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. – Project: 101190180

Our first ask for you today:

Support the development of an effective tool tailored to SMEs by completing the OSCRAT stakeholder survey.

OSCRAT

Open-Source Cyber Resilience Act Tools

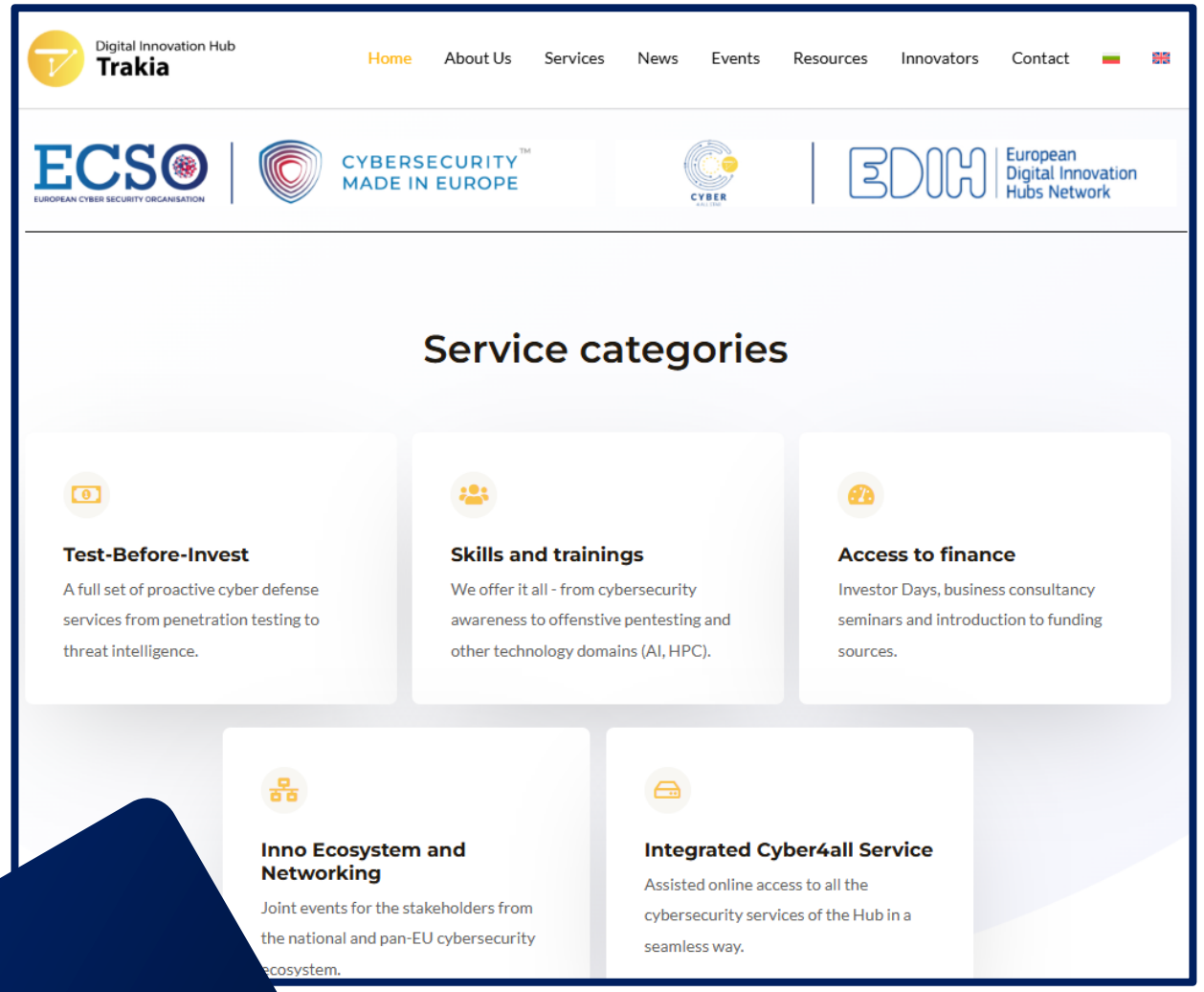
- **Starting date:** 01 / 12 / 2024
- **Ending date:** 31 / 05 / 2026
- **Purpose**: Developing tools that will support compliance procedures for European SMEs, to address the essential requirements of the CRA by facilitating internal compliance processes and enhancing cyber resilience among SMEs.
- **Website**: OSCRAT.eu

Co-funded by the European Union

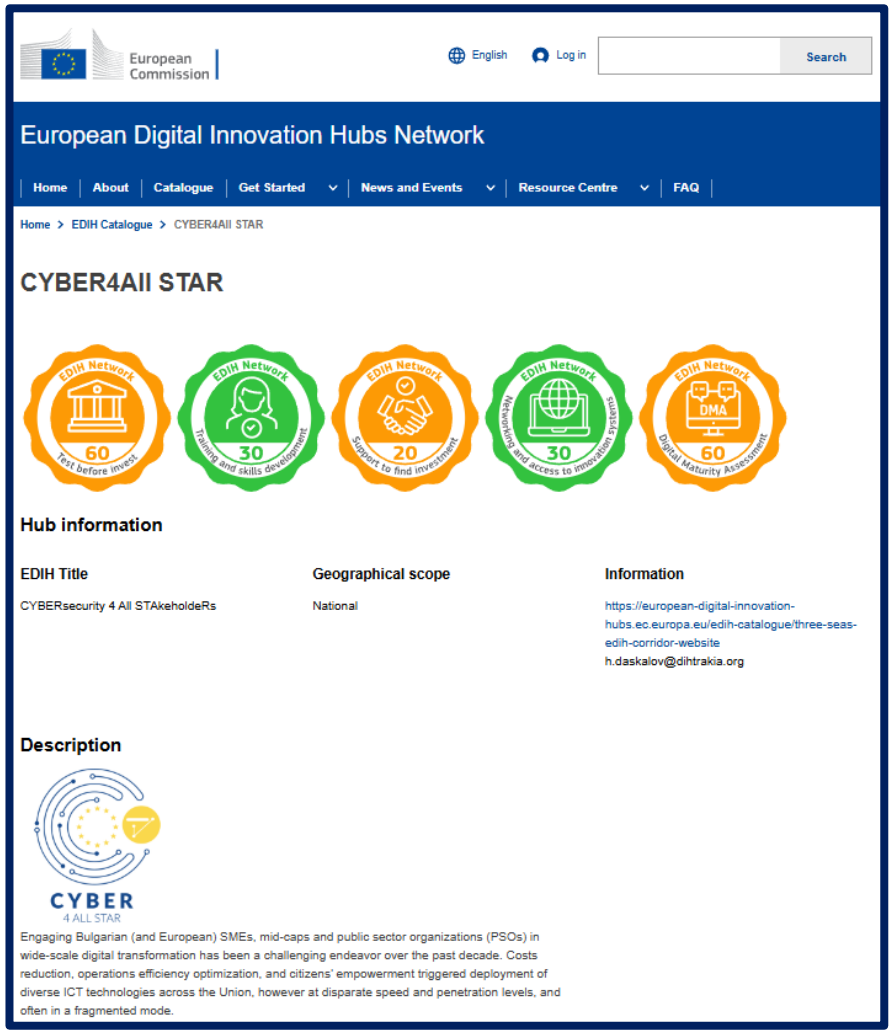
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

European Digital Innovation Hub Trakia
EDIH Trakia / Cyber4AllSTAR EDIH

https://dihtrakia.org



https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue/cyber4all-star



The **OSCRAT Consortium**

The OSCRAT consortium is composed by:

PMF Research

Italy

Project Coordinator

Oves Enterprise

Romania

ENERSEC

Romania

EDIH Trakia

Bulgaria

EMAG

Poland

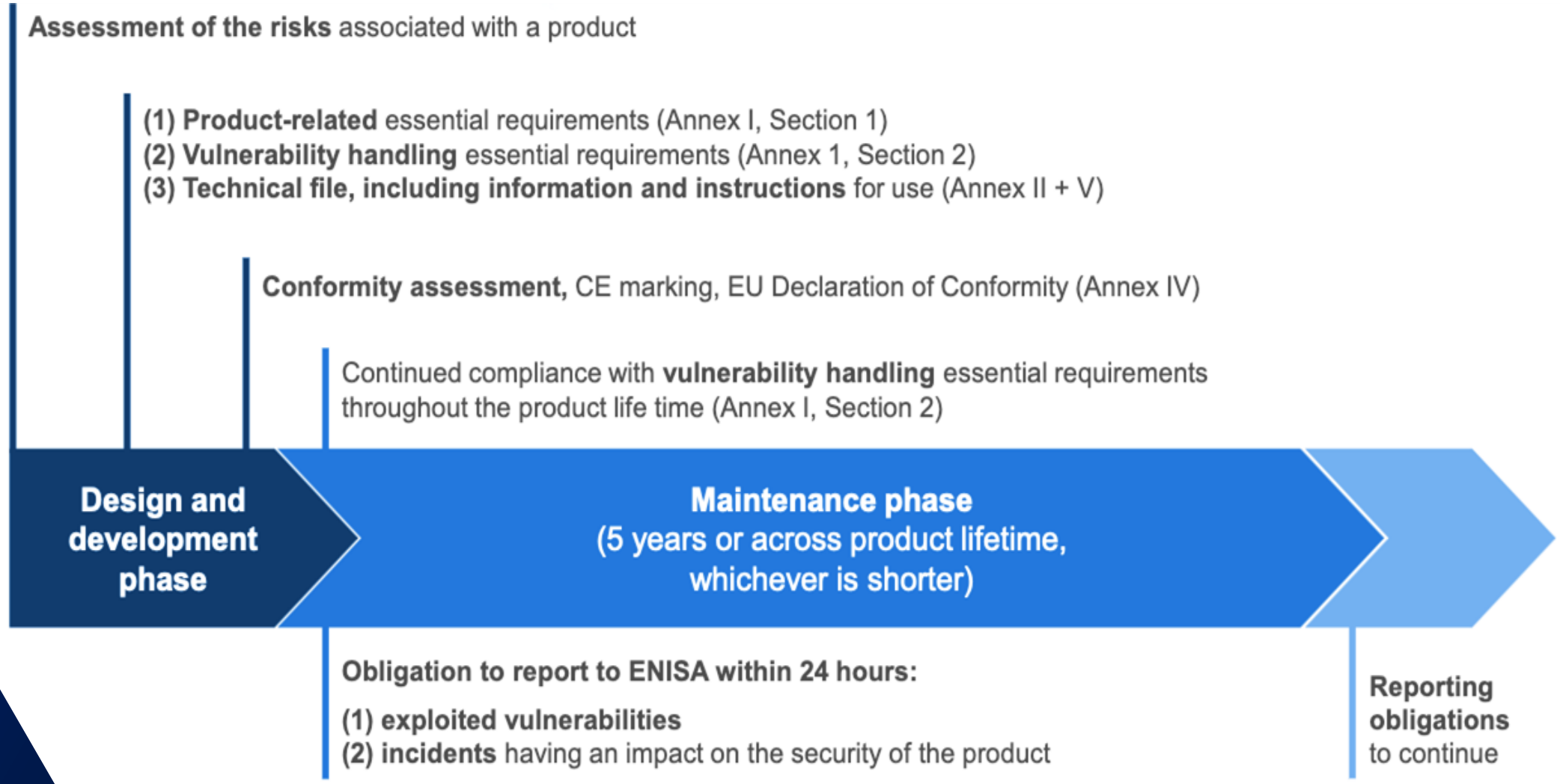
Unicis.Tech OÜ

Estonia

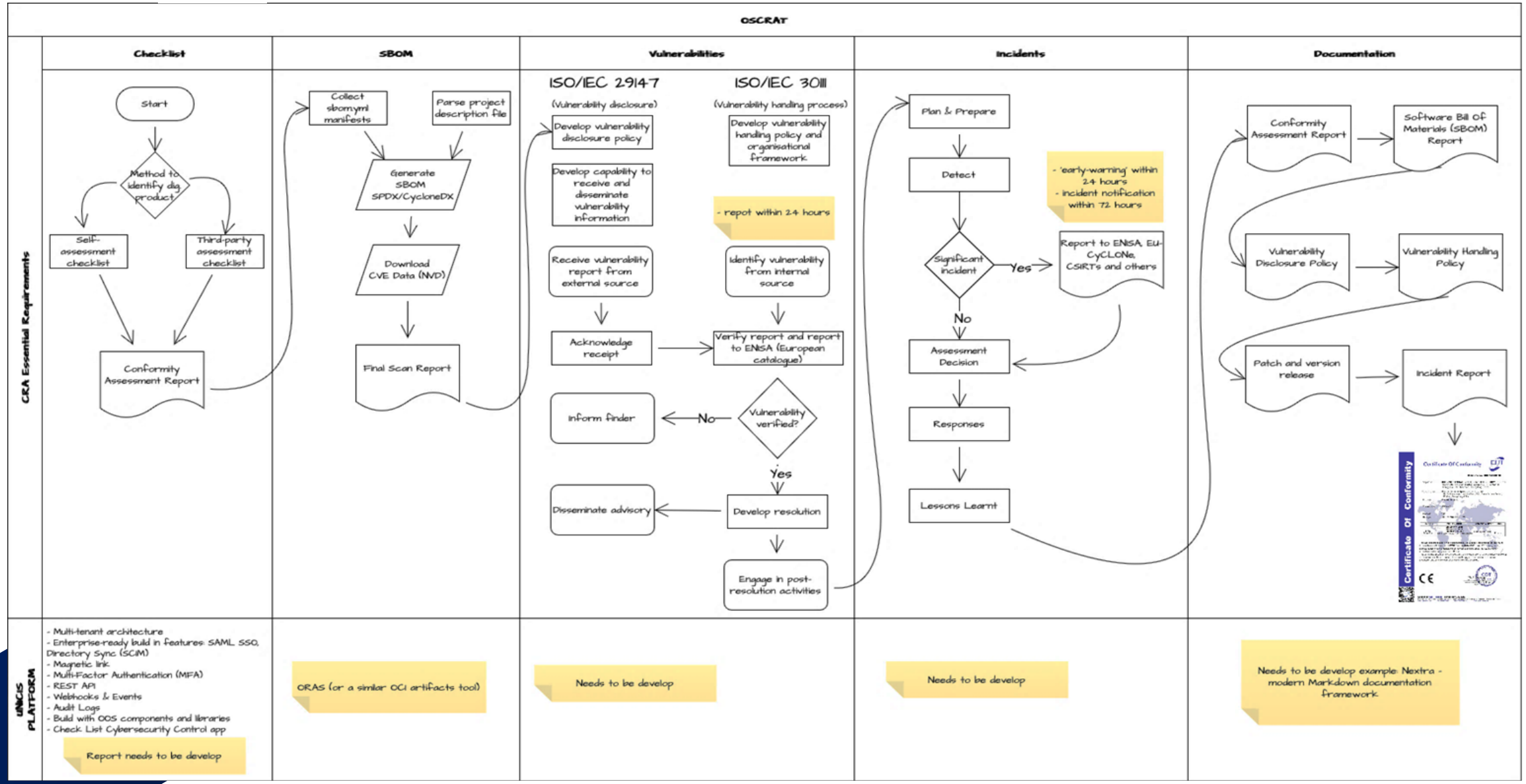
OSCRAT
Open-Source Cyber Resilience Act Tools

The **Need Behind OSCRAT**

Co-funded by the European Union



The **OSCRAT Platform**



OSCRAT
Open-Source Cyber Resilience Act Tools

The **Timing Behind OSCRAT** (1)

Co-funded by the European Union

Actor	Action	Reference	Deadline
European Commission	Adopt an implementing act specifying technical descriptions of categories of products with digital elements	Art. 7(4)	11 December 2025
European Commission	Adopt delegated acts specifying terms and conditions for delaying the dissemination of notifications	Art. 14(9)	11 December 2025
Economic Operators	Conformity assessment bodies notifications provisions apply	Art. 71(2)	11 June 2026
Economic Operators	Reporting obligations concerning actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements apply	Art. 71(2)	11 September 2026
Member States	Ensure a sufficient number of bodies to perform conformity assessments, thus avoiding obstacles to market entry	Art. 35	11 December 2026
ENISA	Prepare and submit a technical report on trends on emerging cybersecurity risks	Art. 17(3)	11 December 2026
Member States	The Cyber Resilience Act fully applies	Art. 69(3)	10 December 2027
Manufacturers/ Retailers	Requirements for products with digital elements placed on the market before December 2027 apply if substantially modified	Art. 69(2)	11 December 2027

OSCRAT
Open-Source Cyber Resilience Act Tools

The **Timing Behind OSCRAT** (2)

Co-funded by the European Union

Actor	Action	Reference	Deadline
Manufacturers/ Retailers	Article 14 obligations to products with digital elements placed on the market before December 2027 apply	Art. 69(3)	11 December 2027
Member States	Provisions regarding infringements by economic operations harming consumers apply	Rec. 124	11 December 2027
Manufacturers/ Retailers	Expiration of EU-type examination certificates and approval decisions	Art. 69(1)	11 June 2028
European Commission	Submit a report on the single reporting platform's effectiveness	Art. 70(2)	11 September 2028
European Commission	Prepare a report concerning delegation of power	Art. 61(2)	10 March 2029
uropean Parliament/ Council	Optionally oppose the extension of the delegation of power, preventing the Commission from continuing to exercise its delegated authority beyond the original timeframe set in the Act	Art. 61(2)	10 September 2029
Commission	Optionally adopt delegated acts, introducing legal provisions that supplement or clarify the main Regulation if necessary for effective implementation	Art. 61(2)	10 December 2029

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. – Project: 101190180

Our second ask for you today:

Fill-in the feedback form from the training event in order to improve the content and its delivery for the upcoming edition next month.

OSCRAT

Open-Source Cyber Resilience Act Tools

- **Type of event:** Training
- **Date:** 13 / 10 / 2025
- **Purpose**: The expert-led session is designed to guide participants through the core regulatory, technical, and documentation expectations under the CRA framework.
- **Website**: OSCRAT.eu

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT
Open-Source Cyber Resilience Act Tools

The **Trainers**

Co-funded by the European Union

Miroslav Mitev, PhD

Artificial Intelligence Institute, Co-Founder

With more than 3,000 audit days under his belt, Miroslav Mitev is one of Bulgaria's most seasoned experts on conformity assessment and ISO-based compliance. He has extensive teaching experience in cyber risk, incident response, and security governance and is frequently consulted on CRA, NIS2, DORA and national legislative alignment. Miroslav is also a co-founder of the Artificial Intelligence Institute (Bulgaria), where he fosters the intersection of artificial intelligence, cybersecurity, and digital trust frameworks.

Sashka Boncheva

Women4Cyber Bulgaria, Co-Founder

Cybersecurity expert and lead ISO auditor, Sashka Boncheva brings over 15 years of hands-on experience in implementing and auditing information security and quality management systems across both the public and private sectors. She is a certified Lead Auditor in ISO/IEC 27001, ISO 20000-1, ISO 27701 and other key standards, and actively advises SMEs on cybersecurity readiness. Sashka is also a co-founder of the Bulgarian chapter of Women4Cyber, where she works to improve gender balance and digital inclusion in cybersecurity.

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. – Project: 101190180

Our third ask for you today:

Explore the other CRA support initiatives / projects and get use of the opportunities they provide.

OSCRAT

Open-Source Cyber Resilience Act Tools

- **Type of activity:** Project knowledge dissemination
- **Source:** 13 / 10 / 2025
- **Purpose**: Helping SMEs navigate CRA compliance with confidence.
- **Website**: OSCRAT.eu

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT
Open-Source Cyber Resilience Act Tools

Essential Tools to Facilitate CRA for SMEs (1)

Co-funded by the European Union

1. Compliance Assessment and Gap Analysis Tools

Automated tools that assess SMEs' current cybersecurity posture, identify gaps in compliance with CRA requirements, and provide recommendations for remediation.

2. Compliance Checklist Generators

User-friendly tools that generate customized checklists based on SMEs' specific industry, size, and regulatory obligations under the CRA, guiding them through the compliance process step-by-step.

3. Policy and Procedure Templates

Pre-designed templates for developing essential CRA compliance policies, procedures, and documentation tailored to SMEs' needs, saving time and resources in creating these foundational documents

4. Risk Management Platforms

Integrated risk management solutions that help SMEs identify, assess, prioritize, and mitigate cybersecurity risks in alignment with CRA requirements, providing a structured approach to risk management.

5. Vulnerability Scanning and Patch Management Tools

Automated vulnerability scanning tools that detect and prioritize security vulnerabilities within SMEs' IT infrastructure and applications, along with patch management capabilities to facilitate timely remediation.

6. Compliance Documentation Automation Platforms

Platforms that streamline the creation, organization, and maintenance of CRA compliance documentation for SMEs, offering templates, version control, and document management functionalities to ensure regulatory adherence.

OSCRAT
Open-Source Cyber Resilience Act Tools

Essential Tools to Facilitate CRA for SMEs (2)

Co-funded by the European Union

7. Security Awareness Training Modules

Interactive e-learning modules and training materials focused on educating SME employees about cybersecurity best practices, CRA compliance obligations, and threat awareness to foster a security-conscious culture.

8. Incident Response Planning Software

Incident response planning tools that guide SMEs through the development of comprehensive incident response plans, including workflows, communication protocols, and escalation procedures, to effectively respond to cybersecurity incidents.

9. Security Configuration Management Solutions

Tools that automate the configuration and hardening of SMEs' IT systems and network devices according to CRA-prescribed security standards and best practices, reducing the risk of misconfigurations and unauthorized access.

10. Continuous Monitoring and Reporting Dashboards

Real-time monitoring dashboards that provide SMEs with visibility into their cybersecurity posture, compliance status, and ongoing performance against CRA requirements, enabling proactive risk management and reporting.

The other **CRA Support Initiatives**

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

OSCRAT
Open-Source Cyber Resilience Act Tools

The other **CRA Support Initiatives**

Co-funded by the European Union

CRACoWi

Cybersecurity Compliance Made Easy

WWW.CRACOWI.EU

AUTOMATED COMPLIANCE & CERTIFICATION

The project introduces an automated system that facilitates CRA compliance assessments, documentation generation, and cybersecurity certification

EMPOWER SMES

Designed to support SMEs in adopting and complying with the Cyber Resilience Act, providing structured processes and automated compliance tools.

HOLISTIC CYBERSECURITY APPROACH

Ensures cybersecurity is covering the entire product lifecycle and proactively monitoring for new vulnerabilities to minimize the risk of cyberattacks.

CAPACITY BUILDING & DISSEMINATION

Enhancing awareness of cybersecurity and compliance; and delivery of extensive capacity building program supported with strategic dissemination.

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT
Open-Source Cyber Resilience Act Tools

The other **CRA Support Initiatives**

Co-funded by the European Union

https://cra-cy.eu/

The other **CRA Support Initiatives**

STRENGTHENING CYBER DEFENSES OF SMES FOR CYBER RESILIENCE ACT (CRA) COMPLIANCE

- ✓ The **18 months EU-cofunded** Project **CYBERFORT** is led by **I-ENERGYLINK (RO)**, supports **SME**s and **Managed Service Providers** (MSPs) in navigating **CRA compliance**
- ✓ **Developing** a tailored **Compliance Management Software** (CMS) solution by:
- ✓ **Offering practical tools, guidance, and collaborative resources** to address **cybersecurity challenges** and simplify adherence to CRA and related standards
- ✓ **Introduces a Comprehensive Concept** aimed at **bolstering the cybersecurity defenses of SMEs**, particularly focusing on **Micro and Small Businesses**.
- ✓ **Rrepresents** an **Innovative Program** designed to equip **European SMEs** with the tools to strengthen their cybersecurity measures and achieve adherence to the **CRA & other relevant cybersecurity compliance standards**.

- ✓ **4 Complementary Use Cases** under implementation:
- ✓ Shipboard Cybersecurity Training Program (**Maritime Sector**)
- ✓ Compliance Management Platform for Financial Institutions (**Finance Sector**)
- ✓ Critical Infrastructure Vulnerability Assessment Tool (**Energy Sector**)
- ✓ Strategically Aligning **Cybersecurity Solutions with CRA Compliance** Standards.

Co-funded by the European Union

This Project has received funding from the Digital Europe Programme under Grant Agreement No: 101190281

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CYBERFORT
RESILIENT EUROPE

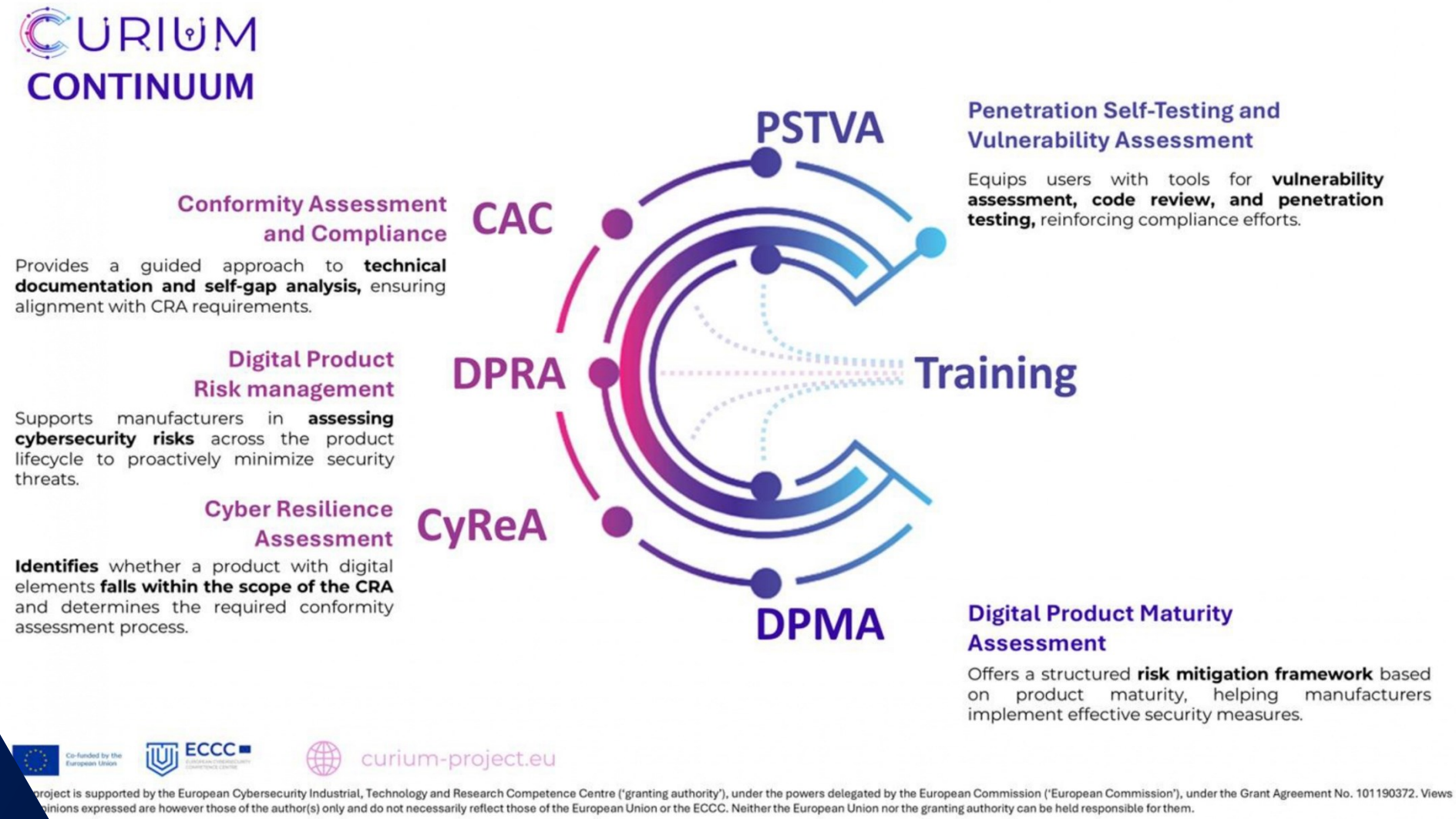
CYBERFORT Webinar, "SMEs and Cyber Resilience Act Compliance: Challenges and Solutions," → Link

- ✓ Over 120 Experts from European Org: **DNSC, ANCOM, ENISA, ECSO, Columbia Shipmanagement, CLONE SYSTEMS**
- ✓ Sharing **Practical Tools, Regulatory insights, and Sectorial Use Cases**
- ✓ Highlighting **how SMEs can effectively tackle CRA compliance** through collaboration

Dr. Mihai PAUN – Founder I-ENERGYLINK

https://cyber-fort.eu/

The other **CRA Support Initiatives**



project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre ('granting authority'), under the powers delegated by the European Commission ('European Commission'), under the Grant Agreement No. 101190372. Views pinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC. Neither the European Union nor the granting authority can be held responsible for them.

https://curium-project.eu/

The other **CRA Support Initiatives**

About CONFIRMATE

CONFormIty assessment, metRics and compliance autoMATion for the cyber resiliencE act

What: A suite of comprehensive open-source tools supported by several instruments to facilitate and automate compliance with the **Cyber Resilience Act (CRA)**, including:

- Automation tool for **CRA** cybersecurity essential requirements conformity assessment
- CRA compliance guide
- Pentesting methodology
- Training modules

in 5 languages: EN, DE, FR, IT, RO
=> cover 60% of EU population

How: Extending an existing open-source tools (Clouditor) with CRA cybersecurity requirements. Adopting a collaborative approach to feed the input and experience of stakeholders into the tools.

Primary target: EU manufacturing SMEs and industry associations

When: Jan 2025 - Jul 2026

Co-funded by the European Union

The project funded under Grant Agreement No. 101190193 is supported by the European Cybersecurity Competence Centre

https://confirmate-project.eu/

OSCRAT
Open-Source Cyber Resilience Act Tools

The other **CRA Support Initiatives**

Co-funded by the European Union

Key Work Packages

Co-funded by the European Union

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 Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The project funded under Grant Agreement No. 101158687 is supported by the European Cybersecurity Competence Centre

❖ **CyberBoost Platform Design and Implementation:**

- SaaS platform to manage cybersecurity certifications,
- real-time dashboards aligning with EU regulations like CRA and NIS2.

❖ **Use Cases Development and Pilot Projects**
to test the platform's effectiveness

❖ **Cross-Border Collaboration and Knowledge Exchange**

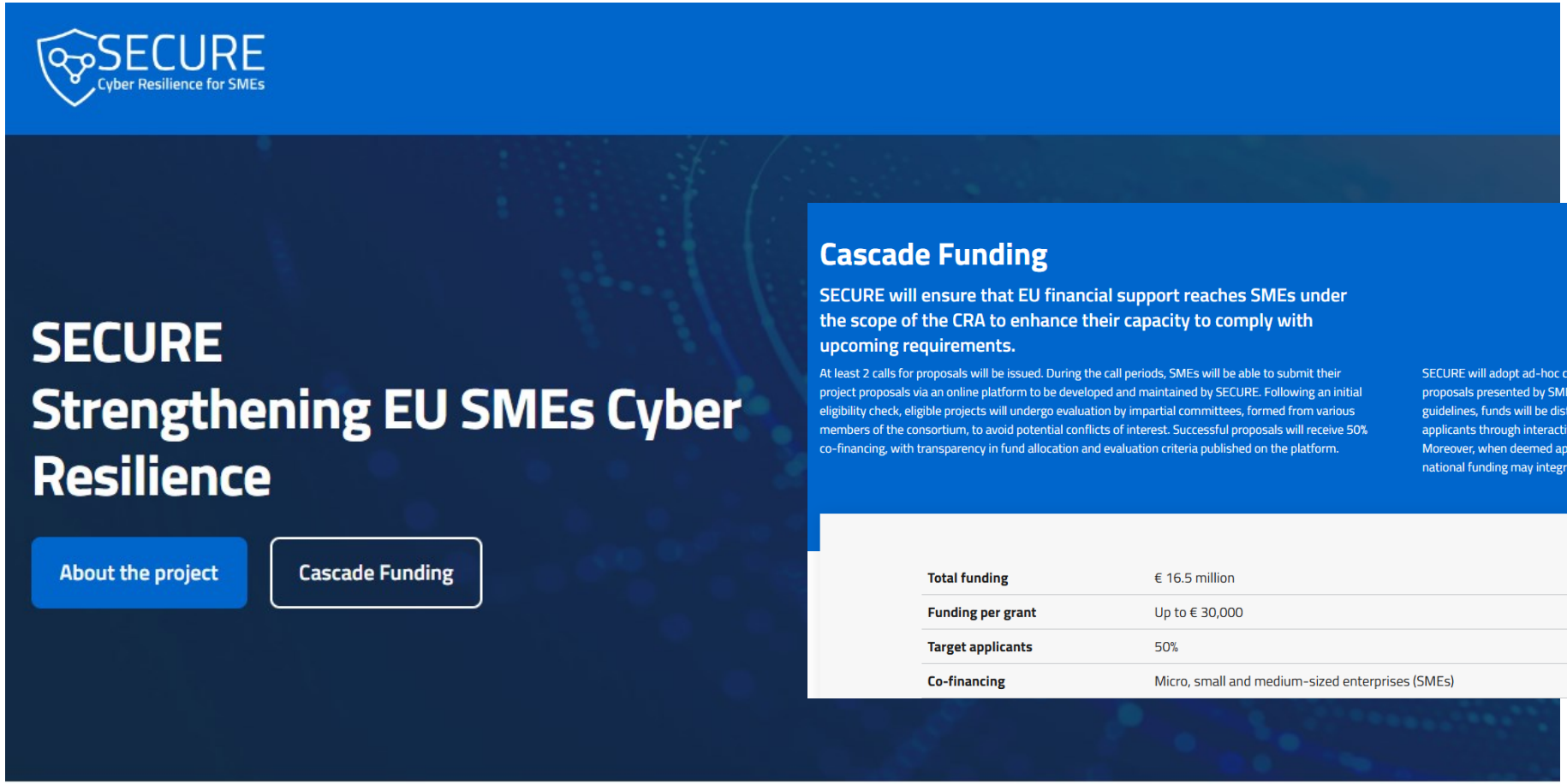
❖ **Finalization and Policy Recommendations**

TrustBoost

www.trustboost.eu

The other **CRA Support Initiatives**

Co-funded by the European Union



SECURE supports and enhances **EU SMEs cyber resilience capabilities**, protecting them from cyber threats and thus contributing to maintaining the integrity of the EU's digital single market.

https://secure4sme.eu/

The other **CRA Support Initiatives**

https://cyberstand.eu/

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. – Project: 101190180

Our final ask for you today:

Download the materials from today's training and keep in touch with us in case you have additional questions throughout your CRA compliance journey.

OSCRAT

Open-Source Cyber Resilience Act Tools

- **Next Training:** 10 / 11 / 2025
- **Registration:** https://eu01web.zoom.us/webinar/register/WN_SKFg2CF3Q5yDBGYkFGqoKg#/registration
- **Additional Benefits**: A deeper look into the broader compliance framework for PDEs in which the Cyber Resilience Act exists.
- **Website**: OSCRAT.eu

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE