

Newsletter from OSC RAT!



The OSC RAT Platform is Live: Start Your Cyber Resilience Journey Today

The OSC RAT project has reached its final milestone with the official launch of the OSC RAT Platform, a free and open-source solution designed to support European organisations, especially SMEs, in addressing the requirements of the **Cyber Resilience Act (CRA)**.

Officially launched on **11 September 2026** during the OSC RAT Final Event, the platform is now fully operational and accessible at:

[Visit the OSC RAT Platform](#)



The launch coincided with the entry into application of the first CRA reporting obligations, marking an important step towards helping companies translate cybersecurity requirements into practical processes.

From this date, manufacturers are required to report actively exploited vulnerabilities and severe incidents affecting products with digital elements, with an early warning within 24 hours and a more detailed notification within 72 hours.

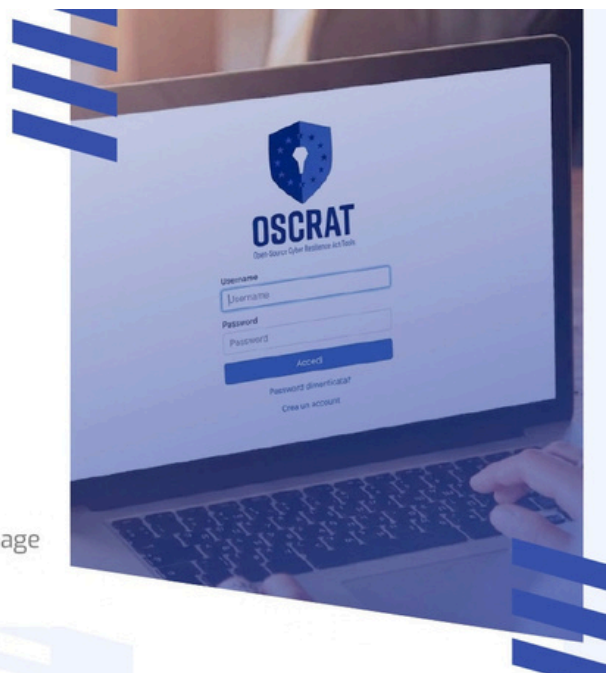
A practical solution for managing CRA compliance



OSCRAT PLATFORM

Start your Cyber Resilience Act compliance journey

A free, open-source platform designed to help organisations — especially SMEs — assess, manage and document their cybersecurity compliance.



The OSCRAT Platform provides organisations with a structured environment to manage cybersecurity activities throughout the lifecycle of products with digital elements.

Developed as a free, open-source solution, OSCRAT brings together key compliance and security processes into a single platform, helping organisations improve visibility, documentation, and traceability of cybersecurity activities.

The platform supports users in:

- **Assessing CRA applicability and compliance requirements**, helping organisations understand which obligations may apply to their products;
- **Managing Software Bills of Materials (SBOMs)** and analysing software components to improve supply-chain visibility;
- **Tracking vulnerabilities and security incidents**, including their assessment, remediation activities and follow-up actions;
- **Performing cybersecurity risk assessments** and managing risk-treatment workflows;
- **Managing configurations and compliance tasks** to ensure structured security processes;
- **Organising technical documentation and compliance evidence**, including workflows supporting the preparation of the EU Declaration of Conformity.

The platform follows a product lifecycle approach, enabling manufacturers and other stakeholders to maintain structured information about products, versions, security activities and documentation over time.

Who can benefit from OSCRAT?

OSCRAT has been designed to support a wide range of stakeholders involved in the cybersecurity and compliance lifecycle, including:

- **Small and medium-sized enterprises (SMEs)** developing or placing digital products on the European market;
- **Manufacturers and product teams** managing cybersecurity requirements throughout product development and maintenance;
- **Compliance and cybersecurity professionals** responsible for risk management and documentation;
- **Digital Innovation Hubs and support organisations** assisting companies in their CRA preparation journey.

By providing accessible open-source tools, OSCRAT aims to reduce complexity and support organisations in building more structured cybersecurity practices. The project's objective is to make CRA-related processes more accessible, particularly for SMEs that may face challenges in allocating dedicated cybersecurity resources.

[Discover the OSCRAT Platform](#)



Join the upcoming OSCRAT online event: OSCRAT in Action: Platform Demo and UPKIP's Cyber Resilience Assessment Journey



The event will provide a practical introduction to the **OSCRAT Platform** through the real-world assessment journey of UPKIP. Participants will see how UPKIP used the platform to carry out its Cyber Resilience Act assessment, while exploring the main OSCRAT functionalities and how they can support organisations throughout their own CRA compliance journey.

During the session, you will:

- Follow UPKIP's assessment journey and discover how the organisation used OSCRAT in practice
- Discover the main features and workflow of the OSCRAT Platform
- Learn how to navigate the platform and use its cybersecurity compliance functionalities
- See how OSCRAT supports organisations in assessing products, managing cybersecurity information and preparing compliance documentation
- Explore how the experience of UPKIP can serve as a practical example for organisations starting their own CRA preparation

The demo is an opportunity for SMEs, cybersecurity professionals, Digital Innovation Hubs and other stakeholders to see OSCRAT in practice, learn from a real assessment experience and explore how the platform can support their own CRA preparation activities. 📌

👉 **Register here** and join the session to discover how OSCRAT can support your cybersecurity compliance journey.

OSCRAT: supporting a more cyber-resilient European digital ecosystem

The OSC RAT Platform is now fully operational and available to organisations looking for practical ways to approach Cyber Resilience Act compliance.

Together with the platform, OSC RAT provides a growing collection of resources, training materials and practical use cases designed to help SMEs, manufacturers, cybersecurity professionals and other stakeholders better understand CRA requirements and translate them into concrete cybersecurity and compliance activities.

Access these resources and discover how OSC RAT can support your organisation's cyber resilience journey.

[Explore OSC RAT's resources here](#)



Follow OSC RAT for updates and cybersecurity resources



[OSCRAT EU Project on LinkedIn](#)



Follow us on social media



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. 10101080 is supported by the European Cybersecurity Competence Centre.