected product

The user has selected the edit product item. The system displays a window with information about the product. The user browses the product details. The system allows you to make changes to the product. Additionally, the system allows you to:

- withdraw the product
- view the event log for the product
- add a file to the product (SBOM, user manual, CAB assessment, technical documentation, other)
- generate an SBOM file
- scan the SBOM file
- view vulnerabilities detected for the product
- view incidents reported for the product
- save the changes made.

2.7.1. Edit selected product details

Editing a selected product is divided into two separate parts: editing the entire product and managing product versions.

For the entire product, the logged-in user can manage external reporting organizations, withdraw the product, and save basic product information (UCs: manage ext. organizations/save/withdraw).

Extended information is available for a specific product version, selected from a list. This information includes:

- viewing the history of operations performed for the product (UC: view log)
- adding an additional external file (UC: attach file)
- adding an activity performed for the product (UC: add activity)
- viewing vulnerabilities and incidents (UCs: review vulnerabilities/incidents)
- analysing the SBOM file (UC: analyse SBOM).

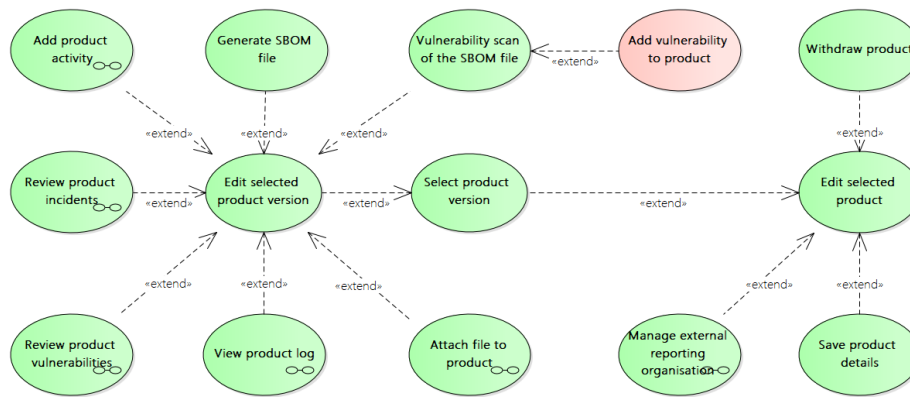


Figure 3 Edit selected product details

2.7.2. Use case - Add product activity

The user selects the option to add an activity for the product version. The system displays the available options: vulnerability - incident. The user selects the appropriate one. Further actions are taken according to the relevant use case.

2.7.2.1. Add product activity details

Adding an activity for a product version means registering a vulnerability or incident for it. For both, it is possible to supplement the information by attaching an external file with written details or a description of the action. Adding an activity always involves sending a notification to the external organization that has been assigned to the product.

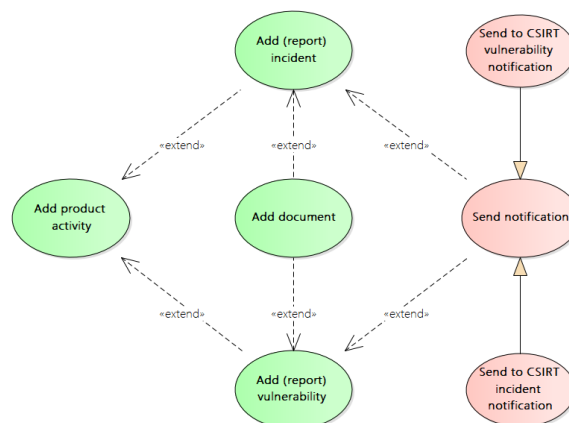


Figure 4 Add product activity details

2.7.2.2. Use case - Add document

For each activity/incident/vulnerability the user has an option to attach one or more files (e.g. evidence, reports, notes etc).

During file attachment system delivers possibility to fill:

- document identifier or label
- document version
- short description
- document type (e.g. procedure, policy, report, note etc.)

2.7.2.3. Use case - Add (report) incident

Use case description

For selected product the user selects option to report incident. OSC RAT tool shows window with fields:

- Incident types:
 - General
 - Confidentiality
 - Integrity
 - Availability
 - Access control
 - Vulnerabilities
 - Technical failure
 - Theft or loss equipment

Attack types:

- Denial of service
- Unauthorized access
- Malware
- Abuse
- Others

Incident details):

- Reporter/Incident Commander
- Description
- Classification/Type
- Attack type
- Assets details

Treatment details:

- Corrective action (Describe the actions that will mitigate and minimise their impact on the future incident)
- Root cause (Describe the root cause of the incident)
- Scope (What is the scope for the future treatment of such incident recurrence)

- Preventive action (List the actions that the organization is taking to prevent such incident in near future).

2.7.2.4. Use case - Add (report) vulnerability

For selected product the user selects option to report a vulnerability. OSC RAT tool shows window with fields:

Vulnerability report should contain:

- Name (short text)
- Description (long text)
- Severity
- Type

2.7.2.5. Use case - Send notification

System generates notification to user. General Use case, see specialized use cases.

2.7.2.6. Use case - Send to CSIRT incident notification

System generate e-mail body based on template and OSC RAT database data related to incident.

2.7.2.7. Use case - Send to CSIRT vulnerability notification

System generate e-mail body based on template and OSC RAT database data related to vulnerability.

2.7.3. Use case - Add vulnerability to product

The external tool found vulnerabilities for the product while analysing the SBOM file. The OSC RAT tool shows vulnerabilities. The user selects vulnerabilities and adds them to the product.

Vulnerability details:

- Severity (CVSS base score)
- Summary
- Affected product (vendor, product and version)
- Advisory IDs (if any)
- Vulnerability information (Published, updated, assigner)
- References

2.7.4. Use case - Attach file to product

The user selected the "Attach file to product" option. The system displays a window in which it is possible to select a file from the file system and indicate the type of document. The user searches for the file and confirms the action. The system adds the specified file and associates it with the product.

For each product applicant should have an option to attach multiple files.

Possible predefined product file types to attach:

- CAB Assessment
- User manual
- SBOM
- Technical documentation
- other

During attaching the file, there should be options available to add:

- document identifier or label,
- document version,
- short description,
- document type (if 'other')

2.7.4.1. Attach file to product details

Adding an external file for a product means that you can add one of the following types of documents:

- CAB assessment
- user manual
- SBOM
- technical documentation

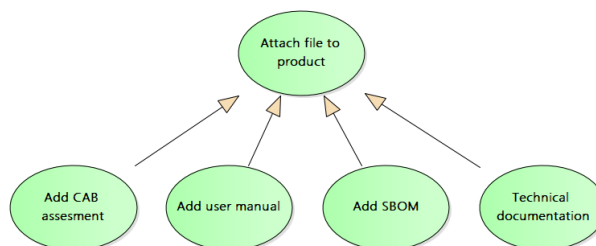


Figure 5 Attach file to product details

2.7.4.2. Use case - Add CAB assessment

Documents, reports from an external assessment laboratory that can be imported for a given product, as proof of compliance with the requirements.

See "Attach file to product".

2.7.4.3. Use case - Add SBOM

See "Attach file to product".

2.7.4.4. Use case - Add user manual

See "Attach file to product".

2.7.4.5. Use case - Technical documentation

See "Attach file to product".

2.7.5. Use case - Edit selected product version

The user has selected the edit product version item. The system displays a window with information about the product version. The user browses the product version details. The system allows you to make changes to the product version.

Additionally, the system allows you to:

- withdraw the product version
- view the event log for the product version
- add a file to the product version (SBOM, user manual, CAB assessment, technical documentation, other)
- generate an SBOM file
- scan the SBOM file
- view vulnerabilities detected for the product version
- view incidents reported for the product version
- save the changes made.

2.7.6. Use case - Generate SBOM file

The user selected the "Generate SBOM file" item.

The OSC RAT system can use an external tool to prepare an SBOM file for a software project. This may require setting the path of that software project. This path, passed as a parameter to the external tool, will allow browsing the project files and generating a list of components in the form of an SBOM file.

2.7.7. Use case - Review product incidents

The user selected the "Review product incidents" item. The system displays a window that displays all incidents registered for the product. The user browses the incidents. The system allows to select an item from the list. For the selected item, the system provides an option to edit it.

2.7.7.1. Review product incidents details

From the incident overview level for a product, it is possible to view the details of a selected incident and edit its parameters (UCs: edit, add document, save). It is also possible to register a new incident (UC: add incident).

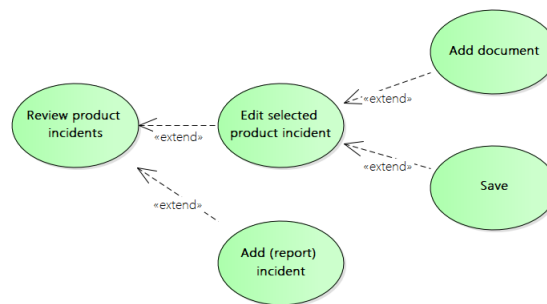


Figure 6 Review product incidents details

2.7.7.2. Use case - Add document

The user selected the option to add the document to the incident. The system displays a window in which it is possible to select a file from the file system and indicate the type of document. The user searches for the file and confirms the action. The system adds the specified file and associates it with the incident.

For each incident applicant should have an option to attach one or more files.

During file attachment should be available options to add:

- document identifier or label
- document version
- short description
- document type (e.g. procedure, policy, report).

2.7.7.3. Use case - Edit selected product incident

The user has selected the option to edit the incident. The system displays a window with the incident details. The system allows you to edit the incident details. The system allows you to set the incident status to one of:

- open
- closed
- <other>

The system provides an option to add an activity or document to the incident.

Incident types:

- General
- Confidentiality
- Integrity

- Availability
- Access control
- Vulnerabilities
- Technical failure
- Theft or loss equipment

Attack types:

- Denial of service
- Unauthorized access
- Malware
- Abuse
- Others

Incident details:

- Reporter/Incident Commander
- Description
- Classification/Type
- Attack type
- Assets details

Treatment details:

- Corrective action (Describe the actions that will mitigate and minimize their impact on the future incident)
- Root cause (Describe the root cause of the incident)
- Scope (What is the scope for the future treatment of such incident recurrence)
- Preventive action (List the actions that the organization is taking to prevent such incident in near future).

2.7.7.4. Use case - Save

The user selects "Save". The system saves the changes.

2.7.8. Use case - Review product vulnerabilities

The user selected the "Review product vulnerabilities" item. The system displays a window that displays all vulnerabilities registered for the product. The user browses the vulnerabilities. The system allows to select an item from the list. For the selected item, the system provides an option to edit it.

2.7.8.1. Review product vulnerabilities diagram

Reviewing vulnerabilities for a product boil down to managing them by: adding, editing, adding an external document and saving.

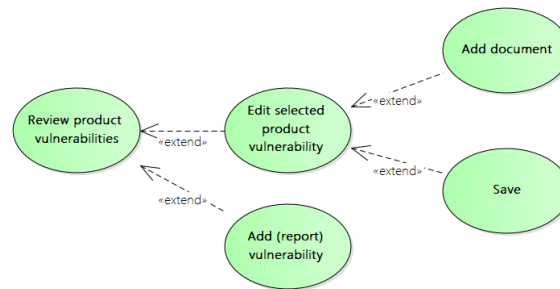


Figure 7 Review product vulnerabilities details

2.7.8.2. Use case - Add document

The user selected the option to add the document to the vulnerability. The system displays a window in which it is possible to select a file from the file system and indicate the type of document. The user searches for the file and confirms the action. The system adds the specified file and associates it with the vulnerability.

For each vulnerability applicant should have an option to attach one or more files.

During file attachment should be available options to add:

- document identifier or label
- document version
- short description
- document type (e.g. procedure, policy, report)

2.7.8.3. Use case - Edit selected product vulnerability

The user has selected the option to edit the vulnerability. The system displays a window with the vulnerability details. The system allows to edit the vulnerability details. The system allows to set the vulnerability status to one of:

- open
- not fixed and closed
- fixed and closed
- <other>

The system provides an option to add an activity or document to the vulnerability.

Vulnerability details:

- Severity (CVSS base score)
- Summary

- Affected product (vendor, product and version)
- Advisory IDs (if any)
- Vulnerability information (Published, updated, assigner)
- References

2.7.8.4. Use case - Save

The user selects "Save". The system saves the changes.

2.7.9. Use case - Save product details

The user selects "Save". The system saves the changes.

2.7.10. Use case - Select product version

The user selects a product version from the list. The OSC RAT tool displays detailed information about the product version and provides additional options for editing the product and its version.

2.7.11. Use case - View product log

The user selects the "Review product log" item. The system displays the event log window. The window displays a list of events registered in the OSC RAT platform for the product version. The user browses the list of events. The system allows you to indicate a single entry. For the selected item, the system allows you to display the entry details.

System delivers possibility to filter logs by:

- vulnerability activities
- incident activities
- handling activities

2.7.11.1. View product log diagram

Viewing the activity history for a product means viewing the history of recorded vulnerabilities or incidents.



Figure 8 View product log details

2.7.11.2. Use case - View incident activity log

See "view product log" use case.

2.7.11.3. Use case - View vulnerability activity log

See "view product log" use case.

2.7.12. Use case - Vulnerability scan of the SBOM file

The user selected the "Scan SBOM" item.

Analysis of SBOM can be made by external tool (e.g. trivy, gype, OWASP dependency check, ...), via a command called from OSC RAT tool. User of OSC RAT can initiate analysis and get the result of this action.

Result of this analysis - the report with the list of vulnerabilities.

2.7.13. Use case - Withdraw product

The user selected the "withdraw product" item. The system asks to confirm the action. If the user confirms, the system sets the "withdrawn" flag. The system does not delete product information. The system blocks adding new elements for the product (documents, actions, analyses, incidents, vulnerabilities, ...). If the user does not confirm - the system returns to displaying product information without making any changes.

2.8. Use case - Fill organisation questionnaire

Questionnaire for organization assessment (questions from CRA related to organization)

Question lists depend of organization role.

Organization Role-Specific Questionnaires

- Manufacturer → Sheet 3a_ESR – organization assessment
- Importer → Sheet 4a_cl - organization assessment
- Distributor → Sheet 5a_CL - organization assessment
- Open-source steward → Sheet 6a_CL - organization assessment
- Authorized representative → Sheet 7a_CL - organization assessment

2.9. Use case - Fill product questionnaire

Questionnaire for product assessment (questions from CRA related to product)

Question lists depend of organization role.

Organization Role-Specific Questionnaires

- Manufacturer → Sheet 3b_ESR – product assessment
- Importer → Sheet 4b_cl - product assessment
- Distributor → Sheet 5b_CL - product assessment
- Open-source steward → no questionnaire

- Authorized representative → Sheet 7b_CL - product assessment

2.10. Use case - Fill questionnaire

Condition: Have a product

Questionnaire is set of the "Answer question" use case activities.

For each product a user has only one active questionnaire.

Questionnaire can be:

- active (in progress) - only one per product and one of each type of questionnaire per product (To Be Agreed)
- closed (archival) - multiple per product.

User can start new questionnaire after closing active.

User selects option "start questionnaire" from the view of product or organization.

System shows questionnaire with questions comes from concrete definition file: product, organization, CRA applicability.

See also the use case "Answer question".

2.11. Use case - Finish questionnaire

User selects option to finish questionnaire. If no more questions are left, system saves answers given. System enables functionality connected with report generation.

2.11.1. Finish questionnaire details

The user can finish filling out the questionnaire at any time (UC: finish questionnaire). In this case, the OSCART tool performs additional tasks that may make it easier for the user to work with the tool in the future (UCs: establish product classification) and generate tasks for product classification based on presented workflow, for applicability questionnaire.

To establish product classification, there is a diagram (product classification workflow), which could be helpful.

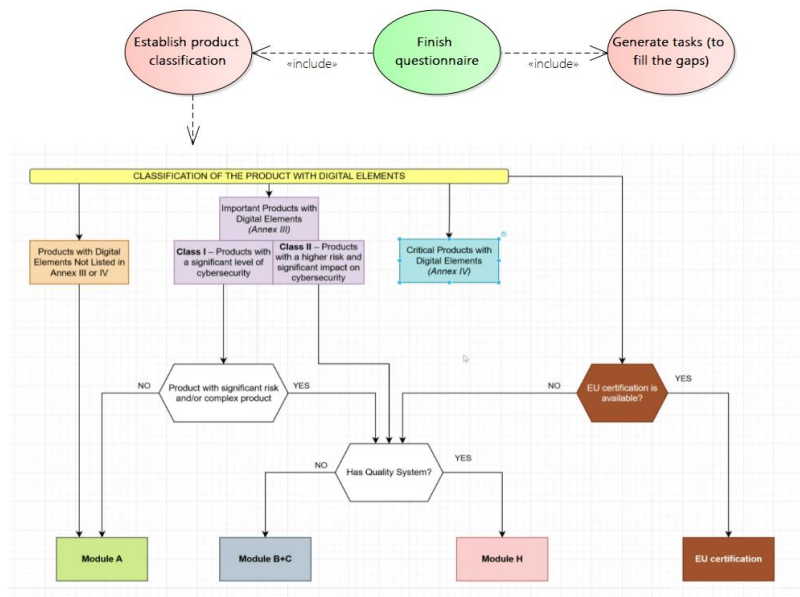


Figure 9 Finish questionnaire details

2.11.2. Use case - Establish product classification

System OSC RAT perform analysis of responses to set a product classification.

2.11.3. Use case - Generate tasks (to fill the gaps)

System OSC RAT prepares list of tasks for a user to do to fill detected gaps.

2.12. Use case - Initialise questionnaire

The OSC RAT tool prepares (serves) the list of questions for main assessment or pre-checklist.

Checklist questions will be downloaded from an external file, dynamically adjusted, depending on the stage of user's activities:

- 1) pre-checklist - checking exclusions and class of the product (ref. document - CRA_oblig_req.xlsx, "1_CL_Exclusions")
- 2) gathering information about the organization (ref. document - CRA_oblig_req.xlsx, "2_CL_Organization")
- 3) Product conformity requirements (CRA_oblig_req.xlsx, worksheet "4_CL_Sec_Req_Pua"):
- 3(a) Product management and documentation (CRA_oblig_req.xlsx, worksheet "4_CL_Sec_Req_Pua") - requirements related to technical aspect, the way of implementation, life cycle (including end of life), labelling, required documentation (Annex VII)

- 3(b) risk assessment Q&As that helps to check if the risk assessment process has been correctly performed (ISO/IEC 27005, ISO/IEC 31000):
 - external and internal context of the product use, intended use, conditions of use specified,
 - risk analysis: risk identification (threats, existing controls, vulnerabilities) and risk level estimation performed (e.g. based on level of consequences, likelihood, probability of occurrence),
 - risk evaluation (criteria selected and risk prioritization performed),
 - risk treatment plan defined,
 - risk acceptance criteria established, and the risk level controlled.
- 3(c) Incident management process (CRA_oblig_req.xlsx, worksheet "4_CL_Sec_Req_Pua", requirements of ISO/IEC 30111 - checklist in progress) - Article 14
- 3(d) Vulnerability management process (CRA_oblig_req.xlsx, worksheet "4_CL_Sec_Req_Pua", requirements of ISO/IEC 29147 - checklist in progress) - Articles 13, 14

The list of questions displayed to the user in point 3) is adjusted, depending on previous form responses and answers provided. For example, based on the answers to the questions about the user's organization type (from worksheet 2_CL_Organization), the scope of questions for the user will be different if the assessment is conducted by the manufacturer, and different if by the importer/distributor. Similarly, the scope will be different, depending on the answers to the questions about the class of the assessed product (e.g. important, critical - as described in questions 1_CL_Exclusions, section 1.10, 1.11).

2.13. Use case - Load questionnaire state

User selects questionnaire to reopen. During questionnaire opening process system loads the state. System shows partially filled questionnaire.

2.14. Use case - Login to OSC RAT

If the user has an account on the OSC RAT platform, they can log in. The login procedure is available after selecting the "Login to OSC RAT platform" option available on the main page.

After successful authentication, the user selects the further path:

- 1. The user wants to review the organizations to which they have access and within which they can perform actions in OSC RAT. In this case, the user indicates the "Review user organizations" option displayed on the main panel.

- 2. The user wants to perform actions within an existing organization. In this case, the user indicates the "Select organization" option displayed on the main panel.

2.15. Use case - Recover password

If a user forgets their account password, they can recover access to their account. The account recovery form and procedure are launched after selecting the "Recover password" option available on the main page.

2.16. Use case - Register in OSC RAT

If the user does not yet have an account on the OSC RAT platform, the user can create one. The account creation form is available after selecting the "Register in OSC RAT platform" option available on the main page.

The system displays a registration form with fields:

- name
- email address
- password (of appropriate strength, see use-case "Recover password")

In addition to basic information, the user indicates the organization to which they want to gain access. If the organization is not on the list, they select the "add organization" option. In such a situation, the system displays an additional field for entering the name of the organization. The user confirms the entered data. The system creates a new user.

If the user wants to gain access to an existing organization - the system sets the user's permission level to "pending". If an organization is also added - the system creates the organization and adds the added user with permissions at the owner level.

2.17. Use case - Reuse questionnaire data

If user fill the same questionnaire one more time (for reassessment) system provides previously used data and answers to speedup reassessment process.

2.18. Use case - Review application main page

The system displays the platform's main page. The system provides options that allow to:

- browse the logged-in user's profile
- browse the user's tasks
- browse detailed information about the organization
- browse products belonging to the organization

- browse reports
- fill in applicability check to check if a new product should be added and assessed
- review organization dashboard

2.19. Use case - Review organisation details

The user selected the command "Review organisation details". The system displays a window with information about the organisation. The user reviews the information. The system allows editing information about the organisation.

In addition, the system allows:

- adding a document related to the organisation (policy, procedure, report, ...)
- browsing the organisation's products
- browsing the organisation's users
- managing connections with external organisations such as CSIRT or ENISA
- saving the changes made.

2.19.1. Review organisation details

A logged-in user can view data about their organizations. To do this, they select an organization in the main window of the tool. For this organization, the tool allows them to view its users, documents, and products (UCs: review users/products). It also allows them to edit and save changes made to the organization's data (UC: save). Each organization can have external organizations defined for each product, which will be notified of vulnerabilities or incidents, for example. The global list of such external organizations can be managed from the organization level (UC: manage external reporting organization).

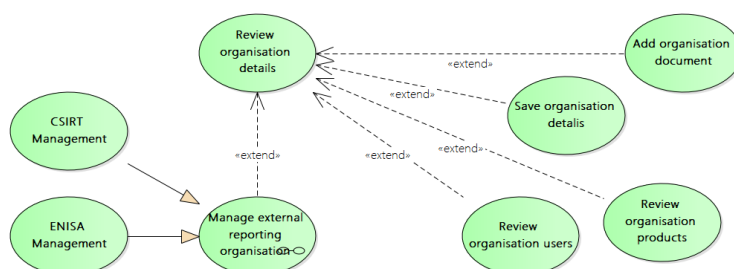


Figure 10 Review organisation details

2.19.2. Use case - Add organisation document

The user selects the "Add organization document" option. The system displays a window with the ability to browse the file system. The user browses the file system and indicates the file to add.

The user selects the type of document from the list:

- policy
- procedure
- certificate
- other

For each organization the user has an option to attach multiple files.

During file attachment there are options available to add:

- document identifier or label
- document version
- short description
- document type (if other)

The user confirms the entered information. The system adds the file to the system and associates it with the organization.

2.19.3. Use case - Configure notifications

The user adds or edits the parameters of an external organization and goes to the window that allows editing notification parameters. The system allows you to define the following values:

- what the notification concerns (incident, vulnerability, report);
- notification template (notification content)
- email address to which the notification will be sent.

2.19.4. Use case - CSIRT Management

See "Manage external reporting organisation". CSIRT is one of external reporting organisation.

2.19.5. Use case - ENISA Management

See "Manage external reporting organisation". ENISA is one of external reporting organisation.

2.19.6. Use case - Manage external reporting organisation

User selects option to show external reporting organizations. System shows list of external reporting organisations, user can add new or select one from list and:

- view details
- delete
- edit

- assign to selected own organisation
- assign to selected product

External reporting organization (See CRA Art 15.1):

- CSIRT
- ENISA

2.19.6.1. Manage external reporting organisation details

Managing external organizations involves viewing and editing the list of such organizations. Adding and editing an external organization involves entering the appropriate values in the relevant fields and configuring notifications sent to it (UCs: add/edit organization, configure notification). Each external organization can also be removed from the list (UC: remove).

Additionally, each product of an organization can be linked to other external organizations (UC: assign reporting organization to product).



Figure 11 Manage external reporting organisation details

2.19.6.2. Use case - Add reporting organisation

User selects option to add new organization. System displays form where user can input external reporting organisation details to add it to the system

- Name (short text)
- Acronym (short text)
- Type ENISA/CSIRT (See CRA Art 15.1)
- Other

2.19.6.3. Use case - Assign reporting organisation to product

The list of organizations (CSIRTs, ENISA) to which vulnerability or incident reports will be sent can be associated with the product to which these reports will apply.

System shows list of organizations. User selects organization. System shows products. User selects (one or more) product and decide, witch kind of report will be sent to that organization. System saves state.

2.19.6.4. Use case - Edit reporting organisation

User selects edit details of external reporting organisation.

System displays form with details to allow user to edit it. User edits values and saves them on cancels editing.

2.19.6.5. Use case - Remove reporting organisation

User deletes selected external reporting organisation.

In case when organisation have assigned some products system displays message and not allow to delete it.

2.19.7. Use case - Review organisation users

The user selects the option "Review organization users". The system displays a window with a list of users who are assigned to the given organization. The list contains all users assigned to the organization along with their level of authorization. The user reviews the list of users.

Privileges levels:

- owner/manager (can edit or delete organisation or products)
- viewer/partner (only can view organization details and products)
- pending (nothing can do, waiting for give privileges from rest above)

Owner of organisation can assign other users (give permissions) to organisation.

2.19.8. Use case - Save organisation details

The user selects "Save". The system saves the changes.

2.20. Use case - Review organisation products

The user selected the "Review organisation products" command. The system displays a window with a list of products that have been entered into the organisation. The user browses the product list.

The system allows to add a new product.

Additionally, the system allows to select an item from the product list. For the selected product, the system provides more options:

- editing the indicated product
- deleting the indicated product
- review product dashboard

2.21. Use case - Review organization dashboard

The system provides a dynamic dashboard view summarizing compliance progress for each organization assessment. This dashboard includes a status table, charts, a progress bar, and export to PDF.

Dashboard Components

- 1. Status Table

A table listing all requirements, their evaluation status, and conformity results.

Columns:

 - Requirement Identifier
 - Requirement Name
 - Requirement Status → Evaluated / Not Evaluated
 - Conformity Status → Compliant, Partially Compliant, Not Compliant, In Evaluation (e.g., 33%), or Not Applicable
 - Progress computation formula: average of answered questions for the requirement (e.g., 1 of 3 answered → 33%).
- 2. Pie Charts

Chart A:

 - Evaluated vs. Not Evaluated (count of requirements)
 - Breakdown of Compliant / Partially Compliant / Not Compliant / Not Applicable

Chart B:

 - Task distribution by type & status (e.g., auto-generated, manual, closed)
- 3. Progress Bar
 - Computed as the arithmetic average of all requirements:
 - Evaluated requirements → 100%
 - Not Evaluated requirements → use their completion percentage (e.g., 33%).
- 4. Export Conformity Assessment Report
 - The dashboard must be exportable as a PDF file, including:
 - Organization identifier

- Status table, questions and given answers (with rationales if added)
- Charts
- Progress bar
- Timestamp of export

2.22. Use case - Review product dashboard

The system provides a dynamic dashboard view summarizing compliance progress for each product assessment. This dashboard includes a status table, charts, a progress bar, and export to PDF.

Dashboard Components

- 1. Status Table

A table listing all requirements, their evaluation status, and conformity results.

Columns:

- Requirement Identifier
- Requirement Name
- Requirement Status → Evaluated / Not Evaluated
- Conformity Status → Compliant, Partially Compliant, Not Compliant, In Evaluation (e.g., 33%), or Not Applicable
- Progress computation formula: average of answered questions for the requirement (e.g., 1 of 3 answered → 33%).

- 2. Pie Charts

Chart A:

- Evaluated vs. Not Evaluated (count of requirements)
- Breakdown of Compliant / Partially Compliant / Not Compliant / Not Applicable

Chart B:

- Task distribution by type & status (e.g., auto-generated, manual, closed)

- 3. Progress Bar

- Computed as the arithmetic average of all requirements:
- Evaluated requirements → 100%
- Not Evaluated requirements → use their completion percentage (e.g., 33%).

- 4. Conformity Assessment Report

- The dashboard must be exportable as a PDF file, including:
- Product and organization identifiers
- Status table, questions and given answers (with rationales if added)

- Charts
- Progress bar
- Timestamp of export

2.23. Use case - Review reports

The user selected the "Review reports" item. The system displays a window that displays all reports for the organization (including product reports). The user browses the reports. The system allows to select an item from the list. For the selected item, the system provides an option that allows to edit it.

The system allows to review reports templates.

The system allows to generate a report using one of the templates added to the system.

2.23.1. Review reports details

The OSC RAT tool can generate various types of reports (UCs: generate report). Reports are based on templates that logged-in users can add to their own organization (UCs: review reports templates, add/remove report template). Currently, there are three different types of reports: conformity assessment, incidents and vulnerabilities. Each generated report can be viewed in the tool (UC: view selected report).

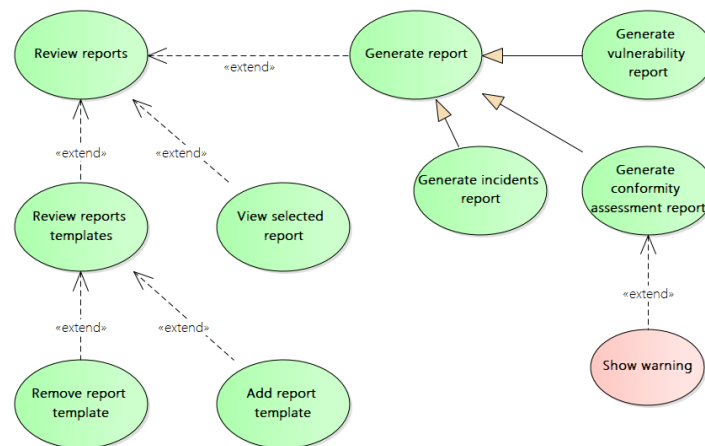


Figure 12 Review reports details

2.23.2. Use case - Add report template

The user selects an option to add template for selected type of report.

Template contains layout of report (header, footer, fonts, logo, etc.)

2.23.3. Use case - Generate conformity assessment report

Generate assessment report based on template. See "Generate report" use case.

2.23.4. Use case - Generate incidents report

Generate incident report based on template. See "Generate report" use case.

2.23.5. Use case - Generate report

The user selects the "Generate report" item. The user indicates what type of report should be generated. The system generates a report based on the specified report template and adds it to the system in the context of the organization.

2.23.6. Use case - Generate vulnerability report

Generate vulnerability report based on template. See "Generate report" use case.

2.23.7. Use case - Remove report template

The user selects option to remove report template. System removes template.

2.23.8. Use case - Review reports templates

The user selects the "Review reports templates" option. The system displays a window that displays all templates for reports with information about their usage. The user browses the templates.

The system allows to add new template for selected type of report (conformity assessment, SBOM, incidents, vulnerabilities, product version releases)

The system allows to select an item from the list. For the selected item, the system provides an option that allows to remove it (in case it is not used).

2.23.9. Use case - Show warning

The system shows hit/warning for user that "If You have changes in ... (list cases when re assessment may be required)" you should do reassessment!

2.23.10. Use case - View selected report

The user selects the "View report" item. The system displays the report in a separate window. The system provides an option to print the report. The system provides an option to save the report in the local file system.

2.24. Use case - Review user organisations

The system displays a list of organizations to which the user has access. The user browses the list of organizations. The system allows to select an organization from the list. For the selected item, the system displays the "Delete organization" option.

The system displays the "Add new organization" option.

2.24.1. Review user organisations details

Each user registered in the OSC RAT tool can be assigned to any number of organizations. In the OSC RAT tool, due to the lack of such a necessity, it was decided not to implement advanced organization management. Therefore, each user can add or join a selected organization or a new organization they have created themselves. They can also delete their organization, with the proviso that all data related to that organization will be unavailable.

Additionally, when creating an organization, the OSC RAT tool will generate a reminder task for that user (UC: generate task - fill organization questionnaire).

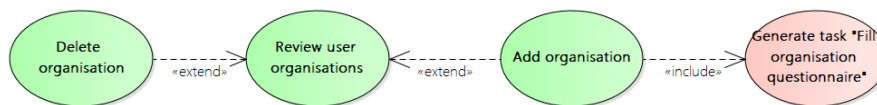


Figure 13 Review user organisation details

2.24.2. Use case - Add organisation

The user selects option to add new organisation. The system shows form with fields:

- organization name - short text field
- tax ID - short text field (optional)
- type: natural person/legal person - 2 radio buttons (file: ESR_TechDoc_Requirements.xlsx, tab 2_CL_Organization, question 2.1 <https://cloud.unicis.tech/f/229087>)
- organization size: micro, small, medium, other - 4 radio buttons (file: ESR_TechDoc_Requirements.xlsx, tab 2_CL_Organization, question 2.2 <https://cloud.unicis.tech/f/229087>) (add hints/details e.g. number of employers)
- organization role (radio button selection: Manufacturer, Authorized representative, Open-source software steward, Importer, Distributor) (file: ESR_TechDoc_Requirements.xlsx, tab 2_CL_Organization, question 2.3 <https://cloud.unicis.tech/f/229087>)
- contact data (postal address, e-mail, phone) - 3 text fields
- additional information/notes - one large text field (optional)

Registered/logged in user may add a new organization to the system.

The user can enter information about the organization within which they want to conduct a product assessment.

According to CRA, a manufacturer, importer, distributor can be "a natural or legal person" (Article 3 - definitions (9), (16), (17)).

Therefore, the user should be able to choose:

- - add an organization within which they will conduct the assessment (legal person) or
- - select the "natural person" option.

If they select the "natural person" option, some of the fields concerning the description of the organization should be disabled.

Instead of information about the organization such as its name, national business registration number, etc., the user will be able to enter their own personal data.

Ref. document: ESR_TechDoc_Requirements.xlsx - questions 2.1, 2.2 of the 2_CL_Organization questionnaires.

2.24.3. Use case - Delete organisation

The user selects an organization. If the selected organization has no other users, OSC RAT displays options allowing the organization to be deleted. The user selects the "Delete organization" command. The system removes the organization from the user's list of organizations in such a way that it becomes unavailable to the user, but all data remains untouched.

2.24.4. Use case - Generate task "Fill organisation questionnaire"

The system generates task to the user to "Fill organisation questionnaire".

2.25. Use case - Review user profile

The user selects the "Review user profile" command. The system displays a window with information about the user profile. The user reviews information about their profile. The system provides the ability to edit profile details.

User profile parameters:

- - name and surname
- - name
- - email address
- - phone number (optional)
- - assigned role in the OSC RAT platform (displayed only, for the administrator role - can be changed)
- - strong authorization (to be turned on and off)
- - strong authorization methods

The system provides items that allow:

- - changing the user's password
- - saving changes made.

2.25.1. Review user profile details

Logged-in users can manage their own accounts. This means they can change their password (UC: change password), edit and save basic user information (UC: save user profile details).



Figure 14 Review user profile details

2.25.2. Use case - Change password

The user selects the item that allows the password to be changed. The system displays a form that allows the password to be changed. The system allows the password to be saved only if it meets the minimum requirements for its strength.

2.25.3. Use case - Save user profile details

The user selects "Save". The system saves the changes.

2.26. Use case - Review user tasks

The user selects the "Review user tasks" command. The system displays a window with a list of tasks assigned to the user. The user reviews the list of tasks. The system provides the ability to mark an item on the list. For the marked item, the system provides an option to edit the task details.

2.26.1. Review user tasks details

For each user, the OSC RAT tool can generate tasks that can help meet CRA requirements. Tasks take the form of recommendations to be carried out either in the OSC RAT tool or in another tool used by the user in their daily work. All of the user's current tasks can be viewed directly from the main application window. In the next steps, it is possible to: edit and save the selected task (UCs: edit selected task, save task details), complete its processing (UC: set task as done), attach an additional file to the task (UC: attach file), and view the task-related rationale.

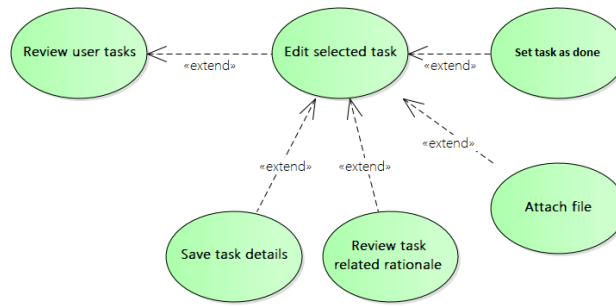


Figure 15 Review user tasks details

2.26.2. Use case - Attach file

The user can attach file (one or more) to task as evidence of activity or result of activity.

The user selects the "Attach file" option. The system displays a window with the ability to browse the file system. The user browses the file system and indicates the file to be added.

The user confirms the entered information. The system adds the file to the system and associates it with the task.

For each task the user has an option to attach one or more files.

During file attachment there are following options to add:

- document identifier or label
- document version
- short description
- document type (e.g. procedure, policy, report)

2.26.3. Use case - Edit selected task

The user selects the "Edit" option for the selected (indicated task on the list). The system displays a window with information about the task. The user browses the information about the task. The system allows editing the task data.

Task data:

- - status (pending, in progress, done)

The system provides options that allow:

- - saving changes to the task
- - adding a file to the task
- - viewing the rationale for the task

2.26.4. Use case - Review task related rationale

The user selects the option "Review task related hints". The system displays a window with hints or goals of the task (based on task type and related documents like CRA and other standards) . The user reviews the information. The user closes the view.

2.26.5. Use case - Save task details

The user selects "Save". The system saves the changes.

2.26.6. Use case - Set task as done

The user selects option to close the task. OSC RAT tool marks the task as closed.

2.27. Use case - Save questionnaire state

Saving questionnaire state is done on the fly after each answer.

For not logged in users (during pre-questionnaire) system stores user session to allow them to get back later.

2.28. Use case - Select organisation

The system displays a list of organizations to which the user has access. The user indicates the appropriate one and confirms the selection. The system creates the basic platform context for the user - the selected organization.

2.29. Use case - Show OSC RAT suggestion based on applicability check result

The suggestion of using OSC RAT tool - if a product is CRA applicable (information that the user can register or log in to complete the assessment and e.g. a link, redirection to the login/registration page).

Once an unregistered user completes a positive applicability check, they can proceed to register and log in to the platform.

In case of negative applicability check - system shows appropriate message with no following action needed "No OSC RAT tool needed".



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 6



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 7

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 7
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

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 an original stakeholders' questionnaire developed as part of the work package. The question groups concern, respectively Stakeholder's characteristic, Inventory/labelling, Risk management, Vulnerability management, Incident management, Security management, documentation, workflow and Users' needs and expectations
Keywords
Users' experience, Users' expectations, Inventory/labelling, Risk management, Vulnerability management, Incident management, Security management, Documentation, Workflow

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.

Table of contents

1. Stakeholders' questionnaire.....	5

Figures

Nie można odnaleźć pozycji dla spisu ilustracji.

List of Tables

Table 1. Original questionnaire questions: number, code, and content.....	5

1. Stakeholders' questionnaire

An original stakeholder questionnaire developed as part of the work package is presented in Table 1. The questions addressed to stakeholders (representatives of micro, small, and medium-sized enterprises) include the original question code (shown at the beginning of each question) and have been organized into the following thematic categories (indicated in bold): Stakeholder Characteristics, Inventory/Labeling, Risk Management, Vulnerability Management, Incident Management, Security Management, Documentation, Workflow, and Users' Needs and Expectations. Table 1 provides a detailed overview of these groupings

Table 1. Original questionnaire questions: number, code, and content

Category name		
Question number	Question Code	Question content
Stakeholder's characteristic		
1	G01 Q01	Which stakeholders' group do you belong to and what type of products do you offer? ☐ Hardware product ☐ Software product ☐ Manufacturer ☐ Importer ☐ Distributor ☐ Open-source software steward - providing support, not a manufacturer - Article 3 (14) of CRA ☐ Other
Inventory/ labelling		
2	G02 Q01	How are you currently handling the labelling (tagging), identifying products, components, and libraries processes in your organization? ☐ We are using a tool / automated process for this (input tools name or details in comments) ☐ We are doing it on an informal basis, with no records kept ☐ We are doing it using manual processes and written / informal records ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC or other relevant standards, SBOM files, etc., please input details in comment) ☐ We are not doing it
3	G02 Q02	If you use solutions that support SBOM, what types of standards do you use or would like to use? ☐ None (we have no solutions to support SBOM) ☐ SPDX® (Software Package Data Exchange) – Linux Foundation format, ISO/IEC 5962 standard ☐ CycloneDX – OWASP Foundation ECMA-424 standard ☐ SWID (Software Identification Tagging) – ISO/IEC 19770-2 ☐ Other
4	G02 Q03	Do You use any SBOM preparing / analysis of SBOM supporting tool? ☐ OWASP dependency-check ☐ cve-bin-tool ☐ gype ☐ trivy ☐ None/No ☐ Other
Risk management		

5	G03 Q01	How are you currently handling the Risk Management processes in your organization? ☐ We are not doing it ☐ We are doing it on an informal basis, with no records kept ☐ We are doing it using manual processes and written / informal records ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27005, 31000, etc., please list standards in comments) ☐ We are using a tool / automated process for this (please input tool name or description in comments)
6	G03 Q02	Do You use any governance, risk management, and compliance (GRC) supporting tools?
Vulnerability management		
7	G04 Q01	How are you currently handling the Vulnerability management processes in your organization? ☐ We are not doing it ☐ We are doing it on an informal basis, with no records kept ☐ We are doing it using manual processes and written / informal records ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 30111, 29147, etc.) ☐ We are using a tool / automated process for this (please input tool name or description in comments)
8	G04 Q02	Is vulnerability classification implemented (how)? ☐ Own (internal) classification ☐ Compliant with standard / guideline / regulation (e.g. CVSS, please list them in comments) ☐ No
9	G04 Q03	Notification Channels of detected / registered / fixed vulnerabilities? ☐ None ☐ E-mail ☐ Dashboard / Internal System ☐ Public Advisory / Website ☐ Automated Alerts (e.g., SIEM, Monitoring tools) ☐ Other
10	G04 Q04	Information Format of detected / registered / fixed vulnerabilities? ☐ Internal (Proprietary Format) ☐ Standard-Compliant (e.g., CVE, ISO, NIST, EUVD) if so, which provide in comments) ☐ Other (if so, which provide in comments) ☐ None/No
11	G04 Q05	Do You use any vulnerability disclosure / handling supporting tools? ☐ Nmap ☐ Nessus ☐ ZAP ☐ BurpSuite ☐ None/No ☐ Other
Incident management		
12	G05 Q01	How are you currently handling the incident management processes in your organization? ☐ We are using a tool / automated process for this (please provide tool name or description in comments) ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27035, etc., please list standards or practices in comments) ☐ We are doing it using manual processes and written / informal records ☐ We are doing it on an informal basis, with no records kept ☐ We are not doing it

13	G05 Q02	Is incident classification implemented (how)? ☐ Own (internal) classification ☐ Compliant with standard / guideline / regulation (e.g. NIS 2 directive) if so, which provide in comment ☐ No ☐ Other if so, please provide details in comment
14	G05 Q03	Who is notified of detected incidents carried out? ☐ Internal Security Team ☐ Affected Customers ☐ Regulatory Authorities ☐ Public Disclosure ☐ Other
15	G05 Q04	Notification Channels of detected incidents carried out? ☐ None ☐ E-mail ☐ Dashboard / Internal System ☐ Public Advisory / Website ☐ Automated Alerts (e.g., SIEM, Monitoring tools) ☐ Other
16	G05 Q05	Do You use any incident detection / analysis, reporting supporting tools? ☐ No ☐ Wazuh ☐ Snort ☐ Suricata ☐ Other
Security management, documentation, workflow		
17	G06 Q01	Have you implemented any documentation management or security management processes in your organization? ☐ We are using a tool / automated process for this (please provide names or details in comment) ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27001 or other relevant standards, etc., please provide names or details in comment) ☐ We are doing it using manual processes and written / informal records ☐ No ☐ We are doing it on an informal basis, with no records kept
18	G06 Q02	Do you use any tools for documents / source code / data repository tools (internal for developers, managers and public for customers)? ☐ GIT ☐ SVN ☐ One Drive ☐ Google Drive ☐ Windows shared folders/Samba ☐ None/No ☐ Other
19	G06 Q03	Do you use any building systems / compilations tools? ☐ GitLab CI/CD ☐ Ansible ☐ Jenkins ☐ Maven ☐ None/No ☐ Other
Needs and expectations		
20	G07 Q01	How important to you is: ☐ [CL - Checklist Automation (CRA self-assessment checklist)] ☐ How important to you is: [SBOM - Software Bill of material – preparing/analysis supporting tool] ☐ How important to you is: [VUL – vulnerability management supporting tool] ☐ How important to you is: [INC – incident management supporting tool] ☐ How important to you is: [DOC – documentation tool (central repository)]

21	G07 Q02	Are you interested in participating in the validation of the tool developed within the project?



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 7



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 8

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 8
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

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 revised stakeholder questionnaire developed after the first stage of the survey. New question groups concern, respectively Organization profile, CRA readiness, Inventory/ labelling (SBOM - Software Bill of Materials), Risk management, Vulnerability management, Incident management, Security management, documentation, workflow and Users' needs and expectations, Participation in workshops and training sessions on the OSCRAT platform.
Keywords
Users' needs, Users' expectations, Inventory/labelling, Risk management, Vulnerability management, Incident management, Security management, Documentation, Workflow

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.

Table of contents

1. Revised stakeholder questionnaire	5

List of Tables

Table 1. Revised stakeholder questionnaire v 2.2: number, code, and content	6

1. Revised stakeholder questionnaire

The evaluation of the initial stakeholder survey (see Annex 7) results revealed that some questions needed simplification, others required expansion or additional details, and the order of certain items had to be adjusted to ensure more accurate data collection. The developed recommendations for the new stakeholder survey are presented below. It is structured as follows: the group name (in bold), followed by a series of numbered questions within the group.

Organization profile

1. What is the type of enterprise within the meaning of European Union regulations
 - a) Microenterprise
 - b) Small Enterprise
 - c) Medium Enterprise
 - d) I do not know
 - a. Other (Text input)

Hint:

The main factors determining whether an enterprise is an SME are

- **number of employees**
- either **turnover** or **balance sheet total**

Type of Enterprise	Number of Employees	Annual Turnover (EUR)	Balance Sheet Total (EUR)
Microenterprise	< 10	< 2 million	< 2 million
Small Enterprise	< 50	< 10 million	< 10 million
Medium Enterprise	< 250	< 50 million	< 43 million

https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en

2. What type of products with digital elements do you offer?
 - a. Hardware product
 - b. Software product
 - c. Other (Text input)
3. Which stakeholders' group do you belong?
 - a. Manufacturer
 - b. Importer
 - c. Distributor
 - d. Open-source software steward - providing support, not a manufacturer
 - e. Other (Text input)
4. What is your position in the company?
 - a. Owner
 - b. IT Director
 - c. IT Specialist
 - d. Compliance Specialist
 - e. Prefer not to say
 - f. Other (Text input)

CRA readiness

1. Are you familiar with the CRA requirements?
 - a. Yes
 - b. No
 - c. Partially
2. Are your products subject to CRA conformity assessment?
 - a. Yes
 - b. No
 - c. I'm not sure

User needs and expectations

1. What kind of convenience or feature would you expect from a tool that supports inventory or SBOM management? (Text input)
2. What do you expect from a tool designed to support vulnerability handling? (Text input)
3. What do you expect from a tool designed to support incident handling? (Text input)
4. What would you like a tool for risk management to help you with? (Text input)
5. What are your requirements for a security management support tool? (Text input)
6. What do you expect from a tool supporting documentation and workflow? (Text input)

Participation in workshops and training sessions on the OSCRAT platform

1. Are you interested in participating in training sessions or workshops conducted on the OSCRAT platform (selected case studies)?
 - a. Yes
 - b. No
 - c. I'm not sure

As a result, an updated version of the survey was prepared (v 2.2). The revised stakeholder questionnaire has been organised into the following thematic categories:

- Organization profile,
- CRA readiness, Inventory/ labelling <SBOM - Software Bill of Materials>,
- Risk management,
- Vulnerability management, Incident management,
- Security management, documentation, workflow
- Users' needs and expectations,
- Participation in workshops and training sessions on the OSCRAT platform.

The complete revised and supplemented stakeholder survey v 2.2 is presented in Table 1. The initial version of the questionnaire is available in Annex 7.

Table 1. Revised stakeholder questionnaire v 2.2: number, code, and content

Question number	Question Code	Question content
Organization profile		
1	G01 Q01	What is the type of enterprise within the meaning of European Union regulations Hardware product ☐ Microenterprise ☐ Small Enterprise

		☐ Medium Enterprise ☐ I do not know ☐ Other (please describe in comments) Hint: The main factors determining whether an enterprise is an SME are • number of employees • either turnover or balance sheet total <table border="1"> <thead> <tr> <th>Type of Enterprise</th><th>Number of Employees</th><th>Annual Turnover (EUR)</th><th>Balance Sheet Total (EUR)</th></tr> </thead> <tbody> <tr> <td>Micro Enterprise</td><td>< 10</td><td>< 2 million</td><td>< 2 million</td></tr> <tr> <td>Small Enterprise</td><td>< 50</td><td>< 10 million</td><td>< 10 million</td></tr> <tr> <td>Medium Enterprise</td><td>< 250</td><td>< 50 million</td><td>< 43 million</td></tr> </tbody> </table> https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en	Type of Enterprise	Number of Employees	Annual Turnover (EUR)	Balance Sheet Total (EUR)	Micro Enterprise	< 10	< 2 million	< 2 million	Small Enterprise	< 50	< 10 million	< 10 million	Medium Enterprise	< 250	< 50 million	< 43 million
Type of Enterprise	Number of Employees	Annual Turnover (EUR)	Balance Sheet Total (EUR)															
Micro Enterprise	< 10	< 2 million	< 2 million															
Small Enterprise	< 50	< 10 million	< 10 million															
Medium Enterprise	< 250	< 50 million	< 43 million															
	G01 Q02	What type of products with digital elements do you offer? ☐ Hardware product ☐ Software product ☐ Other (please describe in comments)																
	G01 Q03	Which stakeholders' group do you belong? ☐ Manufacturer ☐ Importer ☐ Distributor ☐ Open-source software steward - providing support, not a manufacturer ☐ Other (please describe in comments)																
	G01 Q04	What is your position in the company? ☐ Owner ☐ IT Director ☐ IT Specialist ☐ Compliance Specialist ☐ Prefer not to say ☐ Other (please describe in comments)																
CRA readiness																		
	G02 Q01	Are you familiar with the CRA requirements? ☐ Yes ☐ No ☐ Partially																
	G02 Q02	Are your products subject to CRA conformity assessment? ☐ Yes ☐ No ☐ I'm not sure																
Respondents' experience																		
Inventory/ labelling (SBOM - Software Bill of Materials)																		
2	G03 Q01	How are you currently handling the labelling (tagging), identifying products, components, and libraries processes in your organization? ☐ We are using a tool / automated process for this (input tools name or details in comments) ☐ We are doing it on an informal basis, with no records kept																

		☐ We are doing it using manual processes and written / informal records ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC or other relevant standards, SBOM files, etc., please input details in comment) ☐ We are not doing it ☐ Other (please describe in comments)
3	G03 Q02	Do You use any SBOM preparing / analysis of SBOM supporting tool? ☐ OWASP dependency-check ☐ cve-bin-tool ☐ gype ☐ trivy ☐ None/No ☐ Other (please describe in comments)
4	G03 Q03	Do You use any SBOM preparing / analysis of SBOM supporting tool? ☐ OWASP dependency-check ☐ cve-bin-tool ☐ gype ☐ trivy ☐ None/No ☐ Other (please describe in comments)
		If you use solutions that support SBOM, what types of standards do you use or would like to use? ☐ None (we have no solutions to support SBOM) ☐ SPDX® (Software Package Data Exchange) – Linux Foundation format, ISO/IEC 5962 standard ☐ CycloneDX – OWASP Foundation ECMA-424 standard ☐ SWID (Software Identification Tagging) – ISO/IEC 19770-2 ☐ Other (please describe in comments)
Risk management		
5	G04 Q01	How are you currently handling the Risk Management processes in your organization? ☐ We are not doing it ☐ We are doing it on an informal basis, with no records kept ☐ We are doing it using manual processes and written / informal records ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27005, 31000, etc., please list standards in comments) ☐ We are using a tool / automated process for this (please input tool name or description in comments) ☐ Other (please describe in comments)
6	G04 Q02	Do You use any governance, risk management, and compliance (GRC) supporting tools? ☐ Yes (list in comments) ☐ No
Vulnerability management		
7	G05 Q01	How are you currently handling the Vulnerability management processes in your organization? ☐ We are not doing it ☐ We are doing it on an informal basis, with no records kept ☐ We are doing it using manual processes and written / informal records ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 30111, 29147, etc.) ☐ We are using a tool / automated process for this (please input tool name or description in comments) ☐ Other (please describe in comments)
8	G05 Q02	Is vulnerability classification implemented (how)? ☐ Own (internal) classification ☐ Compliant with standard / guideline / regulation (e.g. CVSS, please list them in comments)

		☐ No ☐ Other (please describe in comments)
9	G05 Q03	What types of notification channels does your organization provide for reporting and communicating detected, registered, and resolved vulnerabilities? ☐ None ☐ E-mail ☐ Dashboard / Internal System ☐ Public Advisory / Website ☐ Automated Alerts (e.g., SIEM, Monitoring tools) ☐ Other (please describe in comments)
10	G05 Q04	What is the information format for detected, registered, and fixed vulnerabilities used in your organization? ☐ Internal (Proprietary Format) ☐ Standard-Compliant (e.g., CVE, ISO, NIST, EUVD) if so, which provide in comments) ☐ Other (if so, which provide in comments) ☐ None/No
11	G05 Q05	Do You use any vulnerability disclosure / handling supporting tools? ☐ Nmap ☐ Nessus ☐ ZAP ☐ BurpSuite ☐ None/No ☐ Other (please describe in comments)
Incident management		
12	G06 Q01	How are you currently handling the incident management processes in your organization? ☐ We are using a tool / automated process for this (please provide tool name or description in comments) ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27035, etc., please list standards or practices in comments) ☐ We are doing it using manual processes and written / informal records ☐ We are doing it on an informal basis, with no records kept ☐ We are not doing it ☐ Other (please describe in comments)
13	G06 Q02	Is incident classification implemented (how)? ☐ Own (internal) classification ☐ Compliant with standard / guideline / regulation (e.g. NIS 2 directive) if so, which provide in comment ☐ No ☐ Other if so, please provide details in comment
14	G06 Q03	Who is notified of detected incidents? ☐ None ☐ Internal Security Team ☐ Affected Customers ☐ Regulatory Authorities ☐ Public Disclosure ☐ Other (please describe in comments)
15	G06 Q04	What notification channels are used to report and communicate detected and handled incidents? ☐ None ☐ E-mail ☐ Dashboard / Internal System ☐ Public Advisory / Website ☐ Automated Alerts (e.g., SIEM, Monitoring tools) ☐ Other (please describe in comments)
16	G06 Q05	Do You use any incident detection / analysis, reporting supporting tools? ☐ No ☐ Wazuh

		☐ Snort ☐ Suricata ☐ Other (please describe in comments)
Security management, documentation, workflow		
17	G07 Q01	Have you implemented any documentation management or security management processes in your organization? ☐ We are using a tool / automated process for this (please provide names or details in comment) ☐ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27001 or other relevant standards, etc., please provide names or details in comment) ☐ We are doing it using manual processes and written / informal records ☐ No ☐ We are doing it on an informal basis, with no records kept ☐ Other (please describe in comments)
18	G07 Q02	Do you use any tools for documents / source code / data repository tools (internal for developers, managers and public for customers)? ☐ GIT ☐ SVN ☐ One Drive ☐ Google Drive ☐ Windows shared folders/Samba ☐ Sharepoint ☐ iCloud ☐ Confluence ☐ ISO/ISMS ☐ Jira ☐ None/No ☐ Other (please describe in comments)
19	G07 Q03	Do you use any building systems / compilations tools? ☐ GitLab CI/CD ☐ Ansible ☐ Jenkins ☐ Maven ☐ GitHub ☐ None/No ☐ Other (please describe in comments)
User needs and expectations		
	G08 Q01	What kind of convenience or feature would you expect from a tool that supports inventory or SBOM management?
	G08 Q02	What do you expect from a tool designed to support vulnerability handling?
	G08 Q03	What do you expect from a tool designed to support incident handling?
	G08 Q04	What would you like a tool for risk management to help you with?
	G08 Q05	What are your requirements for a security management support tool?
	G08 Q05	What do you expect from a tool supporting documentation and workflow?
Participation in workshops and training sessions on the OSCRAT platform		
20	G09 Q01	Are you interested in participating in training sessions or workshops conducted on the OSCRAT platform (selected case studies)? ☐ Yes (Contact e-mail) ☐ No



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 8



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 9

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 9
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

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 describes OSC RAT Documentation tool requirements according to CRA Annex VII Technical Documentation.
Keywords
OSCRAT tool, Documentation module, module purpose, module capabilities, Technical Documentation

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.

Table of contents

1. Technical Specification: OSCRA – CRA Annex VII Technical Documentation	5
Purpose	5
1.1 Scope	5
1.2 Objectives	6
System Overview	6
1.3 Functional Requirements – CRA Annex VII Sections	6
1.3.1. General Description	6
1.3.2. Design & Development	7
1.3.3. Vulnerability Handling Processes	7
1.3.4. Production & Monitoring Processes	7
1.3.5. Cybersecurity Risk Assessment	7
1.3.6. Support Period Determination	8
1.3.7. Standards & Specifications	8
1.3.8. Conformity Verification	8
1.4 Workflow and Version Lifecycle	8
1.5 Publication and Access	8
1.6 Non-Functional Requirements	9
1.7 Deliverables	9
1.8 Results / Outcome	9

1. Technical Specification: OSCRA – CRA Annex VII

Technical Documentation

Purpose

This specification defines how OSCRA captures, structures, and publishes the EU Cyber Resilience Act (CRA) Annex VII Technical Documentation for Product with Digital Elements (PDE).

It outlines how each required section is managed, including editable text fields, pre-built templates, and data integration from existing OSCRA modules such as assessment, SBOM, vulnerability, and incident management.

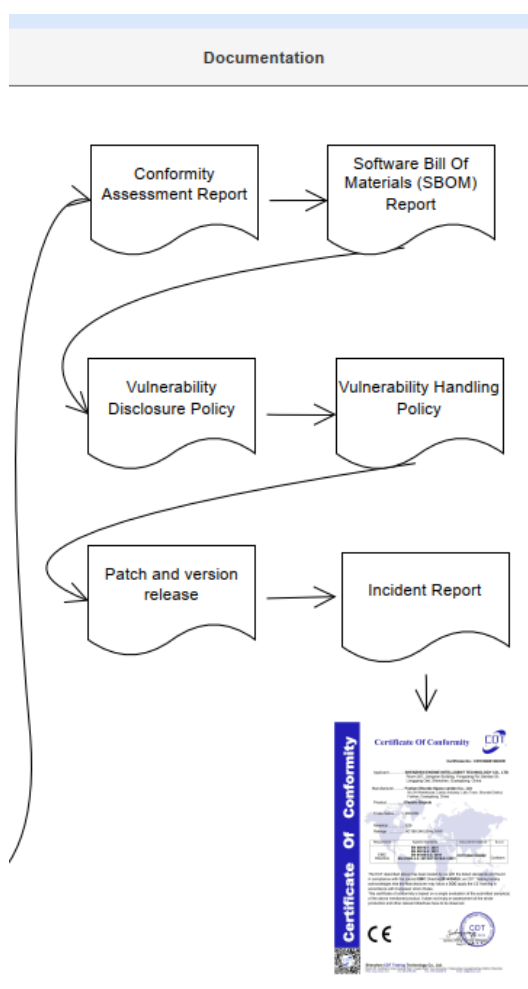


Figure 1 Documentation pillar - basic capabilities based on Grant Agreement

1.1 Scope

This specification covers the CRA Annex VII¹ Technical Documentation module within OSCRAT, focusing on:

- Editable and guided text sections for all eight CRA requirements.
- Integration of structured evidence from assessment and compliance modules.
- Validation, version management, publication, and export of final documentation packages.

1.2 Objectives

- Enable users to create and maintain CRA-compliant technical documentation.
- Provide rich-text editable sections using the OSCRAT Quill² package.
- Supply pre-built, editable templates for key regulatory sections.
- Support the collection of compliance evidence from OSCRAT modules.
- Ensure all eight Annex VII sections are complete and validated before publication.
- Generate versioned, exportable documentation for audit and regulatory submission.

System Overview

The Technical Documentation module aggregates information from across OSCRAT, including:

- Assessment and Conformity modules (checklists, declarations, reports).
- SBOM and Security Scanning module (component inventory and scan results).
- Vulnerability Handling module (disclosure policy, lifecycle data, contacts).
- Incident Management module (risk and post-incident evidence).

Output:

- Complete Annex VII documentation per PDE version.
- Published document under the tenant's namespace:

[https://\[domain\]/teams/<tenant>/public/techdocs/<product>/<version>](https://[domain]/teams/<tenant>/public/techdocs/<product>/<version>)

1.3 Functional Requirements – CRA Annex VII Sections

1.3.1. General Description

Purpose: Describe the product, its software, and its intended use.

Content: Intended purpose, software versions, visuals, user information.

Implementation:

¹ EUR-LEX: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847#anx_VII

² Quill. Website: <https://quilljs.com>. GitHub repository: <https://github.com/slab/quill>

- Open text section using OSCRAT's existing Quill editor package with Markdown syntax support.
- Users can freely edit and format text, add images, and upload related documents.
- Data saved per product version and automatically included in the published report.

1.3.2. Design & Development

Purpose: Explain the architecture and secure design approach.

Content: Architecture diagrams, component relationships, development methodology.

Implementation:

- Open text section using Quill editor.
- Users can embed diagrams, lists, and tables.
- Files and visuals can be attached or linked.
- Allows users to describe how design principles ensure CRA compliance.

1.3.3. Vulnerability Handling Processes

Purpose: Detail how vulnerabilities are reported, disclosed, and addressed.

Content: SBOM, coordinated vulnerability disclosure (CVD) policy, contact details, update process.

Implementation:

- Self-assessment includes sections for SBOM reference, reporting contact, disclosure process, and secure update mechanisms.
- Vulnerability handling process and documentation supported by OSCRAT's vulnerability handling module and SBOM data.
- Public-facing disclosure policy - possible to be published with product documentation.

1.3.4. Production & Monitoring Processes

Purpose: Define quality assurance and monitoring during production.

Content: Quality controls, validation steps, production process, and post-production monitoring.

Implementation:

- Template-based structure with editable sections.
- Pre-filled outline covering production validation, QA methods, monitoring routines, and feedback loops.
- Users modify text via Quill editor.
- Linked to evidence uploaded by third-party assessors or manufacturing partners.

1.3.5. Cybersecurity Risk Assessment

Purpose: Summarize cybersecurity risk assessment and mitigations.

Content: Risk analysis, threat model, mapping to Annex I requirements.

Implementation:

- Template provided based on OSCRAT's risk assessment framework.
- Editable in Quill; users can modify predefined sections and reference risk assessment reports.
- Provided data for user use as part of a product risk assessment (based on the risk analysis template) – this data includes related vulnerabilities and incidents.
- Maintains consistent mapping to CRA Annex I essential requirements.

1.3.6. Support Period Determination

Purpose: State and justify the update and support timeline.

Content: Support duration, rationale, and end-of-support policy.

Implementation:

- Editable text fields connected to lifecycle data in the assessment module.
- Display expected support period; rationale editable by user.

1.3.7. Standards & Specifications

Purpose: Identify applicable standards and alternative solutions.

Content: Harmonised standards, certifications, and alternative measures.

Implementation:

- Evidence attachments for certifications and tests.
- Used to demonstrate conformity with Annex I and II requirements.

1.3.8. Conformity Verification

Purpose: Provide conformity proof and declarations.

Content: Test results, declarations of conformity, SBOM availability confirmation.

Implementation:

- For self-assessments - conformity declarations generation support.
- For third-party assessments - assessors upload the signed Declaration of Conformity.
- Linked to assessment results, SBOM data, and testing reports.

1.4 Workflow and Version Lifecycle

- **Draft** – User creates or edits sections and uploads supporting evidence internally (document not publicly available).
- **Published** – Documentation becomes public on tenant portal.
- **Archived** – Retained for audit; superseded by newer version.

1.5 Publication and Access

- **Internal View:** Full editing and review features for authorized users.

- **Public View:** Read-only presentation under tenant namespace.
- **Access Control:** Private drafts restricted; published docs public.

1.6 Non-Functional Requirements

- **Compliance:** Full alignment with CRA Annex VII and Article 31.
- **Usability:** Rich-text editing via Quill, guided templates, progress indicators.
- **Security:** Role-based access, tenant isolation, encryption, GDPR compliance.
- **Auditability:** Version tracking, edit history, approval timestamps.
- **Performance:** Real-time autosave, public page load under 2 seconds.
- **Scalability:** Multi-tenant, multi-version support.
- **Localization:** Multi-language support for EU users.

1.7 Deliverables

- Fully operational CRA Annex VII Technical Documentation module within OSCRAT.
- Open-text editing for General Description and Design & Development.
- Editable templates for Vulnerability and Incident Handling, Production & Monitoring, and Risk Assessment.
- Integration with assessment, SBOM, vulnerability, and incident modules.
- Validation for completeness across all eight Annex VII sections.
- Publication portal and export functionality for CRA submissions.

1.8 Results / Outcome

The enhanced OSCRAT Technical Documentation module provides an integrated, editable, and compliant system for CRA Annex VII documentation. It combines user-driven descriptive content with pre-built regulatory templates and automated evidence integration, resulting in accurate, transparent, and regulator-ready documentation for every product version.



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 9



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 10

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 10
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

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 template for incident report.
Keywords
Incident report template

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.

Template for incident report

General information

Company Hint: Address details of the company reporting the incident.	
Company name	
State	
Town	
Address	

Reporter Hint: Details of the person reporting the incident.	
Name	
Position/Function	
e-mail	
Phone	

Incident Commander Hint: Details of the incident commander.	
Name	
Position/Function	
e-mail	
Phone	

Incident details

Hint: Detailed information about incident.

Incident description	
Classification	☐ critical ☐ high ☐ medium ☐ low ☐ N/A - False Positive
Timeline & Key Dates • Occurrence Time: [Date Picker] (Est. start of the event) • Detection Time: [Date Picker] (When you found out)	Date/Time of Occurrence: The estimated timestamp when the incident actually started (based on logs or evidence). Date/Time of Detection: The exact timestamp when the organization became aware of the incident. Note: This starts the regulatory clock for mandatory notifications (e.g., 24-hour Early Warning). Date/Time of Reporting: When the incident was officially logged in the system. Date/Time of Closure: When the incident was resolved and the ticket closed. Total Downtime: (Optional/Auto-calculated) Duration of service unavailability.
Affected Components/Assets	
Detection Method: How was the incident discovered? Options: Automated Alert (SIEM/IDS), Internal User Report, External Notification (Customer/Researcher), Audit/Review.	

Regulatory Reporting Required? (Yes/No) – Does this incident meet the threshold for notification to authorities (CSIRT/ENSIA)?	
Incident Status	☐ New: The incident has been logged but is not yet assigned or analyzed. ☐ Under Investigation: The team is actively analyzing the root cause, scope, and severity of the event. ☐ In Progress: Containment measures are being executed to stop the threat from spreading. ☐ In Remediation: Long-term fixes (patches, configuration changes) are being applied to resolve the root cause. ☐ Monitoring: The system is under observation to ensure stability and prevent recurrence after the fix. ☐ Resolved: Technical issues are fixed and services are restored, pending final documentation. ☐ Closed: All post-incident activities, including reporting and lessons learned, are completed. ☐ False Positive: Investigation confirmed the event was not a security incident; no further action required. ☐ On Hold: Resolution is temporarily paused awaiting external input (e.g., vendor patch, legal advice).

Incident type

Hint: Select all applicable types of incident.

☐	Incident type
☐	General
☐	Confidentiality
☐	Integrity
☐	Availability
☐	Access control
☐	Vulnerabilities
☐	Technical failure
☐	Theft or loss equipment

Attack type

Hint: Select all applicable types of attacks.

☐	Attack type
☐	Denial of service
☐	Unauthorized access
☐	Malware
☐	Abuse
☐	Others

Impact Assessment

1. Affected Jurisdictions

- **Field Type:** Multi-select Dropdown
- **Options:** List of EU Member States, Non-EU/Global.
- **Tooltip:** Select the specific countries or regions where service disruption, data breach, or operational failure is currently occurring.

2. Estimated User Impact

- **Field Type:** Single Select (Range)
- **Options:**
 - < 100 (Minor / Localized)
 - 100 – 1,000 (Substantial)
 - 1,001 – 100,000 (Significant)
 - 100,001 – 1,000,000 (Major)
 - 1,000,000 (Critical / Mass Event)
- **Tooltip:** Estimate the number of end-users experiencing service unavailability, performance degradation, or data compromise.

3. Affected Device Volume

- **Field Type:** Numeric / Percentage
- **Tooltip:** Indicate the total number of devices (or percentage of the fleet) that are offline, infected, or malfunctioning due to the incident.

Treatment details (part 1)

Corrective action

Hint: Describe the actions that will mitigate and minimize their impact on the future incident.

No	Description
1	
2	
3	
4	
5	

Root cause

Hint: Describe the root cause of the incident.

No	Description
1	
2	
3	
4	
5	

Treatment details (part 2)

Scope	
Hint: What is the scope for the future treatment of such incident recurrence.	
No	Description
1	
2	
3	
4	
5	

Preventive action	
Hint: List the actions that the organization is taking to prevent such incident in near future.	
No	Description
1	
2	
3	
4	
5	



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 10



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 11

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 11
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

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 template for vulnerability report.
Keywords
Vulnerability report template

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.

Template for Vulnerability report

General information

Company Hint: Address details of the company reporting the vulnerability.	
Company name	
State	
Town	
Address	

Reporter Hint: Details of the person reporting the vulnerability.	
Name	
Position/Function	
e-mail	
Phone	

General Vulnerability Information

- **Vulnerability Title:** A short, descriptive name (e.g., "Buffer Overflow in Login Module").
- **Vulnerability Source:** Where did the report come from?
 - *Options:* Internal Audit, Pentest, External Researcher (CVD), Automated Scan, Public CVE.
- **External Reference (CVE/Advisory ID):** If the vulnerability already has a public identifier (e.g., CVE-2024-12345), it must be logged here.

Assessment & Severity (Risk Level)

- **CVSS Score (Base Score):** The numerical score (0.0 - 10.0) based on the Common Vulnerability Scoring System.
- **CVSS Vector String:** The textual representation of the metric (e.g., CVSS:3.1/AV:N/AC:L...).

Impact & Scope Assessment

1. Affected Jurisdictions

- **Field Type:** Multi-select Dropdown
- **Options:** List of EU Member States, Non-EU/Global.
- **Tooltip:** Select the specific countries or regions where the affected devices are deployed or where users are impacted.

2. Estimated User Impact

- **Field Type:** Single Select (Range)
- **Options:**
 - < 100 (Limited / Testing)
 - 100 – 1,000 (Local Scale)
 - 1,001 – 100,000 (Significant)
 - 100,001 – 1,000,000 (Major)
 - > 1,000,000 (Critical / Mass Scale)
- **Tooltip:** Provide a rough estimate of the number of end-users or customers potentially exposed to this vulnerability.

3. Affected Device Volume

- **Field Type:** Numeric / Percentage
- **Tooltip:** Indicate the total number of units (or the percentage of the active fleet) currently running the vulnerable version.

Stage

- ☐ Early Warning (24h)
☐ Vulnerability Notification (72h)
☐ Final Report (14d)

Vulnerability Scope – Early Warning (24h)

EU member states that are affected (where the product has been made available)	
Date (when observed)	

Vulnerability General Information - Vulnerability Notification (72h)

Vulnerability description – general information about the vulnerability and general nature of its exploitation	

Products affected – general information about affected software/hardware	

Corrective/Mitigating measures taken Vulnerability Notification (72h)

Corrective/Mitigating measures	
Hint: Describe the actions that were taken to mitigate and minimize the impact of the vulnerability	
No	Description
1	
2	
3	
4	
5	

Corrective/Mitigating measures users can take Vulnerability Notification (72h)

Corrective/Mitigating measures	
Hint: Describe the actions that users can take to mitigate and minimize the impact of the vulnerability	
No	Description
1	
2	
3	
4	

5	

Vulnerability details Final Report (14d)

Hint: Detailed information about vulnerability.

Vulnerability description – short description	
Vulnerability details – additional context helping to reproduce the problem and description of its consequences (severity) and impact	
URL address/software name version and affected components/device model and identifier	
Malicious actors that exploited/are exploiting the vulnerability	

Vulnerability Remediation Final Report (14d)

Security updates/Corrective measures

Hint: Describe security update or other corrective measures that have been made available to remedy the vulnerability

No	Description
1	
2	
3	
4	

5	

Vulnerability Status

- ☐ New / Triage: Just reported, waiting for validation.
- ☐ Confirmed: Validated as a real vulnerability; awaiting scheduling.
- ☐ In Remediation: Developers are working on the fix/patch.
- ☐ Fix Available: Patch is ready but not yet deployed/released.
- ☐ Mitigated: A temporary workaround is in place (e.g., WAF rule), but the root cause exists.
- ☐ Closed (Fixed): The patch is deployed and verified.
- ☐ Accepted Risk: The business decided not to fix it (requires justification/sign-off).
- ☐ False Positive: Analysis showed it is not a vulnerability.

Timeline

- Discovery Date: When was the vulnerability first identified?
- Remediation Target Date: When is the fix due?
- Resolution Date: When was the fix verified and closed?



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 11



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.



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. 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

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

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.

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)

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**,

or an applicable EU cybersecurity certification scheme (assurance $\geq$ “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.)

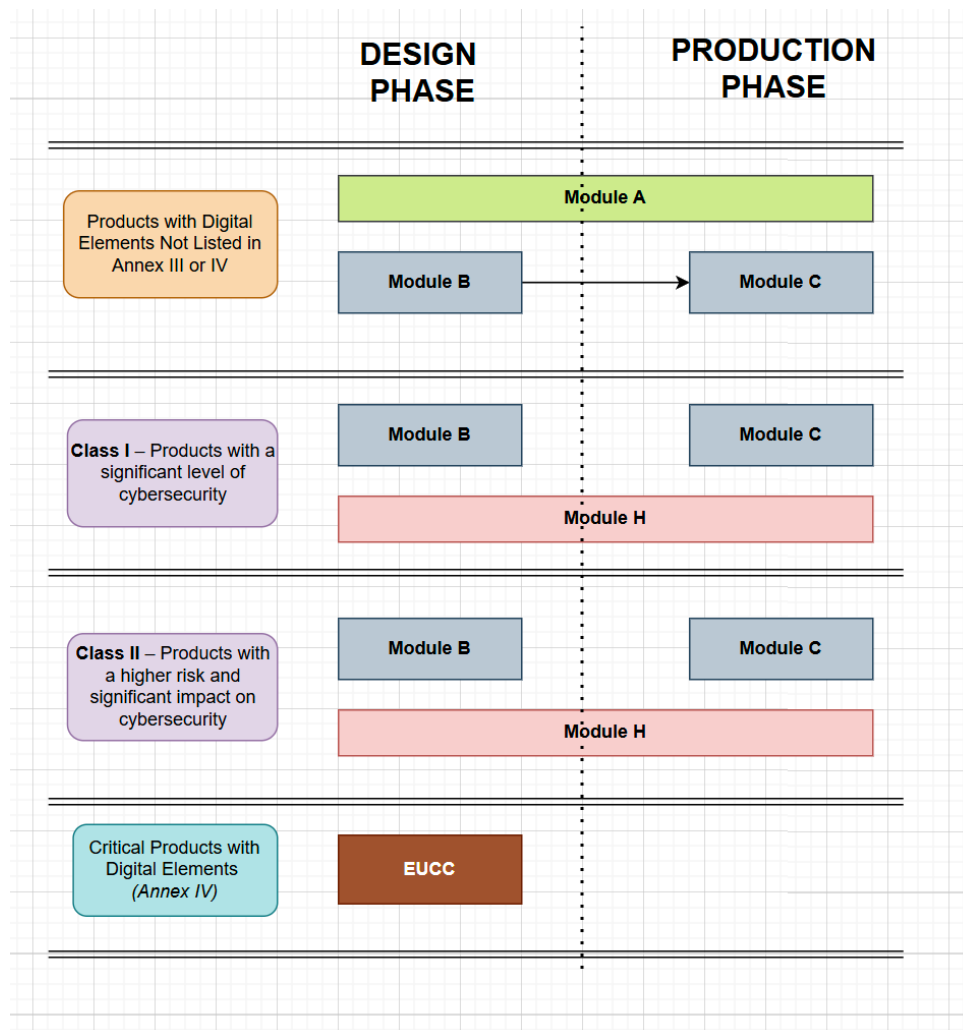
B. Use the Blue Guide’s risk-based rationale to pick the module

- **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 $\geq$ “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.

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.

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.

- 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.

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.

- **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).



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 13

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 13
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

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 Template for Risk Assessment.
Keywords
Risk Assessment Template

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.

Template for Risk Assessment

General information

Company Hint: Address details of the company reporting the vulnerability.	
Company name	
State	
Town	
Address	

Risk Assessor Hint: Details of the person assessing the risk.	
Name	
Position/Function	
e-mail	
Phone	
Date	

Risk Details

Hint: Detailed information about risk assessment.

Asset Hint: The process or (information) asset that the risk applies to.	
Threat Hint: A detailed description of the threat.	
Category Hint: In what category) or categories) does the risk fall? CONFIDENTIALITY = information could fall into wrong hands; INTEGRITY = information could be modified; AVAILABILITY = Information could be available when needed.	
Likelihood Hint: The likelihood of the risk to materialize. How often do you expect the threat to happen?	
Impact Hint: The impact when the risk materializes. What could happen to the organization?	
Exposure Hint: The exposure is calculated as likelihood x impact.	
Owner	

Hint: The person that take ownership of the risk and decided how the risk is going to be treated. This person is usually a manager or business owner.	

Risk Treatment

Hint: Detailed information about risk treatment and mitigation measures.

Treatment Hint: How is the organization going to respond to the risk? ACCEPT = Management accepts the risk REDUCE = Measures will be implemented to reduce the risk AVOID = The activity that the risk is related to will be stopped TRANSFER = The risk will be transferred to another entity, such as an insurance company	
Measures Hint: In case of reduction, write down the measures you are going to take to reduce the likelihood and/or impact of the threat. Try to link them to the relevant Annex A controls.	
Residual Exposure Hint: An estimation of the exposure after the measures have been taken.	
Responsible Hint: The person (or role) responsible for implementing the measures.	

Risk Level

Risk Score / Exposure	Risk levels / Impact			
Likelihood		Low	Medium	High
	High	Medium (M)	High (H)	High (H)
	Medium	Low (L)	Medium (M)	High (H)
	Low	Low (L)	Low (L)	Medium (M)

Risk Likelihood

Likelihood	Description
Low	The event is unlikely; it has rarely happened or conditions make it improbable.
Medium	The event could occur occasionally; not frequent but plausible.
High	The event is expected to occur or has occurred frequently in similar situations.

Risk Impact

Impact	Description
Low	Minor consequences, limited disruption, easily manageable.
Medium	Noticeable effects on objectives, processes, or resources; may require time and cost to resolve.
High	Major consequences, significant financial or operational damage, reputational harm, or safety issues.



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 13



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 14

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 14
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

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 Annex relates to a CRA-specific requirements which were identified and applicable articles to the OSCRAT tools were marked. The table shows the tools' capabilities to be implemented to cover identified CRA-specific requirements.
Keywords
CRA-specific requirements, OSCRAT tool capabilities

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.

Table of contents

1. CRA requirements for the OSCRAT tool capabilities / functionality.....	1

List of Tables

Table 1 CRA-specific requirements – mapping on OSCRAT tool requirements and capabilities.....	19

1. CRA requirements for the OSCRAT tool capabilities / functionality

CRA chapter	CRA ref.	CRA article name	OSCRAT related CRA-specific requirements	OSCRAT tool capabilities to implement	Applicable articles	No. of articles
Chapter I General provisions	Article 1	Subject matter	N/A (<i>The provisions of the act do not generate any particular requirement for OSCRAT</i>)			1
	Article 2	Scope	Need to check whether PDE is subject to CRA requirements	Applicability Check (and Classification)	1	1
	Article 3	Definitions	N/A	List of terms used		1
	Article 4	Free movement	N/A	Refers to the availability of products on the European market		1
	Article 5	Procurement or use of products with digital elements	N/A			1
	Article 6	Requirements for products with digital elements	Support for self-assessment of meeting the cybersecurity requirements for the product (from Annex I, Part I), and for the procedures used by the manufacturer (Annex I, Part II).	- New Product Creation - Product Details Page - Add New Product Version - Product Version Details Page - CRA Compliance Assessment for a Product Version - Organization creation	1	1

	CRA Process Assessment for an Organization					
	Article 7	Important products with digital elements	Support in classifying the product in accordance with the guidelines in Annex III.	Applicability Check (and Classification)	1	1
	Article 8	Critical products with digital elements	Support in classifying the product in accordance with the guidelines in Annex IV.	Applicability Check (and Classification)	1	1
	Article 9	Stakeholder consultation	N/A			1
	Article 10	Enhancing skills in a cyber resilient digital environment	N/A			1
	Article 11	General product safety	N/A			1
	Article 12	High-risk systems	AI Support for self-assessment of meeting the cybersecurity requirements relates also to High-risk AI systems	- CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization	1	1
Chapter II Obligations of manufacturers	Article 13	Obligations of manufactures			1	1
	(1), (5)		Support for self-assessment of whether the product being introduced to the market has been designed, developed and manufactured in accordance with cybersecurity requirements (Annex I, Part I)	- CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization - Documentation (General description, Specification of the design &		

(2), (3), (4)

(6), (7), (9)

Support in conducting risk assessments.

Ability to describe the product and its components. Gather information about vulnerabilities and support vulnerability management, in accordance with the requirements of Annex I, Part II. Ability to provide information about countermeasures or attach files, e.g., with version updates.

development process of the product,
Production

Specification, description of the
design & development process of the
product)

- Product Assessment Dashboard, Visualization, PDF Export
- Organization CRA Compliance Dashboard, Visualization & PDF Export

- Risk assessment report template for the user

- Documentation (General description, Specification of the design & development process of the product, Production

Specification, description of the
design & development process of the
product)

- Vulnerability/Incident details page, vulnerability/incident reports - to consider during the risk assessment

- Vulnerability handling (Add new vulnerability, Edit vulnerability, Vulnerability details page)

- Documentation (General description, Vulnerability handling process, Vulnerability report template)

	(8), (19)	Possibility to assign a support period to a product version. The support period should be clearly specified for the product version. Self-assessment questionnaire includes checking these elements and uploading evidence (photos, documents).	- Documentation (General description) - Product version details page (product support period) - CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization		
	(10),(11)	Possibility to assess, manage the self-assessment data at the product version level	- New Product Creation - Product Details Page - Add New Product Version - Product Version Details Page - CRA Compliance Assessment for a Product Version		
	(12)	Support in self-assessment of the content of required documentation	Documentation (Production & monitoring processes documentation, conformity verification - self-assessment questionnaire to check the content of required technical documentation)		
	(13)	Possibility to store, publish product related documentation	Documentation (General description, Specification of the design & development process of the product, Vulnerability handling process, Vulnerability/Incident reports, Cyber risk assessment, Conformity verification)		
	(14)	Support for self-assessment to check if there are procedures for the product that are parts of a series of production to remain conformity with CRA. Possibility to adapt the tool to new standards, harmonized standards, and	- CRA Process Assessment for an Organization - Administration of an Organization Assessment Questionnaire Template - Administration of a Product Assessment Questionnaire Template		



		change the scope of self-assessment questions.		
	(15), (16), (22)	Possibility to describe product, its versions, adding evidence, the ability to add files (photos, descriptions) that are evidence of compliance with the requirement for proper product labelling. Self-assessment report, related evidence, can be used for the authorities to prove the conformance.	- Product version details page (adding description, files) - CRA Compliance Assessment for a Product Version - Documentation (General description, Production & monitoring process documentation, Conformity verification)	
	(17)	Include questions in the questionnaires regarding the establishment of a single point of contact.	CRA Compliance Assessment for a Product Version	
	(18)	Self-assessment questionnaires include requirements regarding the scope of user documentation. The ability to attach documentation as evidence.	- Documentation (General description, Conformity verification) - CRA compliance self-assessment for the product version (questionnaire for the documentation scope and content)	
	(20)	Support for preparation of Declaration of Conformity for each product version (based on a template in OSCRAT) or uploading an external file. Evidence of conformity can be gathered in the tool	- Product version details page (view/upload Declaration of conformity for the product version). - Documentation (Conformity validation - template for the Declaration of conformity)	
	(21)	Self-assessment and user support in detecting gaps in requirements fulfilment. Additional guidance for users on meeting requirements.	Requirements evaluation - automatic task generation (for evaluated requirements)	

	(24), (25)		The evidence should also include SBOM files - support in preparing SBOM files and checking vulnerabilities based on these files.	SBOM management		
	Article 14	Reporting obligations of manufacturers	Support in collecting information on vulnerabilities and incidents - the scope of data as specified in Article 14, required for notifications, reporting to ENISA, CSIRT. Support in preparing reports on detected vulnerabilities and severe incidents. Support in incidents classification (severe/not severe).	• CRA Compliance Assessment for a Product Version • CRA Process Assessment for an Organization • Product version details page (product version related vulnerabilities, incidents) • Add New Vulnerability • Edit Vulnerability • Vulnerability Details Page • Add New Incident • Edit Incident • Incident Details Page • Documentation (General description, Vulnerability handling process - vulnerability report template, vulnerability reports)	1	1
	Article 15	Voluntary reporting	To the extent and in the manner that will be available at the time of tool implementation, support in reporting vulnerabilities / incidents to the relevant authorities (ENISA/CSIRT).	• CRA Compliance Assessment for a Product Version • Product version details page (product version related vulnerabilities, incidents) • Vulnerability Details Page • Incident Details Page • Documentation (Vulnerability handling process -	1	1

				vulnerability/incident report templates - to prepare the vulnerability/incident reports, to send reports to ENISA/CSIRT)		
Article 16	Establishment of a single reporting platform	Preparation for the submission of reports and incidents in accordance with the rules defined by ENISA for the single reporting platform (once established by ENISA).		- Product version details page (product version related vulnerabilities, incidents) - Vulnerability Details Page - Incident Details Page - Documentation (Vulnerability handling process - vulnerability/incident report templates - to prepare the vulnerability/incident reports, to send reports to ENISA/CSIRT)	1	1
Article 17	Other provisions related to reporting	N/A		Refers to the responsibilities of ENISA and CSIRTs		1
Article 18	Authorised representatives	Include requirements for authorised representatives in self-assessment questionnaires		- CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization - Product Assessment Dashboard, Visualization, PDF Export - Organization CRA Compliance Dashboard, Visualization & PDF Export	1	1
Article 19	Obligations of importers	Include requirements for product importers in self-assessment questionnaires		- CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization	1	1

				- Product Assessment Dashboard, Visualization, PDF Export - Organization CRA Compliance Dashboard, Visualization & PDF Export		
	Article 20	Obligations of distributors	Include requirements for product distributors in self-assessment questionnaires	- CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization - Product Assessment Dashboard, Visualization, PDF Export - Organization CRA Compliance Dashboard, Visualization & PDF Export	1	1
	Article 21	Cases in which obligations of manufacturers apply to importers and distributors	Where producers/distributors are subject to the same obligations as manufacturers (placing products on the market under their own name, trademark or making a significant modification), the same requirements of the CRA self-assessment questionnaires apply to them.	- CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization - Product Assessment Dashboard, Visualization, PDF Export - Organization CRA Compliance Dashboard, Visualization & PDF Export	1	1
	Article 22	Other cases in which obligations of manufacturers apply		- CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization	1	1
	Article 23	Identification of economic operators	Possibility of describing the product, including information about the entity that supplied the product or to which the product	Documentation (General description)	1	1

			was supplied, also in the event that there is a need to provide information to market surveillance authorities.			
	Article 24	Obligations of open-source software stewards	Include requirements for product open-source software stewards in self-assessment questionnaires	- CRA Process Assessment for an Organization - Product Assessment Dashboard, Visualization, PDF Export - Organization CRA Compliance Dashboard, Visualization & PDF Export	1	1
	Article 25	Security attestation of free and open-source software	N/A	Refers to the Commission's authority to establish voluntary security attestation programmes for free and open-source software developers.		1
	Article 26	Guidance	N/A	Refers to the Commission's obligations to publish guidelines for economic operators (especially small and medium-sized enterprises).		1
Chapter III Conformity of the product with digital elements	Article 27	Presumption of conformity	Readiness for changes in requirements, to include assessment of conformity with harmonised standards' requirements (Harmonised standards to be defined by the Commission).	- Administration of an Organization Assessment Questionnaire Template - Administration of a Product Assessment Questionnaire Template	1	Chapter III Conformity of the product with digital elements
	Article 28	EU declaration of conformity	Support in preparing or possibly adding a Declaration of Conformity for a given product version. Possibility to use a Declaration of Conformity template containing the elements required by the CRA.	- CRA Compliance Assessment for a Product Version - CRA Process Assessment for an Organization - Product Assessment Dashboard, Visualization, PDF Export	1	



	Article 29	General principles of the CE marking	CRA compliance self-assessment questionnaire should also include a question about ensuring proper CE marking. Possibility to upload files (photos, documents) confirming the product's proper labelling, CE marking.	- Organization CRA Compliance Dashboard, Visualization & PDF Export - Product version details page (view/upload declaration of conformity) - Documentation (General description, Production, monitoring processes documentation, Conformity verification)		
	Article 30	Rules and conditions for affixing the CE marking	and CRA compliance self-assessment questionnaire should also include a question about ensuring proper CE marking. Possibility to upload files (photos, documents) confirming the product's proper labelling, CE marking.	- Product version details page 1 (description, related files - documents, pictures) - CRA Compliance Assessment for a Product Version - Documentation (General description, Conformity Verification)		
	Article 31	Technical documentation	CRA compliance self-assessment questionnaire should include a question about the scope and content of a technical documentation that should be.	Documentation (General description, 1 Specification description of the design & development process of the product, Vulnerability handling process, Production & monitoring processes documentation,		

Chapter IV Notification of			Possibility to upload files (photos, documents) confirming the required documentation scope, content.	conformity verification - self-assessment questionnaire to check the content of required technical documentation) • CRA Compliance Assessment for a Product Version • CRA Process Assessment for an Organization		
	Article 32	Conformity assessment procedures for products with digital elements	Support of self-assessment (internal control procedure) according to module A (as specified in Annex VIII) with Possibility to upload a report/certificate on the product version assessment carried out by an external Conformity Assessment Body Providing a guide in the system, tips for users on how to choose the appropriate assessment module (from among the modules listed in Annex VIII).	• Guideline for selecting the 1 assessment module (procedure) • CRA Compliance Assessment for a Product Version • CRA Process Assessment for an Organization • Administration of an Organization Assessment Questionnaire Template.		
	Article 33	Support measures for microenterprises and small and medium-sized enterprise, including start-ups	N/A	It addresses possible actions by Member States to support micro and small enterprises in applying CRA. OSC RAT, as a publicly available tool supporting self-assessment and preparation for CRA compliance, could also be part of such actions.		
	Article 34	Mutual recognition agreements	N/A	Refers to agreements on mutual recognition of conformity.		
Chapter IV Notification of	Article 35	Notification	N/A			1

conformity assessment bodies	Article 36	Notifying authorities	N/A			1
	Article 37	Requirements relating to notifying authorities	N/A			1
	Article 38	Information obligation on notifying authorities	N/A			1
	Article 39	Requirements relating to notified bodies	N/A			1
	Article 40	Presumption of conformity of notified bodies	N/A			1
	Article 41	Subsidiaries of and subcontracting by notified bodies	N/A			1
	Article 42	Application for notification	N/A			1
	Article 43	Notification procedure	N/A			1
	Article 44	Identification numbers and lists of notified bodies	N/A			1
	Article 45	Changes to notifications	N/A			1

	Article 46	Challenge of the competence of notified bodies	N/A			1
	Article 47	Operational obligations of notified bodies	N/A			1
	Article 48	Appeal against decisions of notified bodies	N/A			1
	Article 49	Information obligation on notified bodies	N/A			1
	Article 50	Exchange of experience	N/A			1
	Article 51	Coordination of notified bodies	N/A			1
Chapter V Market surveillance and enforcement	Article 52	Market surveillance and control of products with digital elements in the Union market	N/A			1
	Article 53	Access to data and documentation	Support in collecting and providing materials confirming conformity with a product and processes CRA requirements.	Documentation (General description, 1 Specification description of the design & development process of the product, Vulnerability handling process, Production & monitoring processes documentation, conformity verification - self-assessment	1	1

			questionnaire to check the content of required technical documentation)		
Article 54	Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk	N/A			1
Article 55	Union safeguard procedure	N/A			1
Article 56	Procedure at Union level concerning products with digital elements presenting a significant risk	N/A			1
Article 57	Compliant products with digital elements which present a significant cybersecurity risk	N/A			1
Article 58	Formal non-compliance	N/A			1

	Article 59	Joint activities of market surveillance authorities	N/A			1
	Article 60	Sweeps	N/A			1
Chapter VI Delegated Powers and Committee procedure	Article 61	Exercise of the delegation	N/A			1
	Article 62	Committee procedure	N/A			1
Chapter VII Confidentiality and penalties	Article 63	Confidentiality	The platform and tool ensure the confidentiality of data, commercial information, business secrets, and personal data.	End user data confidentiality - Unicis platform 1		1
	Article 64	Penalties	N/A			1
	Article 65	Representative actions	N/A			1
Chapter VIII Transitional and final provisions	Article 66	Amendment to Regulation (EU) 2019/1020	N/A			1
	Article 67	Amendment to Directive (EU) 2020/1828	N/A			1
	Article 68	Amendment to Regulation (EU) No 168/2013	N/A			1

	Article 69	Transitional provisions	N/A			1
	Article 70	Evaluation and review	N/A			1
	Article 71	Entry into force and application	N/A			1
	Annex I Part I	Essential cybersecurity requirements	Support in self-assessment of compliance with essential cybersecurity requirements for product and processes, determining the degree of compliance, planning tasks to achieve compliance, uploading and storing evidence to confirm fulfilling the requirements.	• CRA Compliance Assessment for a Product Version • CRA Process Assessment for an Organization • Requirements Evaluation - Automatic Task Generation • Product Assessment Dashboard, Visualization, Export • Organization Assessment Dashboard, Visualization, Export • Documentation - General description		1
	Annex I Part II		Support for identifying vulnerabilities based on SBOM. Support for logging vulnerabilities in the system, collecting and storing information about them, storing analysis evidence, vulnerability management files, mechanisms for storing and sharing information, and security updates.	• Vulnerability handling • SBOM Management		
	Annex II	Information and instructions to the user	Support in verifying the scope and content of the user documentation required by the attachment.	• CRA compliance assessment for a product version • Documentation (Production & monitoring processes)		1

				documentation, conformity verification - self-assessment questionnaire to check the content of required technical documentation)		
	Annex III	Important products with digital elements	Support in determining the class of a product with digital elements and determining whether the product is subject to CRA.	Applicability Check (and Classification)	1	1
	Annex IV	Critical products with digital elements	Support in determining the class of a product with digital elements and determining whether the product is subject to CRA.	Applicability Check (and Classification)	1	1
	Annex V	EU declaration of conformity	Support preparation of Declaration of Conformity for each product version (based on a template in OSCRAT) or uploading an external file. Evidence of conformity can be gathered in the tool	• CRA Compliance Assessment for a Product Version • CRA Process Assessment for an Organization • Product Assessment Dashboard, Visualization, PDF Export • Organization CRA Compliance Dashboard, Visualization & PDF Export • Product version details page (view/upload declaration of conformity) • Documentation (General description, Production, monitoring processes documentation, Conformity verification)	1	1

	Annex VI	Simplified declaration conformity	EU Support preparation of Declaration of Conformity for each product version (based on a template in OSCRAT) or uploading an external file. Evidence of conformity can be gathered in the tool	• CRA Compliance Assessment for a Product Version • CRA Process Assessment for an Organization • Product Assessment Dashboard, Visualization, PDF Export • Organization CRA Compliance Dashboard, Visualization & PDF Export • Product version details page (view/upload declaration of conformity) • Documentation (General description, Production, monitoring processes documentation, Conformity verification)	1	
	Annex VII	Content of the technical documentation	For products and product versions registered in the tool, you can add descriptions and files (photos, documents) specified in the Annex.	• Documentation (General description, Specification description of the design & development process of the product, Vulnerability handling process, Production & monitoring processes documentation, conformity verification - self-assessment questionnaire to check the content of required technical documentation) • CRA compliance assessment for a product version • Product details page • Product version details page	1	1

				• Vulnerability details page • Incident details page • SBOM management • Incident/Vulnerability reports, related documents • SBOM files		
	Annex VIII	Conformity assessment procedures	Support of self-assessment (internal control procedure) according to module A (as specified in Annex VIII) Possibility to upload a report/certificate on the product version assessment carried out by an external Conformity Assessment Body Providing a guide in the system, tips for users on how to choose the appropriate assessment module (from among the modules listed in Annex VIII).	• Guideline for selecting the 1 assessment module • CRA Compliance Assessment for a Product Version • CRA Process Assessment for an Organization	1	1

Table 1 CRA-specific requirements – mapping on OSCRAT tool requirements and capabilities



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 14



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.



OSCRAT

Open-Source Cyber Resilience Act Tools

D2.1

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 15

Submission date: 30 11, 2025

Author: Dariusz Rogowski
Lukasiewicz-AI



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 15
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

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 template for vulnerability Disclosure Policy.
Keywords
Vulnerability Disclosure Policy

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.

Vulnerability Disclosure Policy Template

```
# Security & Vulnerability Disclosure Policy

## Our Commitment

At [Your Company Name], we are committed to ensuring the security of our products
and services. We value the work of the independent security research community, and
we welcome the responsible disclosure of any potential vulnerabilities.

## Safe Harbor

We consider security research conducted under this policy to be authorized and will
not pursue or support any legal action against you for good-faith, accidental, non-
disruptive violations of this policy. We explicitly waive any claims against you
for circumventing the technological measures we have in place to protect our
services.

## Scope

This policy applies to the following products and services:
* [List your in-scope products, e.g., "Product A Firmware version 2.0 and later"]
* [List your in-scope services, e.g., "api.example.com"]

**Out of Scope:**
* Any services hosted by third-party providers.
* Denial of service (DoS or DDoS) testing.
* Social engineering or phishing of our employees or customers.
* Physical attacks against our property or data centers.

## How to Report a Vulnerability

Please send a detailed report to our security team at **security@example.com**. If
possible, encrypt your message using our [PGP Key](link-to-your-gpg-key.asc).

To help us triage and validate your finding as quickly as possible, your report
should include:
* The product or service affected and the version number.
* A detailed description of the vulnerability.
* Step-by-step instructions to reproduce the issue.
* Any proof-of-concept exploits, scripts, or screenshots.

## Our Commitments (SLAs)

When you report a vulnerability to us under this policy, we will:
* Acknowledge receipt of your report within **2 business days**.
* Provide an initial assessment and expected timeline for remediation within **10
business days**.
* Keep you informed of our progress as we work to resolve the issue.
* Notify you when the vulnerability has been fixed.

## Public Recognition

We believe in recognizing the valuable contributions of security researchers. With
your permission, we will offer public thanks and credit for your discovery on our
website or in our release notes once the vulnerability has been remediated.
```



OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – COMPREHENSIVE PROJECT REQUIREMENTS DOCUMENT – ANNEX 15



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.