

CURIMUM

ENISA's ECSF Workshop
20-21/11/2025



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.

Implementation of the ECSF

- The project is creating/importing resources and content (training material) to support the services and activities of the CURIUM Compliance Continuum and build capacity and knowledge through experimentation, testing, training, consulting, etc.
- CURIUM has conducted an analysis of the CRA and related requirements. Based on this analysis, it has identified that the implementation of the CRA affects multiple ECSF roles. To create a connection to the CRA, the project team has identified the tasks, has refined them based on the requirements of the CRA and have cross related them to the needed skills, knowledge and e-competencies.
- The project is currently in the phase of preparing the training courses and related material, based on the above mapping. We have designed a template to be linked with the training material, containing Course title, Short description of the course, Learning Objectives, Language of delivery, Delivery mode, Duration, Status, Target audience, ECSF skills & knowledge covered, Type of training , EQF level, Requirements of the CRA covered

Designing and delivering training activities for specific workforce sectors

- The project is currently in the phase of preparing the training courses and related material, based on the explained mapping, while keeping in line with the restrictions imposed by the scope of the project.
- Our sector: Manufacturers of products with digital elements
- Number of individuals trained to date per sector: around 60 people
- Target number of individuals to be trained by the end of 2026 per sector: 500 (the project is ending in June26)

Designing and delivering training activities for specific workforce sectors

- What challenges did you encounter when upskilling professionals in this sector: lack of awareness about the CRA, lack of resources in the SMEs, fragmentation
- What has been the measurable impact of your training on the workforce: this will be measured at the end of the project
- Based on your experience, what three key recommendations would you propose to overcome the challenges: single entry point (CyberSkills Academy), endorsement by local Authorities (in our case, The National Cybersecurity Authority of Greece and the Digital Authority of Cyprus are part of the project partners and are committed in providing access to the tools and training to the stakeholders in both countries)

Designing and delivering horizontal training and education initiatives

- Tools, methods, and approaches used in the training activities: surveys, online training, cloud-based testing infrastructure, consulting services
- Which ECSF profiles are targeted by your training activities? CISO, Cyber Legal, Policy & Compliance Officer, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Implementer, Penetration Tester

Analysis of cyber skills gaps in the workforce

- CURIUM has not performed a cyber skills gap analysis, but has run two different surveys with stakeholders:
 - Through a structured questionnaire provided openly (91 responses collected). It was stated that almost 44% of the respondents have limited or no awareness of the CRA related topics. Only 16% of the respondents claimed to have high knowledge of the CRA.
 - Webinar with around 40 participants. 40% again provided answers that indicated that there is a lack of knowledge on the CRA
- CURIUM activities are mostly focused on the partners' countries: BE, HR, CY, DE, EL, IT, ES

Kind of support	Total Number
Training on the CRA	77 / 91
Technical assistance (for the implementation of relevant security controls)	49 / 91
Policy guidance and legal support	48 / 91
Access to technical and organizational tools to guide you through the requirements	46 / 91
Access to technical and organizational tools to help you implement the requirements	41 / 91
Consulting services	50 / 91
Other	2 / 91

Types of cyber skills certificates

- CURIMUM will only issue certificates of Achievement/Participation

Additional Info

- Contact details: esther.garrido@28digital.eu
- Project's website [here](#)
- List of public deliverables [here](#)
- Some LinkedIn posts with surveys results:

https://www.linkedin.com/posts/curium-project_cra-cybersecurity-activity-7396508481299689473-v3Bi?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAJG_8kBD_QkqOulfNL73VI8-LraWvmMJl0

https://www.linkedin.com/posts/curium-project_cyberresilience-cra-curium-activity-7353052982998921217-oB-W?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAJG_8kBD_QkqOulfNL73VI8-LraWvmMJl0

https://www.linkedin.com/posts/curium-project_cybersecurity-cra-euregulations-activity-7382394725468651520-gTMV?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAJG_8kBD_QkqOulfNL73VI8-LraWvmMJl0

https://www.linkedin.com/posts/curium-project_cyberresilience-cra-digitalproducts-activity-7378413405604487169-BO3T?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAJG_8kBD_QkqOulfNL73VI8-LraWvmMJl0

https://www.linkedin.com/posts/curium-project_cybersecurity-cyberresilienceact-digitalproducts-activity-7316043663707451392-cl5i?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAJG_8kBD_QkqOulfNL73VI8-LraWvmMJl0