PRESS RELEASE

OSCRAT: WP2 completed. Tool development begins

OSCRAT completes WP2 and kicks off the development phase of the tool that will help SMEs strengthen cybersecurity and ensure CRA compliance.

OSCRAT: WP2 completed. Development of the cybersecurity and CRA compliance tool begins

OSCRAT, the European project developing open-source tools to help SMEs comply with the Cyber Resilience Act (CRA), is entering a crucial phase. The consortium has just completed Work Package 2 (WP2), dedicated to requirements gathering and analysis, and is now moving into the design and actual development of the platform.

Why OSCRAT?

The lack of dedicated cybersecurity resources exposes European SMEs to significant economic and reputational risks. OSCRAT (**Open-Source Cyber Resilience Act Tools**), funded by the European Union's **Digital Europe** program, was created to address this gap through three high-level policy objectives:

- strengthening the Union's competitiveness in the global economy;

Co-funded by the European Union

The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre. 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.

- reducing the **digital divide** among Member States;
- enhancing the EU's capacity to act in strategic digital technologies.

At the core of the project is the development of a free and open-source tool that enables businesses to:

- assess their cybersecurity posture;
- verify compliance with the requirements of the Cyber Resilience Act, the European regulation that defines cybersecurity standards for products with digital elements.

OSCRAT is aligned with broader EU policies and pursues five operational goals: strengthening SME resilience, facilitating CRA compliance, promoting cross-border collaboration, contributing to environmental sustainability, and ensuring adherence to the EU's cybersecurity policy framework.

A new milestone: completion of WP2

Led by the partner Łukasiewicz AI, the consortium has now entered a new strategic phase: the production of the deliverable **D.2.1 - Comprehensive Project Requirements Document**. This document collects and systematically organizes all the requirements that will guide the design, development, and validation of the OSCRAT tools.

The completion of WP2 also made it possible to:

1. Define the technical scope of the OSCRAT tools

The functionalities of the main modules have been described in detail:

- Checklist Automation;
- SBOM Management;
- Vulnerability & Incident Handling;
- Documentation Centralization

2. Design CRA-compliant workflows

The partners modeled the entire compliance process, including:

- product classification
- pre-market and post-market obligations
- definition and verification of cybersecurity controls
- user stories and use cases specific to each tool.

Co-funded by the European Union

The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre. 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.

3. Map CRA requirements and cybersecurity requirements

The consortium conducted a systematic review of the CRA regulation identifying, for each tool:

- applicable CRA requirements;
- mandatory assessment and documentation processes;
- essential security elements to be verified.

In other words, the regulation has been "translated" into **operational software features**, an essential step to truly automate compliance processes.

The role of stakeholders and SMEs

One of the key elements of WP2 was the involvement of stakeholders. The requirements analysis highlighted:

- the **technical expertise** of the consortium partners (research, software development, cybersecurity consulting, digital innovation hubs);
- two rounds of **Stakeholder Surveys** conducted to understand the needs, expectations, and challenges of SMEs and other potential users of the OSCRAT tools;
- the current landscape of tools and initiatives related to the CRA across Europe.

Two strong messages also emerged:

- SMEs place high value on compliance automation tools, which reduce internal workload, costs, and the need for highly specialized expertise.
- there is a concrete willingness to participate in testing—an essential aspect for the tool validation phase.

These inputs have been directly incorporated into the tool workflows and development priorities, ensuring that OSCRAT is not a theoretical exercise, but a **platform designed "from the real-world needs**" of European SMEs.

Co-funded by the European Union

The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre. 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.

What happens next?

With the completion of WP2, OSCRAT can now begin **Work Package 3 – Software design and development**, coordinated by the partner **Oves Enterprise**.

The next planned activities include:

1. Architectural design of the platform

Definition of the software architecture, modules, interfaces, and integrations among the various tools (checklists, SBOM, incident management, and documentation repository).

2. Development and integration of CRA features

Implementation of the features mapped during WP2, with particular focus on usability for SMEs and precise alignment with CRA requirements.

3. Validation through real-world use cases

Testing of the system through concrete scenarios, in collaboration with SMEs and stakeholders who have already expressed interest and availability to participate.

4. Workshops

Organization of training and demonstration activities to support the adoption of the tools and increase awareness of CRA and cybersecurity topics.

Expected impact: an open-source cybersecurity platform serving European SMEs

Looking at the overall picture, OSCRAT is shaping up to become a platform that is:

- open source and free, making it accessible even to organizations with limited budgets.
- designed for SMEs, which often lack dedicated teams for compliance activities.
- aligned with the EU regulatory framework, not only the CRA, but also broader digital strategies.
- built collaboratively, thanks to the involvement of multiple partners from Italy, Romania, Bulgaria, Poland, and Estonia, along with other stakeholders.

Co-funded by the European Union

The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre. 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.

- sustainable, in line with the objectives of the European Green Deal and the vision of responsible digital transformation.

The completion of WP2 is far more than a simple administrative milestone: it is the step that turns the initial vision (**as described earlier**) into a concrete technical roadmap for developers and for the entire consortium.

In the coming months, as **WP3** progresses and **testing and training activities** advance, OSCRAT will demonstrate how to transform the project into tangible results, **helping SMEs strengthen their cybersecurity posture** and be fully prepared for the regulatory landscape introduced by the Cyber Resilience Act.

Contact us to join similar projects

If you want to learn more about OSCRAT or are looking for partners for similar projects, you can reach out to us by:

- Call us on **+390950936053**.
- Send an email to **projects@jogroup.eu**
- Fill out the contact form in the "Contact" section of OSCRAT website!

Co-funded by the European Union

The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre. 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.