Capacity Building

CURIUM is committed to enhancing cybersecurity across Europe by supporting CRA adoption through:

- **Training:** Tailored materials and activities covering CURIUM tools and EU policies.
- **Experimentation & Testing:** In secure cloud-based testing environments availed for consortium and external stakeholders.
- **Consulting & Support:** Expert consulting services for industries and SMEs on cybersecurity resilience and compliance.
- **Awareness & Knowledge Transfer:** Engaging stakeholders across sectors to maximize impact, with a focus on innovation and public understanding of energy-sustainability technologies. The EU Cybersecurity Skills Academy will play a key role in training and dissemination.
- **Collaboration & Sustainability:** Post-project sustainability will be supported through active collaboration with European Digital Innovation Hubs, ENISA, national authorities, and the European Cybersecurity Competence Centre (ECCC), ensuring continued growth and collaboration across Europe's cybersecurity landscape.

Follow us

curium-project

@Curium_Project

CuriumProject

curium-project.eu

Co-funded by the European Union

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.

CURIUM Project

Transforming Europe into a Trustworthy Certified Digital Valley

Transforming Europe into a Trustworthy Certified Digital Valley

Digital innovation is revolutionizing industries, with advancements like Smart Manufacturing, Industry 4.0, and Digital Twins reshaping business models. However, these developments also bring heightened cybersecurity risks due to increased interconnectivity. To address these challenges, the European Cybersecurity Act (EUCSA) and the Cyber Resilience Act (CRA) create a unified regulatory framework to enhance cybersecurity across ICT products, services, and processes.

Vision

CURIUM envisions a secure, resilient digital environment by strengthening the security, privacy, and accountability of hardware and software with digital elements. The core of CURIUM's approach is the Compliance Continuum, a set of tools and services designed to streamline compliance with the CRA. By simplifying and automating compliance processes, CURIUM empowers European SMEs to conduct self-assessments, prepare for third-party certification, and reduce costs, while accelerating time to market.

Objectives

CURIUM aims to achieve its objectives by:

- 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.

Through these efforts, CURIUM will contribute to a **Trustworthy Certified Digital Valley,** strengthening Europe's cybersecurity ecosystem.

Approach

CURIUM follows a structured methodology to implement the CRA, combining technical innovation with stakeholder engagement.

Stakeholder Engagement: The project involves three key actors ensuring a comprehensive, industry-driven framework for cybersecurity resilience and compliance:

- Standardization & Certification Experts: Ensure alignment with the CRA and EU cybersecurity policies and regulatory frameworks.
- Security Providers: Technology companies and research institutes that collaborate to enhance security tools.
- End Users: SMEs, large industries, critical infrastructure operators, and digital asset developers benefit from CURIUM's tools to assess cybersecurity maturity and mitigate risks.

Compliance Continuum: This integrated framework helps evaluate digital products, considering both individual components and system-wide interconnections. Tailored for SMEs and micro-enterprises, the Compliance Continuum includes:

- Cyber Resilience Assessment (CyReA): Identifies whether a digital product falls under the CRA and the necessary conformity assessment process.
- Digital Product Risk Management (DPRA): Supports manufacturers in assessing cybersecurity risks throughout the product lifecycle.
- Digital Product Maturity Assessment (DPMA): Provides a structured risk mitigation framework based on product maturity.
- Conformity Assessment & Compliance (CAC): Guides technical documentation and self-gap analysis to meet CRA requirements.
- Penetration Self-Testing & Vulnerability Assessment (PSTVA): Equips users with tools for vulnerability assessment, code review, and penetration testing.

By incorporating these services into an agile validation framework, CURIUM continuously improves its tools, ensuring sustainability and effectiveness in enhancing Europe's cybersecurity.