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

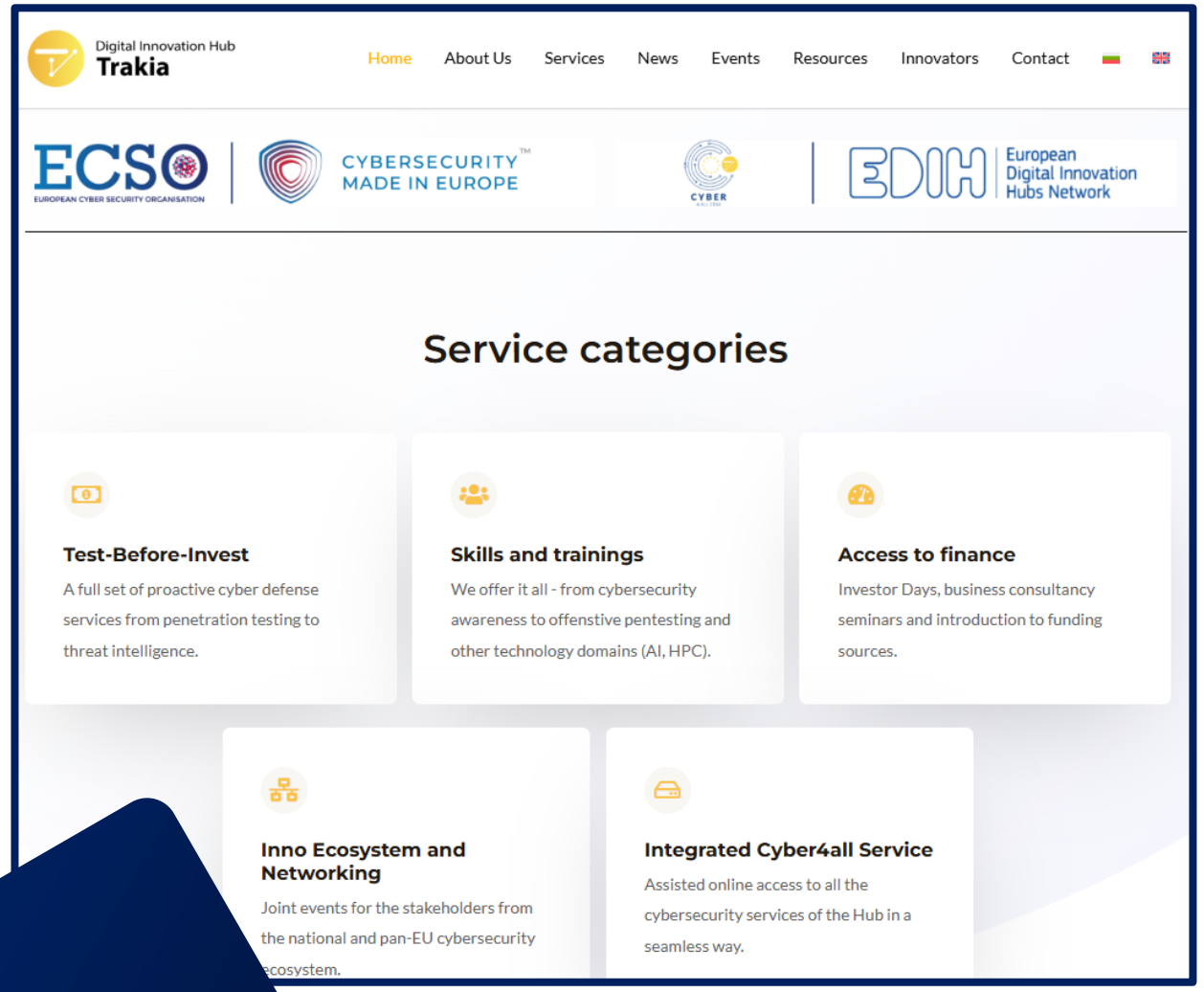
- **Starting date:** 01 / 12 / 2024
- **Ending date:** 31 / 05 / 2026
- **Purpose**: Developing tools that will support compliance procedures for European SMEs, to address the essential requirements of the CRA by facilitating internal compliance processes and enhancing cyber resilience among SMEs.
-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

Co-funded by the European Union

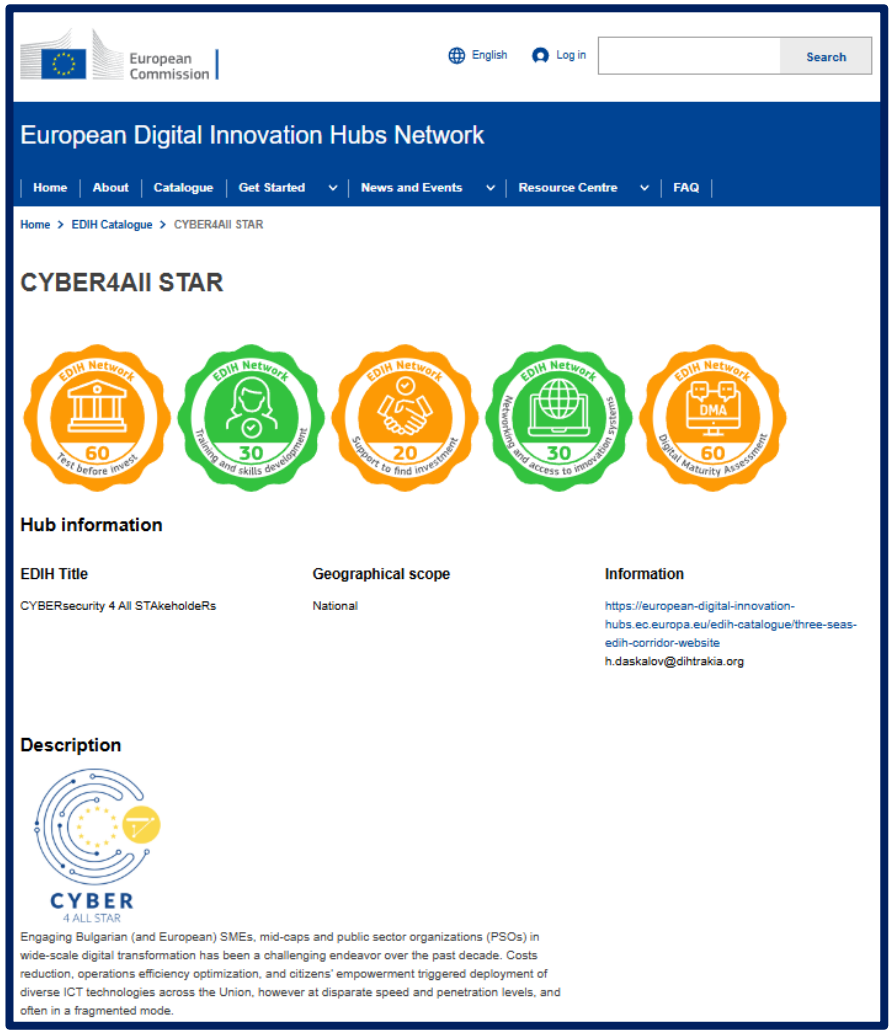
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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

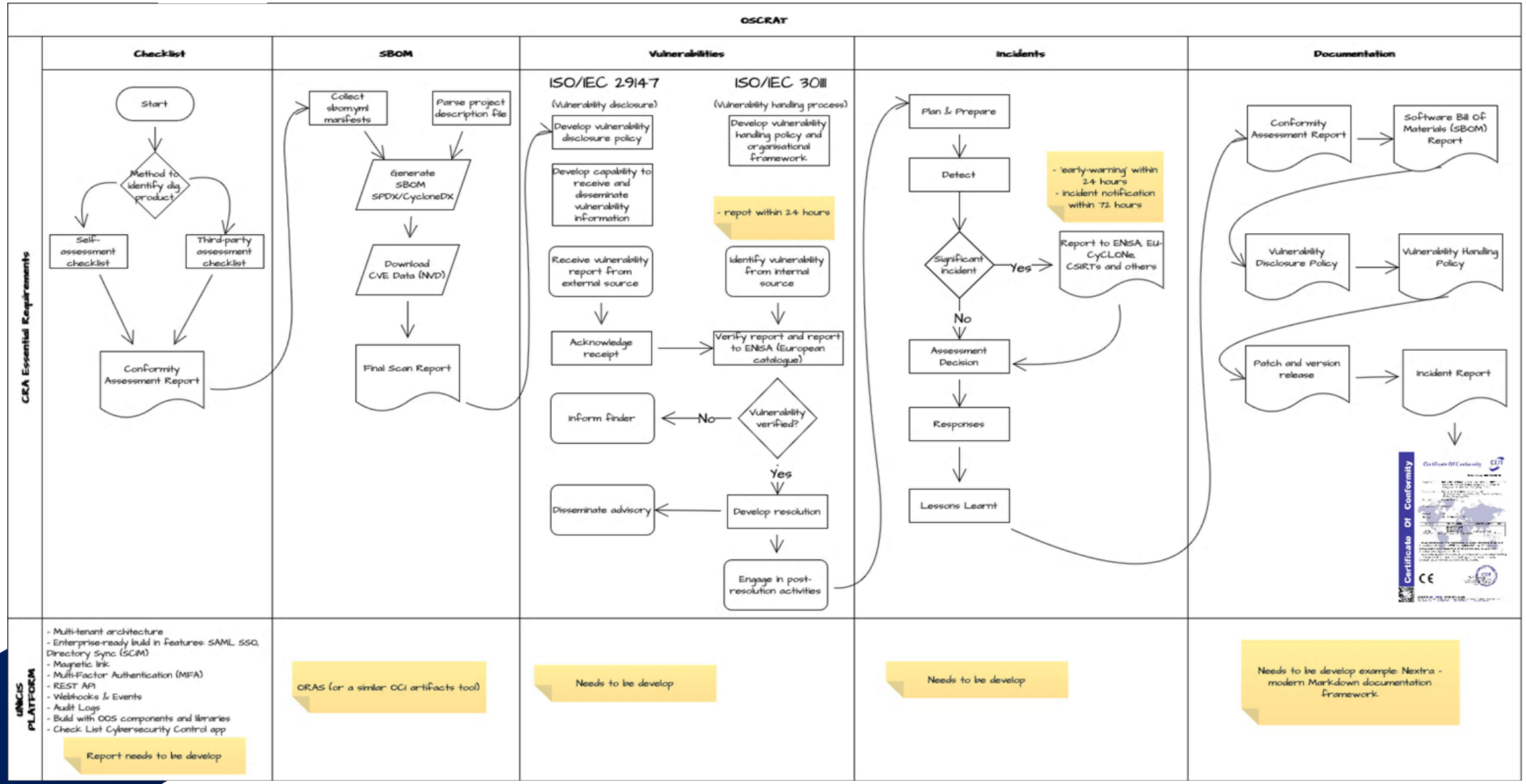
EMAG

Poland

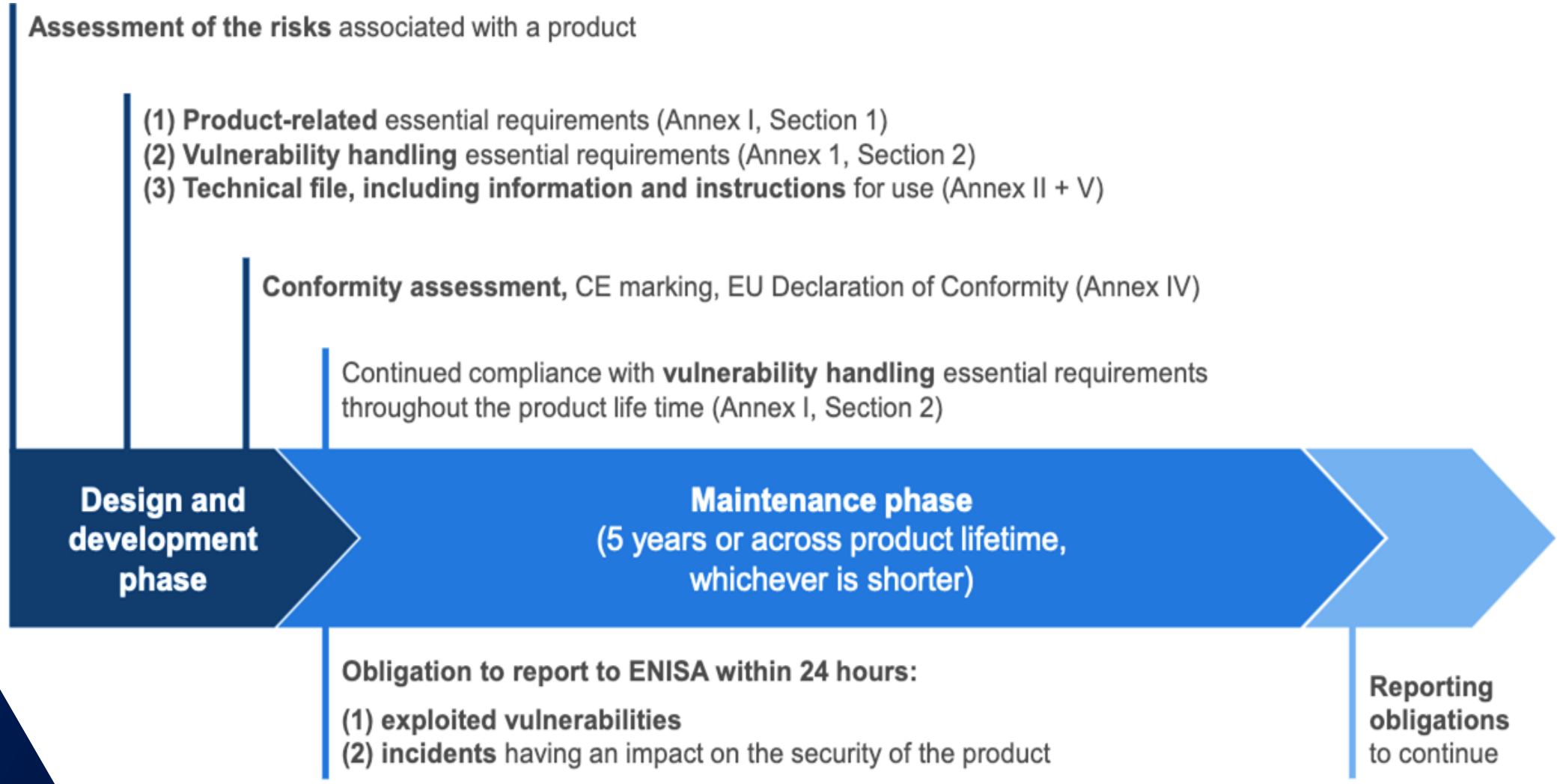
Unicis.Tech OÜ

Estonia

The **OSCRAT Platform**



The **Need Behind OSCRAT**



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:** 08 / 09 / 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 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:** 13 / 10 / 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