Compliance Continuum: Tools Supporting CRA Compliance "CURIUM Project"

Chatzopoulou Argyro

Co-founder, Senior Cybersecurity Policy Advisor, APIROPLUS Solutions

05.05.2025

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The 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 and opinions 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.

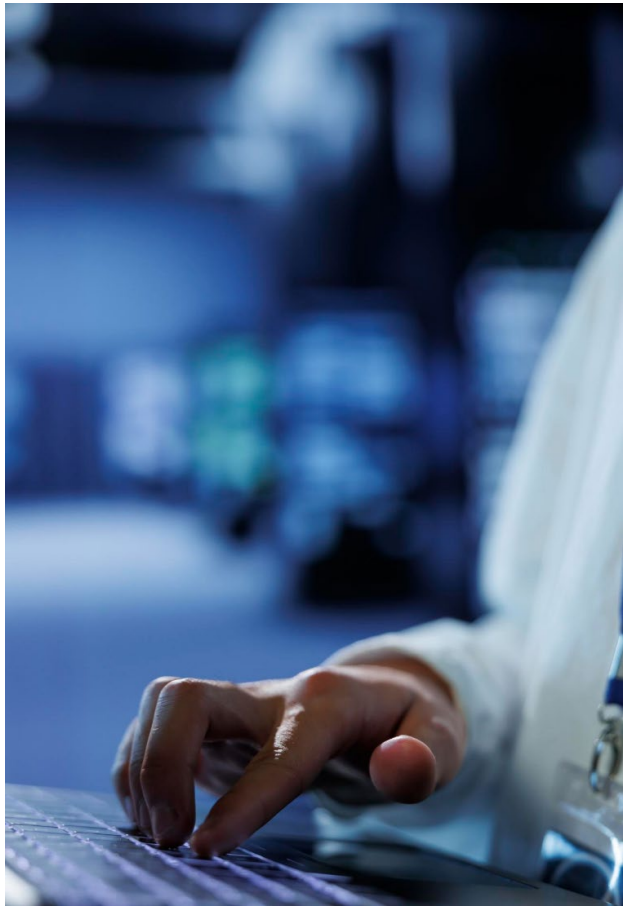
Vision

The CURIUM project envisions a more secure and resilient digital landscape by strengthening the security, privacy, and accountability of hardware and software products with digital elements. At its core, 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.

Objectives

- Developing an innovative **Compliance Continuum** to automate CRA compliance.
- Driving widespread adoption with modular, cost-efficient, and **open-source solutions** tailored to industry needs.
- **Fostering knowledge and capacity building** to support CRA implementation.
- Utilizing an **agile validation process** with continuous feedback loops.
- Fostering **long-term sustainability** by actively engaging industry stakeholders and policymakers in tool development and training.



The consortium

The CRA

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024, on horizontal cybersecurity requirements for **products with digital elements** and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828

= CRA

CRA shall apply from **11 December 2027**.
However, Article 14 (reporting) shall apply from **11 September 2026**
Chapter IV (Articles 35 to 51) (notification) shall apply from 11 June 2026.

The subject

The Regulation lays down:

- (a) rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products;
- (b) essential cybersecurity requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity;
- (c) essential cybersecurity requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the products are expected to be in use, and obligations for economic operators in relation to those processes;
- (d) rules on market surveillance, including monitoring, and enforcement of the rules and requirements.

Products with digital elements

‘**product with digital elements**’ means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately (Article 3, Definitions)

with exceptions and specifics

CyReA

Cyber Resilience Assessment

Identifies whether a product with digital elements **falls within the scope of the CRA** and determines the required conformity assessment process.

Products with digital elements shall be made available on the market only where:

- they **meet the** **essential cybersecurity requirements** set out in Part I of Annex I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed; and
- the **processes put in place by the manufacturer** **comply** with the essential cybersecurity requirements set out in Part II of Annex I.

Products with digital elements

Manufacturers shall undertake **cybersecurity risks assessment**.

Manufacturers shall take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.

The cybersecurity risk assessment shall be **documented and updated.**

DPRA

Digital Product Risk management

Supports manufacturers in **assessing cybersecurity risks** across the product lifecycle to proactively minimize security threats.

Products with digital elements

Manufacturers shall undertake **cybersecurity risks assessment**.

The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.

Digital Product Maturity Assessment

Offers a structured **risk mitigation framework** based on product maturity, helping manufacturers implement effective security measures.

Products with digital elements

Manufacturers of products with digital elements shall:

(1) **identify and document vulnerabilities** and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

(2) in relation to the risks posed to products with digital elements, **address and remediate vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) apply **effective and regular tests and reviews of the security of the product** with digital elements;

(4) once a security update has been made available, **share and publicly disclose information about fixed vulnerabilities**...

Penetration Self-Testing and Vulnerability Assessment

Equips users with tools for **vulnerability assessment, code review, and penetration testing**, reinforcing compliance efforts.

Products with digital elements

Manufacturers shall either provide a **copy of the EU declaration of conformity or a simplified EU declaration of conformity** with the product with digital elements. Where a simplified EU declaration of conformity is provided, it shall contain the exact internet address at which the full EU declaration of conformity can be accessed. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product with digital elements.

Conformity Assessment and Compliance

Provides a guided approach to **technical documentation** and **self-gap analysis**, ensuring alignment with CRA requirements.

Capacity Building

- **Training**: The CURIUM platform will offer tailored training materials and activities, leveraging resources from consortium partners and external sources. The content will cover CURIUM Compliance tools and relevant EU policies.
- **Experimentation & Testing**: CURIUM's partner p-NET will provide cloud-based testing infrastructure for the consortium and external stakeholders, ensuring secure and reliable operations.
- **Consulting & Support**: Consulting services will connect industries and SMEs with relevant expertise, addressing cybersecurity resilience and regulatory compliance in Europe.
- **Awareness & Knowledge Transfer**: CURIUM aims to raise awareness and engage stakeholders across various sectors (government, academia, industry, etc.) to maximize its impact on Europe's economy and society. Activities will promote innovation and public understanding of energy-sustainability technologies. The EU Cybersecurity Skills Academy will be a key partner in training and dissemination efforts. Workshops and information days will be held to support the activity.
- **Collaboration & Sustainability**: Post-project sustainability will be ensured through CURIUM's partner, EIT, which actively participates in multiple European Digital Innovation Hubs. Additionally, collaboration with ENISA, national authorities, and the European Cybersecurity Competence Centre (ECCC) will strengthen Europe's cybersecurity capabilities and foster long-term growth.

Let’s keep in touch!

curium-project

@Curium_Project

curium-project.eu

https://ec.europa.eu/eusurvey/runner/EU_CRA_CURIUM

Thank you!

Chatzopoulou Argyro

Co-founder, Senior Cybersecurity Policy Advisor, APIROPLUS Solutions

ac@apiroplus.solutions