



Cra sUppoRt contInuUM

CURIUM Compliance Continuum

final release

Document Summary Information

Grant No	Agreement	101190372	Acronym	CURIUM
Full Title	Cra sUppoRt contInuUM			
Start Date	01.01.2025	Duration	21 months	
Project URL	www.curium-project.eu			
Deliverable	D3.2: CURIUM Compliance Continuum final release			
Work Package	WP3: Development and release of CURIUM Compliance Continuum			
Contractual due date	30/9/2026	Actual submission date	30/9/2026	
Type	DEM	Dissemination Level	PU	
Lead Beneficiary	AEGIS			
Responsible Author	Marinos Tsantekidis			
Contributions from	All Partners			

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
0.1	03/03/2026	5	Initial Table of Contents and assignment of activities and sections to partners	AEGIS
0.2	08/06/2026	55	Executive Summary, Introduction, Chapters 3-7, Abbreviation, ToC	AEGIS
0.3	18/06/2026	60	The key enhancement related to final deployment is added for both CyReA and DPRA	NLG
0.4	31/07/2026	85	All partners contribution to all chapters	All partners
1.0	31/08/2026	90	Final Draft – most of comments are solved, missing input added	AEGIS
1.1	07/09/2026	93	Internal Review	CYS
1.2	21/09/2026	95	Internal Review	SPHYNX
1.3	28/09/2026	100	Quality Assurance and Final Version	AEGIS

Disclaimer

The content of the deliverable is the sole responsibility of the authors and contributors, and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the author(s) or any other participant in the CURIUM consortium make no warranty of any kind with regard to this material including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CURIUM Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CURIUM Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

©CURIUM Consortium, 2025-2026. This Deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Table of Contents

Table of Contents	3
Table of Figures	5
List of Tables	6
1 Executive Summary	7
2 Introduction	8
2.1 Purpose and Scope	8
2.2 Relationship to WP3 Tasks and Overall Project Objectives	8
2.3 Deliverable Structure	9
3 CURIUM Compliance Continuum - Final Architecture and Service	10
3.1 High-Level Overview of the Compliance Continuum	10
3.2 Alignment with Cyber Resilience Act (CRA) Essential Requirements	10
4 Final Release of CURIUM Tools and Services	11
4.1 CURIUM Portal (Landing Page)	11
4.2 Cyber Resilience Assessment (CyReA)	15
4.3 Digital Product Risk Assessment (DPRA)	17
4.4 Digital Product Maturity Assessment (DPMA)	19
4.5 Penetration Self-Testing & Vulnerability Assessment (PSTVA)	20
4.6 Conformity Assessment and Compliance (CAC)	23
5 Final Deployment and Operations	24
5.1 Final Production Environment	24
5.1.1 CURIUM Portal (Landing Page)	26
5.1.2 Cyber Resilience Assessment (CyReA)	27
5.1.3 Digital Product Risk Management (DPRA)	28
5.1.4 Digital Product Maturity Assessment (DPMA)	28
5.1.5 Penetration Self-Testing & Vulnerability Assessment (PSTVA)	29
5.1.6 Conformity Assessment and Compliance (CAC)	30
5.2 Data Management and Privacy	31
6 Feedback-Driven Refinements (AEGIS)	32
6.1 Overview of the Feedback Management Framework	33
6.2 Synthesis of Feedback from WP4 Validation Rounds	33
6.2.1 Riga Validation workshop	33
6.2.2 Nicosia Validation workshop	34
6.2.3 Athens Validation workshop	35
6.2.4 Zagreb Validation workshop	36
6.2.5 Nicosia “Skills” validation workshop	37
6.2.6 BEYOND validation workshop	38
7 Final Capacity Building and Support Outcomes	40

7.1	Cyber Range CRA Training	40
7.2	Capacity Building and Stakeholder Support Activities	42
7.2.1	Training - Capacity Building Workshops and Webinars.....	42
7.2.2	Collaboration and Sustainability	47
7.2.3	CRA Guidance and Knowledge Transfer for Stakeholders	47
7.2.4	Experimentation and Testing.....	47
7.2.5	Consulting and Support Services	48
7.2.6	LinkedIn Awareness Campaign	49
7.3	Evaluation of Capacity Building KPIs.....	51
8	Conclusions (AEGIS)	53

Table of Figures

Figure 1. CURIUM Portal Landing Page	12
Figure 2. CURIUM Portal (“Sign In” page)	12
Figure 3. CURIUM Portal (Registration page)	13
Figure 4. Specialized cybersecurity tools of CURIUM	13
Figure 5. Training feature	14
Figure 6. CURIUM Portal Feedback	15
Figure 7. Breadcrumb Navigation System	15
Figure 8. CyReA look and feel with specific background and organization option	16
Figure 9. Overview of the CyReA	16
Figure 10. Product is within scope of CRA Detailed	17
Figure 11. Class I product Detailed	17
Figure 12. List of active vulnerabilities for a specific asset	18
Figure 13. Threats associated with specific vulnerabilities	18
Figure 14. Each vulnerability level from CVSS3	19
Figure 15. Fully unified, dashboard-driven application	21
Figure 16. Five layers of PSTVA’s architecture	22
Figure 17. Technical documentation and reports	23
Figure 18. Feedback_to_Action Tracker	26

List of Tables

Table 1. Zagreb workshop user feedback loop 27

Table 2. Validation logs for PSTVA from the Feedback-to-Action Tracker 29

Table 3. Key entries to the Feedback-to-Action Tracker 31

Table 4. Evaluation of Capacity Building KPIs #1 51

Table 5. Evaluation of Capacity Building KPIs #2 51

Table 6. Evaluation of Capacity Building KPIs #3 52

1 Executive Summary

Deliverable D3.2 “CURIUM Compliance Continuum final release” presents the final release and consolidation of the CURIUM Compliance Continuum developed within WP3. Building upon the initial releases and activities documented in Deliverable D3.1, this deliverable reports the completion of the technical, operational, and capacity-building activities required to provide an integrated framework supporting the implementation of the Cyber Resilience Act (CRA).

WP3 aimed to define, develop, deploy, refine, and operationalize the components and services of the CURIUM Compliance Continuum, while also delivering the supporting resources necessary for training, knowledge transfer, and capacity building activities. More specifically, WP3 focused on: (i) defining and finalizing the components/modules of the Compliance Continuum and preparing them for validation activities, (ii) integrating and extending the required components and APIs, (iii) building and deploying the technical services and tools of the Continuum, and (iv) implementing the non-technical resources supporting awareness raising, training, and stakeholder support.

The deliverable documents the final outcomes of the following WP3 tasks:

- **T3.1 Adaptations of mature security tools and systems to include in the CURIUM Compliance Continuum**, resulting in the final versions of the core CURIUM services, namely the Cyber Resilience Assessment (CyReA), Digital Product Risk Management (DPRA), Digital Product Maturity Assessment (DPMA), Conformity Assessment and Compliance (CAC), and Penetration Self-Testing and Vulnerability Assessment (PSTVA). The tools have been further refined, aligned with CRA essential requirements, and optimized based on validation feedback and user experience considerations.
- **T3.2 Deployment of CURIUM services and tools to support CRA implementation**, focusing on the final deployment and operationalization of the CURIUM Compliance Continuum, including the final production environment, service integration, release stabilization, and accessibility through the CURIUM Portal.
- **T3.3 Continuous feedback collection and refinements for CURIUM Compliance Continuum**, implementing a structured feedback management process that collected and analyzed validation results and stakeholder feedback from WP4 activities and translated them into concrete technical refinements, usability improvements, and functional enhancements across the Continuum.
- **T3.4 CURIUM support, knowledge and capacity building**, finalizing the project’s training, awareness raising, and stakeholder support activities, including the provision of training resources, user guidance material, and supporting assets to facilitate adoption and long-term use of the CURIUM solutions.

The deliverable provides an overview of the finalized CURIUM Compliance Continuum, including its architecture, deployment status, integrated tools and services, implemented refinements, operational environment, and achieved capacity-building outcomes. It demonstrates how the Continuum provides a practical and modular framework that supports organizations - particularly SMEs and micro-enterprises - in understanding and addressing CRA-related cybersecurity and conformity assessment requirements through integrated assessment, testing, guidance, and compliance support services.

Overall, D3.2 confirms the successful completion and final release of the CURIUM Compliance Continuum and highlights its contribution towards strengthening cybersecurity resilience, regulatory preparedness, and compliance capabilities within the European digital ecosystem.

2 Introduction

2.1 Purpose and Scope

This deliverable, D3.2 “CURIUM Compliance Continuum Final Release”, presents the final release of the CURIUM Compliance Continuum developed under Work Package 3 (WP3) of the CURIUM project. The deliverable documents the finalization, integration, deployment, and refinement of the CURIUM tools and services, as well as the operational and capacity-building activities performed to support their adoption and use.

The purpose of this deliverable is to provide a consolidated overview of the final state of the CURIUM Compliance Continuum, including:

- the finalized architecture and integrated framework of the Continuum,
- the final release of the core CURIUM services and tools,
- the deployment and operational environment of the Continuum,
- the refinements and technical adjustments resulting from validation and stakeholder feedback activities,
- and the final outcomes of the training, support, and capacity-building activities.

The scope of D3.2 covers the complete set of technical and non-technical activities implemented in WP3 to support the project’s objective of providing a modular and practical framework for addressing the requirements of the Cyber Resilience Act (CRA). The deliverable demonstrates how the CURIUM Compliance Continuum supports organizations - particularly SMEs and micro-enterprises - in assessing cybersecurity risks, evaluating product maturity, performing security testing, preparing technical documentation, and facilitating conformity assessment processes.

The deliverable includes the final versions of the five core CURIUM services:

- Cyber Resilience Assessment (CyReA),
- Digital Product Risk Management (DPRA),
- Digital Product Maturity Assessment (DPMA),
- Penetration Self-Testing and Vulnerability Assessment (PSTVA),
- and Conformity Assessment and Compliance (CAC).

In addition, the deliverable presents the final deployment status of the CURIUM Portal, which acts as the unified access point to the Compliance Continuum and supports the orchestration of the individual services and tools.

D3.2 builds upon the activities and intermediate outcomes presented in Deliverable D3.1 and reflects the final operational release of the CURIUM Compliance Continuum following iterative development, validation, feedback collection, and refinement activities performed in collaboration with WP4 and external stakeholders.

2.2 Relationship to WP3 Tasks and Overall Project Objectives

WP3 represents the core implementation and operationalization work package of the CURIUM project, transforming the legal, regulatory, and functional requirements identified in WP2 into concrete tools, services, and supporting resources. D3.2 consolidates the final outcomes of these activities and presents the finalized CURIUM Compliance Continuum following deployment, validation, refinement, and capacity-building activities performed throughout the project lifecycle.

WP3 acts as the bridge between:

- the regulatory and requirements analysis activities of WP2, and
- the real-world validation and assessment activities of WP4.

Through this interaction, the CURIUM Compliance Continuum evolved through iterative releases, validation workshops, stakeholder feedback collection, and continuous refinements, ensuring alignment with both CRA requirements and end-user needs.

The final release documented in this deliverable directly contributes to the achievement of the overall CURIUM project objectives:

- **Objective 1:** Through the implementation of the CURIUM Compliance Continuum and its integrated services supporting cybersecurity assessment, testing, maturity evaluation, and conformity assessment activities aligned with the CRA.
- **Objective 2:** Through the adoption of a modular, flexible, and SME-oriented architecture, leveraging open-source and low-cost technologies where applicable.
- **Objective 3:** Through the delivery of training material, awareness raising activities, guidance resources, and stakeholder support services supporting cybersecurity capacity building and CRA readiness.
- **Objective 4:** Through the implementation of an agile validation and refinement process driven by continuous stakeholder feedback and multiple validation rounds.
- **Objective 5:** Through engagement with industry stakeholders, SMEs, validation participants, and ecosystem actors supporting sustainability and future exploitation of the project results.

Overall, D3.2 demonstrates how WP3 operationalized the strategic vision of the CURIUM project by delivering a practical and integrated Compliance Continuum that supports cybersecurity resilience, regulatory preparedness, and CRA compliance for European organizations, particularly SMEs and micro-enterprises.

2.3 Deliverable Structure

This deliverable documents the final release, deployment, operationalisation, and refinement of the CURIUM Compliance Continuum and its supporting services. It describes how the tools developed throughout the project have been consolidated into a stable and integrated production environment, while also documenting the feedback-driven improvements introduced during the final development cycle.

The deliverable is structured as follows:

- **Section 1** provides the executive summary of the deliverable, highlighting the main achievements of the final release and the transition of the CURIUM Compliance Continuum towards operational deployment.
- **Section 2** introduces the deliverable, maps its contents to the relevant CURIUM Grant Agreement tasks and objectives, and provides an overview of the document structure.
- **Section 3** provides an overview of the final release of the CURIUM Compliance Continuum, summarising the evolution from the previous release towards the final ecosystem and the consolidation of the individual tools and services.
- **Section 4** describes the final release and integration of the CURIUM tools and services, covering the main technical and functional developments implemented across the Compliance Continuum and the integration of the individual components within the CURIUM Portal.
- **Section 5** presents the final deployment and operational environment. It describes the production infrastructure, deployment and maintenance approach, and the final operational status of the CURIUM Portal and the five core tools: CyReA, DPRA, DPMA, PSTVA, and CAC. It also addresses data management, privacy, and security considerations applicable to the operational environment.
- **Section 6** presents the feedback-driven refinement process applied during the final phase of the project. It describes the Feedback Management Framework and synthesises the feedback collected through the WP4 validation rounds, documenting how identified usability, functional, accessibility, and integration requirements were translated into concrete technical refinements and incorporated into the final releases.
- **Section 7** presents the final outcomes of the knowledge and capacity building activities. It describes the training, knowledge-transfer, experimentation, testing, consulting, stakeholder support, and other capacity-building activities implemented during the project, including the CRA Cyber Range training programme and the resources and services made available through the CURIUM ecosystem. The section also evaluates the achievement of the relevant capacity-building KPIs.

Section 8 concludes the deliverable by summarising the overall outcomes of the final CURIUM release, the transition towards an operational and integrated Compliance Continuum, the impact of feedback-driven refinement, and the foundations established for continued use, maintenance, and evolution beyond the project lifetime.

3 CURIUM Compliance Continuum - Final Architecture and Service

3.1 High-Level Overview of the Compliance Continuum

The CURIUM Compliance Continuum constitutes the integrated operational framework developed within the CURIUM project to support organisations in addressing the cybersecurity requirements introduced by the Cyber Resilience Act (CRA). It is designed as a toolchain-based compliance ecosystem that enables structured assessment, continuous risk management, and conformity support for products with digital elements.

The Continuum provides an end-to-end support environment covering the full lifecycle of digital products, from initial CRA scope determination and cybersecurity risk assessment to vulnerability management, conformity assessment preparation, and post-market cybersecurity activities. It is particularly targeted at SMEs and micro-enterprises, offering a modular, accessible, and cost-efficient approach to regulatory readiness and cybersecurity improvement.

The framework is delivered through the CURIUM Portal as a unified access point integrating five core services:

- **Cyber Resilience Assessment (CyReA):** supports CRA scope determination and identifies applicable conformity assessment pathways for products with digital elements
- **Digital Product Risk Management (DPRA):** enables lifecycle-oriented cybersecurity risk assessment and mitigation across product development and maintenance phases
- **Digital Product Maturity Assessment (DPMA):** provides structured evaluation of cybersecurity maturity and readiness against CRA expectations
- **Conformity Assessment and Compliance (CAC):** supports conformity assessment preparation through structured gap analysis, documentation support, and compliance guidance
- **Penetration Self-Testing and Vulnerability Assessment (PSTVA):** provides vulnerability assessment capabilities, including penetration testing and code review support for security validation

These services operate as interoperable components within a modular architecture, allowing organisations to adopt either the full Continuum or individual services depending on their cybersecurity maturity, operational needs, and regulatory context.

The Continuum follows a user-centric and validation-driven development approach, incorporating stakeholder feedback, iterative refinement cycles, and usability improvements throughout the project lifecycle. This includes enhancements in workflow orchestration, reporting consistency, and guidance support, ensuring alignment with real-world SME needs and CRA implementation challenges.

Overall, the CURIUM Compliance Continuum provides a scalable and structured ecosystem that transforms CRA requirements into operational cybersecurity processes, supporting organisations in improving resilience, readiness, and regulatory preparedness across the European digital landscape.

3.2 Alignment with Cyber Resilience Act (CRA) Essential Requirements

The CURIUM Compliance Continuum is structured as a modular platform composed of five independent but conceptually interconnected services accessible through the CURIUM Portal. Each service addresses a specific functional domain of CRA-related cybersecurity and compliance activities, while collectively forming a coherent compliance support framework.

The platform follows a modular architecture approach, where each service operates as a standalone component but is positioned within a unified user journey covering the product cybersecurity lifecycle. Integration between services is primarily logical and workflow-based, rather than based on direct technical coupling.

This design enables flexible adoption, allowing organisations to use individual services or combine multiple services depending on their regulatory needs, cybersecurity maturity, and organisational priorities.

The CRA-aligned coverage provided by the Continuum includes the following key domains:

- CRA scope determination and product classification
- Cybersecurity risk identification and lifecycle risk management
- Cybersecurity maturity assessment and organizational readiness evaluation
- Secure technical documentation and Software Bill of Materials (SBOM) support
- Vulnerability assessment, penetration testing, and security validation
- Conformity assessment preparation and gap analysis
- Post-market cybersecurity monitoring and vulnerability handling
- Security update and lifecycle management support

This coverage is operationalised through a direct functional mapping of CRA requirements to the CURIUM service components:

- CRA scope determination, digital product classification, and conformity assessment process determination (CyReA)
- Cybersecurity risk assessment and lifecycle risk management (DPRA)
- Cybersecurity maturity evaluation and readiness assessment (DPMA)
- Technical documentation, self-gap analysis, and conformity preparation (CAC)
- Security validation, vulnerability assessment, code review, and penetration testing (PSTVA)

The Continuum also integrates cross-cutting CRA support functions, including secure-by-design and secure-by-default principles, coordinated vulnerability disclosure processes, and structured post-market cybersecurity support.

In addition, the Continuum contributes to awareness raising and capacity-building activities aimed at improving CRA readiness, particularly for SMEs and micro-enterprises, by providing structured guidance and practical tools for compliance implementation.

Through this structured mapping and modular architecture, the CURIUM Compliance Continuum supports the operationalisation of CRA requirements into an actionable cybersecurity framework, strengthening organisational resilience and regulatory preparedness across the European digital ecosystem.

The described modular structure reflects the current implementation state of the platform and supports future extensibility of the CURIUM Compliance Continuum.

4 Final Release of CURIUM Tools and Services

4.1 CURIUM Portal (Landing Page)

In strict alignment with the General Data Protection Regulation (GDPR), the portal entry architecture has been upgraded to include a specialized landing page. This page serves a dual purpose: educating users on the overarching objectives of the CRA and providing transparent access to the privacy policy governing the Curium Continuum itself (Figure 1).



FIGURE 1. CURIUM PORTAL LANDING PAGE

The user can then proceed to the compliance portal serving as the primary user entry point, where they have the option to either authenticate themselves to the portal (Figure 2) or register to it (Figure 3).

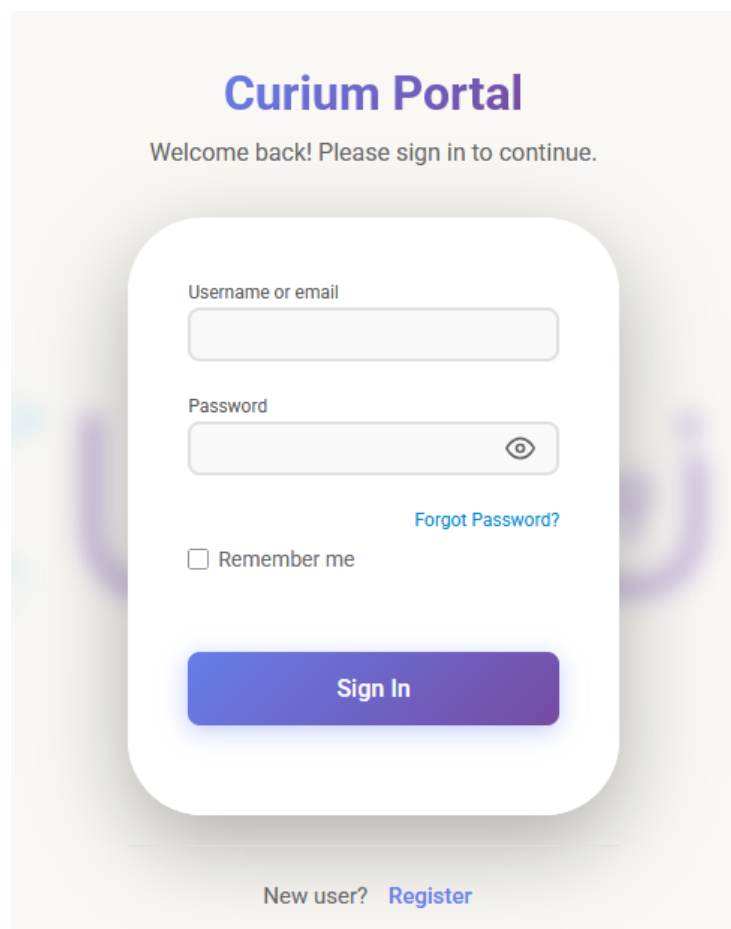
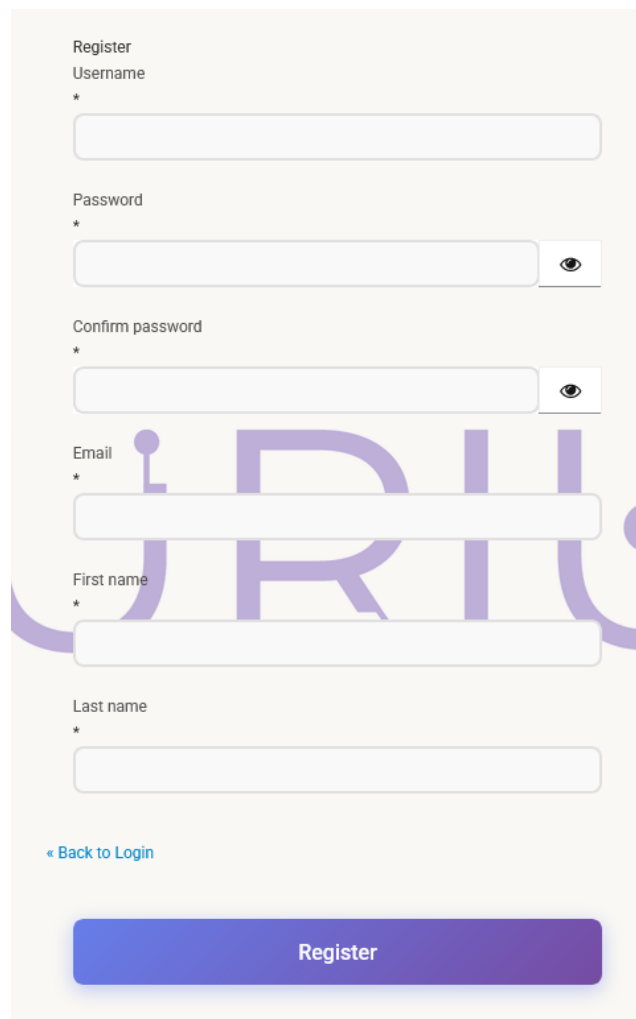


FIGURE 2. CURIUM PORTAL ("SIGN IN" PAGE)



The registration form is titled "Register" and includes the following fields:

- Username**: A text input field with an asterisk (*) indicating it is required.
- Password**: A text input field with an asterisk (*) and a toggle icon (eye) to show or hide the password.
- Confirm password**: A text input field with an asterisk (*) and a toggle icon (eye) to show or hide the password.
- Email**: A text input field with an asterisk (*) indicating it is required.
- First name**: A text input field with an asterisk (*) indicating it is required.
- Last name**: A text input field with an asterisk (*) indicating it is required.

Below the fields, there is a link: [« Back to Login](#). At the bottom, there is a large blue button labeled **Register**.

FIGURE 3. CURIUM PORTAL (REGISTRATION PAGE)

After signing in, the user accesses a curated dashboard presenting five specialized cybersecurity tools of CURIUM project (Figure 4): Cyber Resilience Assessment (CyReA), Digital Product Risk Management (DPRA), Digital Product Maturity Assessment (DPMA), Penetration Self-Testing & Vulnerability Assessment (PSTVA) and Conformity Assessment and Compliance (CAC).

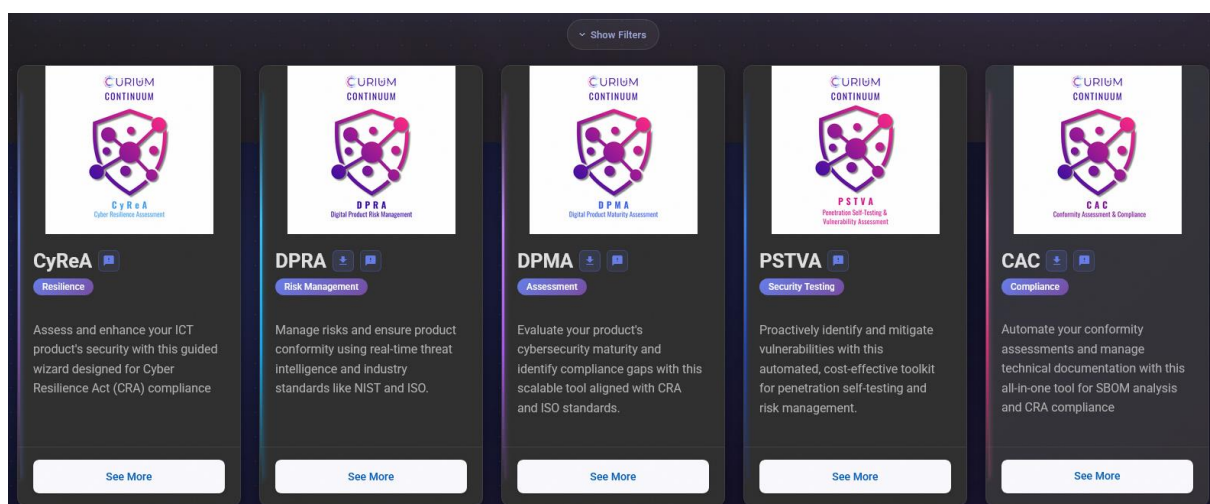


FIGURE 4. SPECIALIZED CYBERSECURITY TOOLS OF CURIUM

Four of these tools (CyReA, DPRA, DPMA, and CAC) operate as independent web services, each accessible via dedicated URLs with seamless redirection upon user selection from the tool list to streamline workflow transitions, facilitated by Single Sign-On (SSO) service that propagate authentication tokens from the portal to downstream services, ensuring frictionless, secure session continuity without redundant logins. The PSTVA toolkit includes a user manual, embedded directly within the portal, providing step-by-step guidance on local installation, utilities, and service startup procedures. Complementing the embedded manual of the PSTVA toolkit, the portal now features dedicated download controls for the remaining integrated services, enabling users to seamlessly download the respective user manuals locally for offline technical reference (Figure 4 – download arrow next to each tool’s name).

Building upon the foundational architecture of the initial release, the Curium Continuum portal has undergone significant functional expansion and regulatory refinement. While the core framework continues to provide centralized, authenticated access to the specialized cybersecurity toolset via streamlined Single Sign-On (SSO) and token propagation, the latest iteration introduces key features designed to enhance user competency, workflow guidance, and legislative compliance.

To baseline and elevate user proficiency regarding the Cyber Resilience Act (CRA), a dedicated training feature has been integrated into the portal (Figure 5). This module features a curated repository of knowledge self-assessment questions powered by the Sphynx Cyber-Range, allowing users to dynamically evaluate and identify their level of understanding regarding critical CRA tenets.

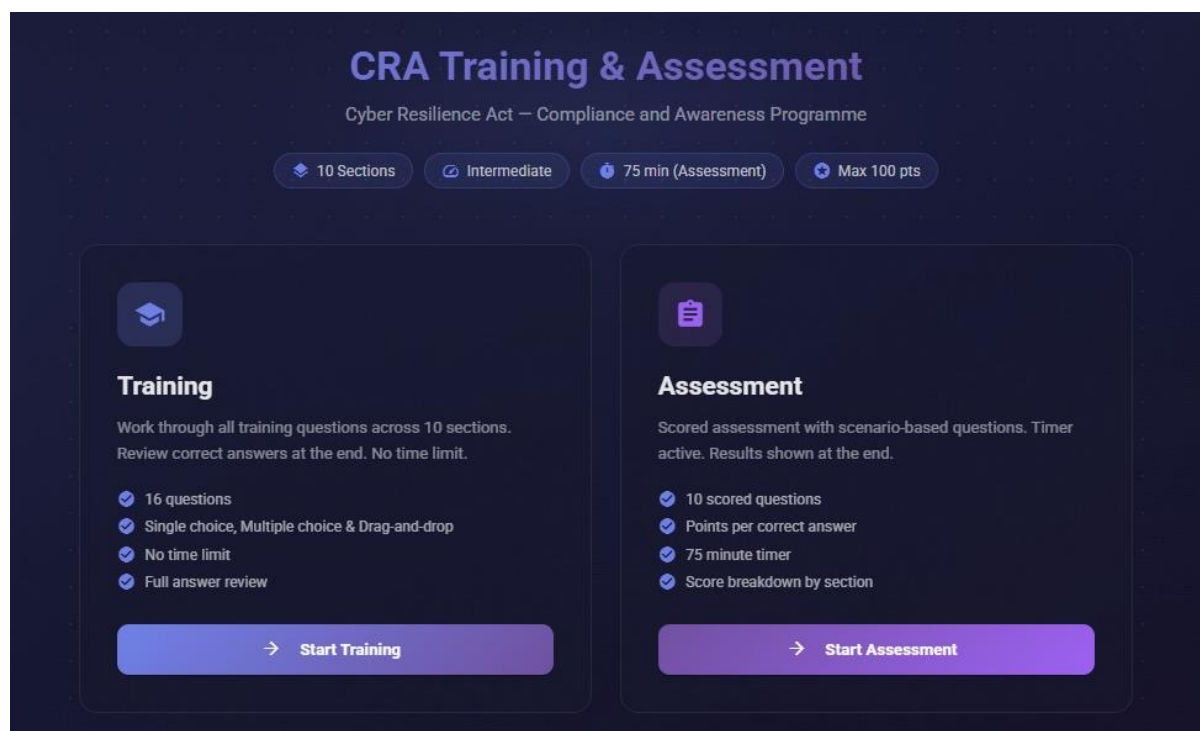


FIGURE 5. TRAINING FEATURE

To facilitate continuous improvement and user engagement, a structured feedback mechanism has been deployed utilizing embedded form architectures (Figure 6). This interface enables users to systematically rate individual tools as well as the overarching portal ecosystem, while empowering stakeholders to submit direct inquiries, propose novel functionalities, and suggest feature enhancements to the development pipeline.

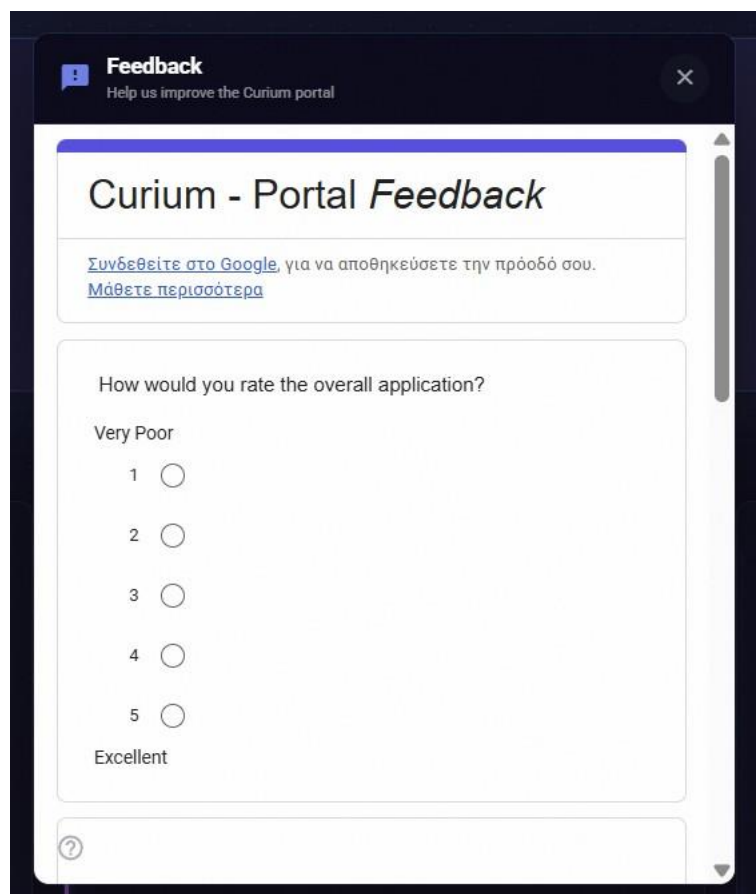
The image shows a feedback form titled "Curium - Portal Feedback" within a dark-themed window. At the top, there's a "Feedback" header with a close button. Below it, a sub-header says "Help us improve the Curium portal". The main content area has a title "Curium - Portal Feedback" and a link to "Συνδεθείτε στο Google" for saving progress. A question asks "How would you rate the overall application?" with a 5-point scale from "Very Poor" to "Excellent". The scale uses radio buttons for each number. A help icon (?) is at the bottom left of the form area.

FIGURE 6. CURIUM PORTAL FEEDBACK

User navigation and operational clarity have also been optimized through the implementation of a visual breadcrumb navigation system (Figure 7). This guide maps sequential workflows, providing users with a clear, step-by-step visual trajectory to ensure compliance with CRA requirements through the Curium Continuum framework.



FIGURE 7. BREADCRUMB NAVIGATION SYSTEM

4.2 Cyber Resilience Assessment (CyReA)

CyReA is developed to help stakeholders involved with ICT products determine whether the product is within the scope of CRA. This assessment service enables key actors — such as manufacturers, importers, distributors, authorized representatives, and owners—to systematically verify that their products with digital elements are within the scope of CRA and requires specific level of assessment.

The tool has been finalized and updated to ensure full readiness for deployment, with enhancements focused on creation of questionnaires in a dynamic manner and documentation with database scheme. Specifically, these improvements include the implementation of dynamically generated questionnaires to support flexible and scalable assessments for the scope determination, comprehensive documentation supported by a well-defined database schema, and the integration of a Single Sign-On (SSO) mechanism of CURIUM to ensure secure and seamless user access. Moreover, a detailed guideline is also incorporated to support the users' understanding and link with the CRA. These extensions have been thoroughly tested and validated, resulting in a user-friendly solution ready for deployment in supporting CRA compliance activities for ICT products. Initially, the last version allows users to choose a specific organization they have belonged to and look and feel with specific background as shown in Figure 8.

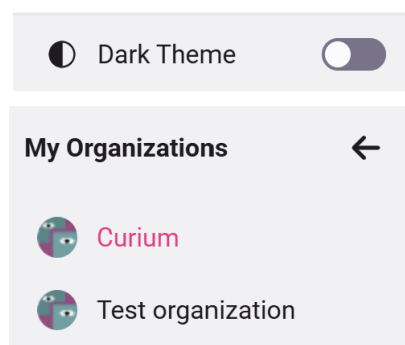


FIGURE 8. CyReA LOOK AND FEEL WITH SPECIFIC BACKGROUND AND ORGANIZATION OPTION

CyReA also provides an overview of how the scope is determined by this tool with definition of product with digital element as stated in Figure 9.

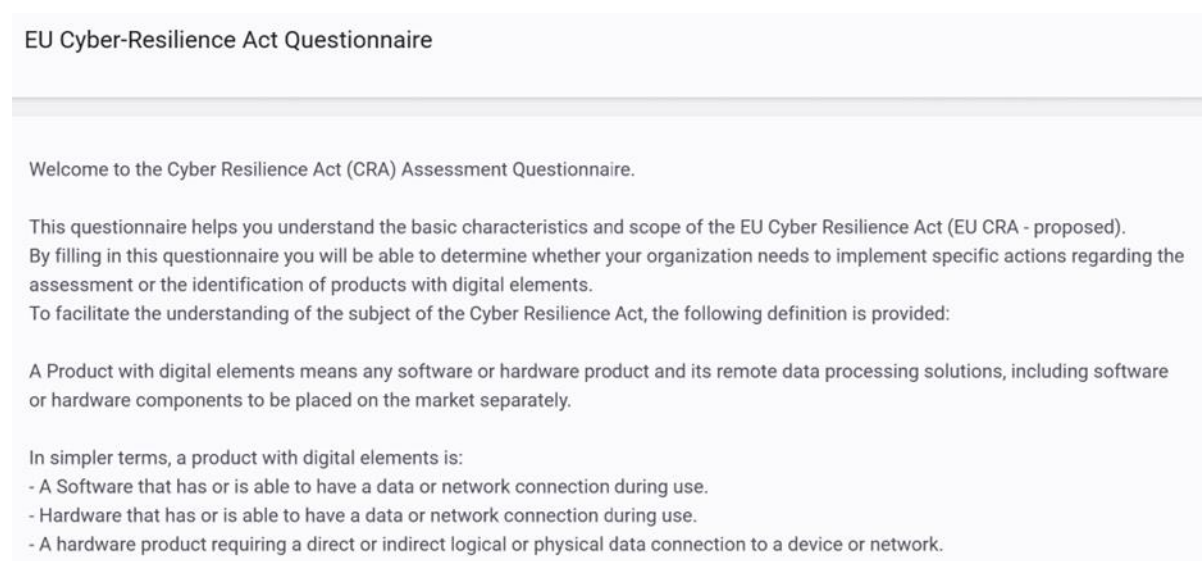


FIGURE 9. OVERVIEW OF THE CyReA

As a part of the final release, a detailed guideline is provided at each phase when the users provide their response. For example, once the product is determined within the scope of CRA, the following outcome is provided and links with Article 17 of CRA as shown in Figure 10 and detailed about product with class I as shown in Figure 11.

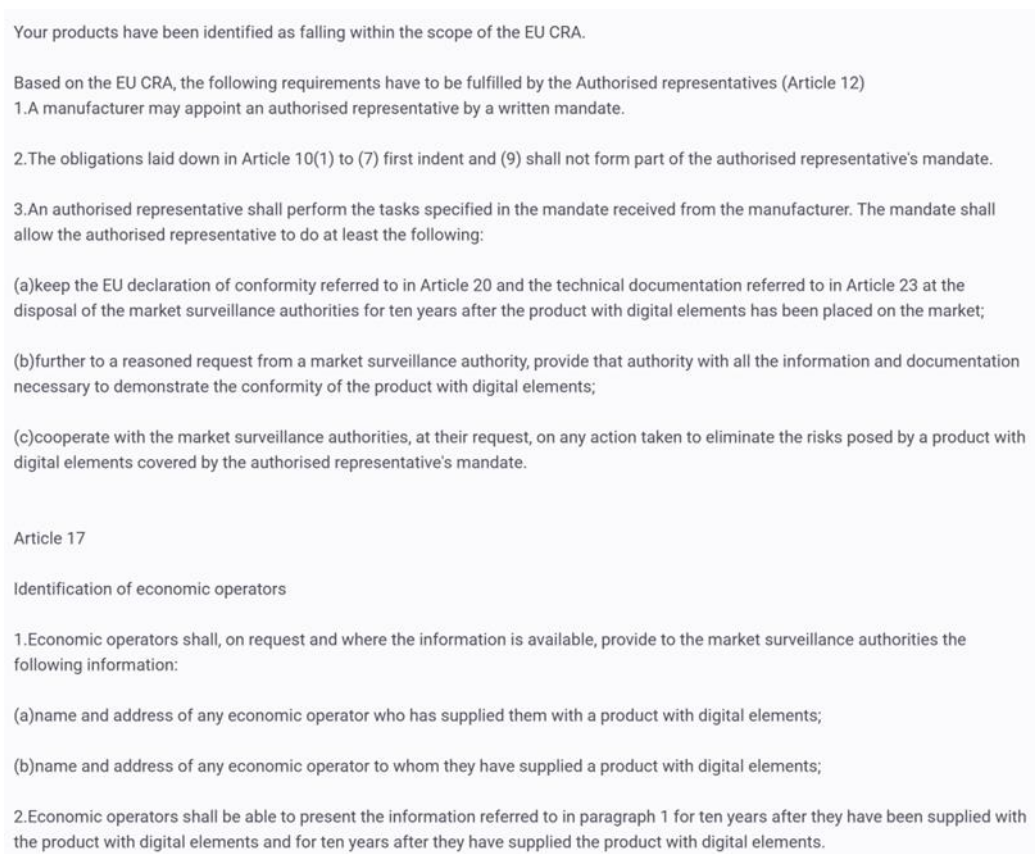


FIGURE 10. PRODUCT IS WITHIN SCOPE OF CRA DETAILED

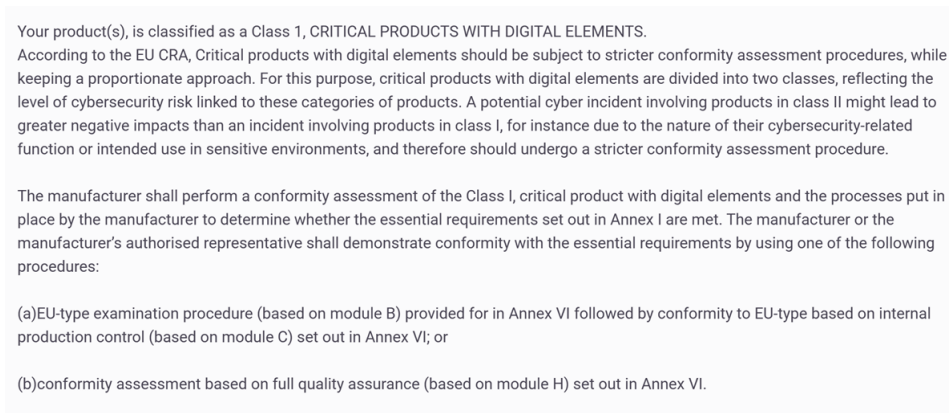


FIGURE 11. CLASS I PRODUCT DETAILED

4.3 Digital Product Risk Assessment (DPRA)

The final release of the Digital Product Risk Assessment (DPRA) provides enhanced capabilities for risk calculation, significantly improving the accuracy and effectiveness of cyber risk evaluation. Building on its evidence-driven and systematic approach, the updated tool now incorporates up-to-date vulnerability score, threat level, enabling more precise estimation of risks across ICT products and organizational infrastructures. The optimization of risk calculations ensures more reliable prioritization of threats and vulnerabilities, aligned with international cybersecurity standards such as NIST 800-53 and ISO/IEC 15408, supporting a unified and robust security evaluation framework. For instance, each asset is linked with active vulnerabilities as shown in Figure 12 and each vulnerability is specified with the related threat as shown in Figure 13.

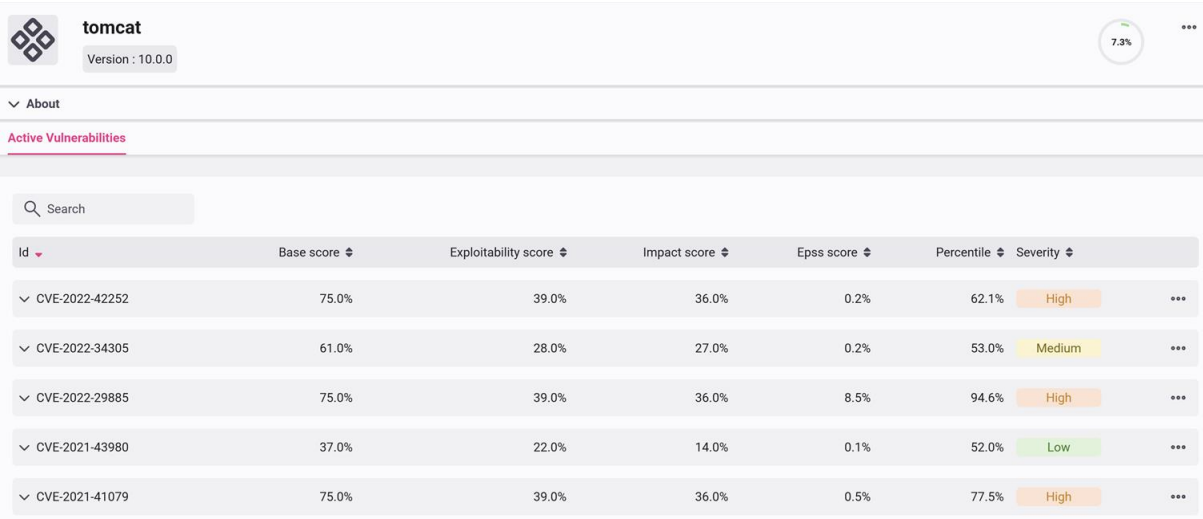


FIGURE 12. LIST OF ACTIVE VULNERABILITIES FOR A SPECIFIC ASSET



FIGURE 13. THREATS ASSOCIATED WITH SPECIFIC VULNERABILITIES

In addition, the DPRA now supports a more dynamic assessment of risk by considering the real-time contextual vulnerability scores from CVSS3. This enables continuous and adaptive risk assessment, allowing organizations to evaluate how previously occurred incidents influence current risk profiles. The introduction of dynamic risk assessment capabilities ensures that risks are not only assessed periodically but also continuously updated based on evolving security landscapes and operational conditions. These enhancements provide stakeholders with a more comprehensive, proactive, and resilient approach to managing cyber risks in products with digital elements. As shown in Figure 14, each vulnerability level is updated based on the values from CVSS3 about base, temporal and environment scores to support accurate calculation of risk.

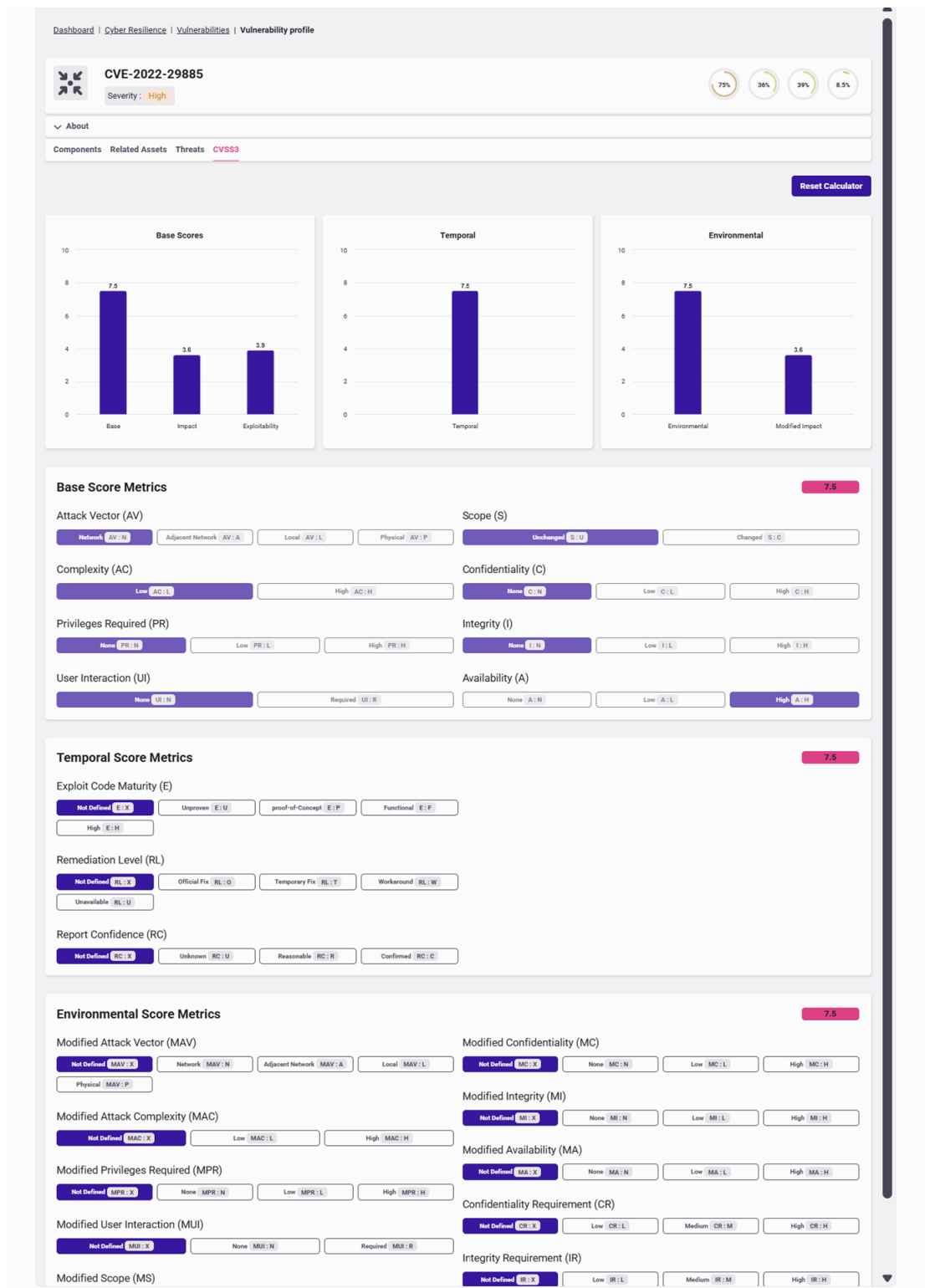


FIGURE 14. EACH VULNERABILITY LEVEL FROM CVSS3

4.4 Digital Product Maturity Assessment (DPMA)

The Digital Product Maturity Assessment (DPMA) Tool is a web-based application that helps organizations, especially SMEs, micro-enterprises, start-ups, product managers, and technical leads, make sense of the increasingly complex cybersecurity requirements landscape for digital products.

With the growing regulatory pressure (notably from the Cyber Resilience Act) and widespread adoption of standards such as ISO/IEC 27001, ISO 27002, NIST SP 800-53 and CIS Controls v8, many organizations are finding it difficult to determine which measures apply to them and how to prioritise them. The DPMA tool addresses this issue by consolidating cybersecurity requirements and recommendations from numerous established standards and frameworks into a single, navigable format that supports an organisation's broader risk management process.

A significant change in the final version is the authentication mechanism. Rather than logging in independently, users now access the DPMA tool via the Curium platform's Single Sign-On (SSO) feature (Figure 2). This integrates the DPMA Tool into the Curium ecosystem, meaning users only need to authenticate once with their Curium credentials to access the tool, providing a unified and more secure experience while leaving all of the tool's functionality unchanged.

The final version was updated using a Retrieval-Augmented Generation (RAG) platform, which was taken as a service from a third party. It was then configured and adapted to the specific needs of APIROPLUS SERVICE Ltd. and the DPMA tool within the CURIUM project. Although the platform is hosted by a third party, it operates as a closed environment: it runs on local LLMs only, does not make any external API calls and has no internet access for retrieving information. It only processes the content that has been uploaded to it and is based on a set of standards and framework documents. The uploaded documentation covers ISO/IEC 27001 (2013 and 2022), ISO/IEC 27002 (2013 and 2022), ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27007, ISO/IEC 27008, ISO 19011, ISO 31000, CIS Critical Security Controls v8, NIST SP 800-53 (Rev. 5), NIST SP 800-160 (Vol. 1, Rev. 1), SAFECode's 'Defining Risks and Responsibilities for Securing Software in the Global Supply Chain', ISACA's Information Security Management Audit/Assurance Programme and ENISA's Technical Guidelines for the implementation of minimum security measures for Digital Service Providers.

The RAG platform is not embedded in the DPMA tool, it is a separate app (platform) used for preparing datasets rather than a feature exposed to end users. It is data quality focused, designed to review all entries and identify measures with a common description so that duplicate entries describing the same control in the same way can be consolidated. This reduces redundancy in the dataset and ensures that each control is represented consistently, thereby improving the clarity and reliability of the tool's search results and exports.

4.5 Penetration Self-Testing & Vulnerability Assessment (PSTVA)

The PSTVA (Penetration Self-Testing and Vulnerability Assessment) toolkit is engineered as an extensible, on-premises, microservices-driven platform, PSTVA orchestrates network and web security scans while centralizing vulnerability intelligence within a graph-native database.

The final release marks the transition from an API or CLI-dependent utility to a fully unified, dashboard-driven application (Figure 15). Crucially, the standardized output structure and comprehensive reporting engine of PSTVA have been tailored to directly satisfy the technical documentation requirements outlined in Article 31 of ANNEX VII, establishing an objective, reproducible testing process for organizational compliance.

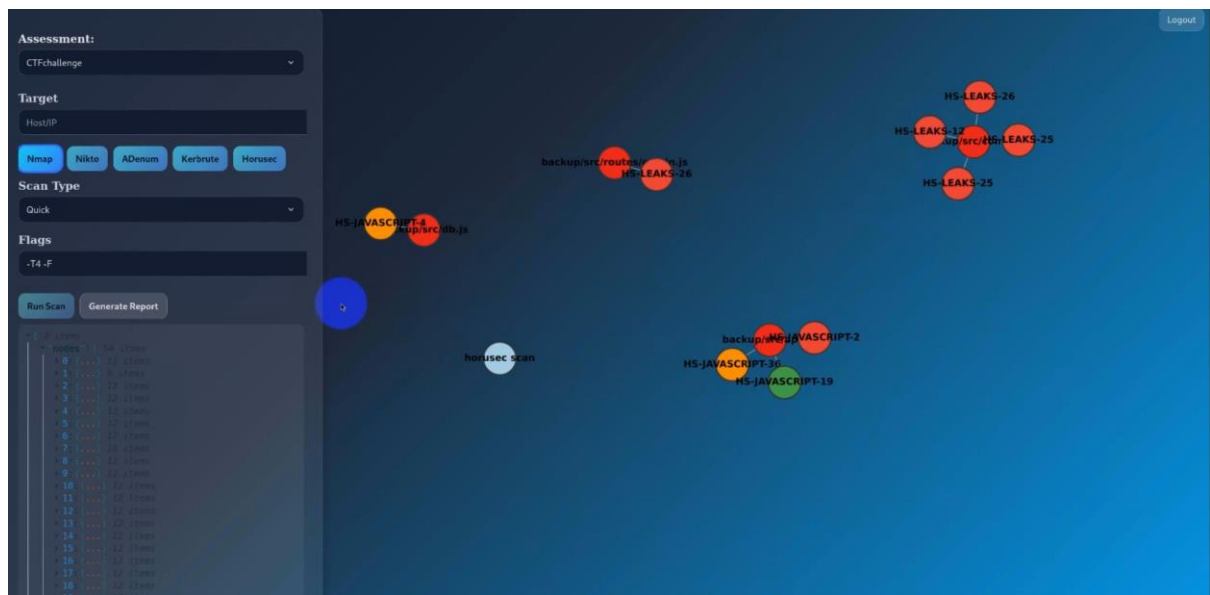


FIGURE 15. FULLY UNIFIED, DASHBOARD-DRIVEN APPLICATION

PSTVA's final release deploys as a fully containerized, zero-dependency microservices architecture managed through Docker. The architecture operates across five distinct layers (Figure 16):

- **Client Layer:** A centralized web dashboard that handles project lifecycle management, tool execution, and visual data exploration.
- **API Layer:** Built on FastAPI, managing input sanitization, rapid request routing, and dynamic OpenAPI/Swagger documentation.
- **Security Layer:** Implements Role-Based Access Control (RBAC) enforced through secure JSON Web Tokens (JWT) and API key validation.
- **Task Layer:** Utilizes a producer-consumer pattern via Celery and Redis to execute concurrent, asynchronous workloads across optimized, isolated Docker containers.
- **Data Layer:** Powered by a Neo4j graph database that models' security posture by linking assets, services, and vulnerabilities via a formalized cybersecurity ontology.

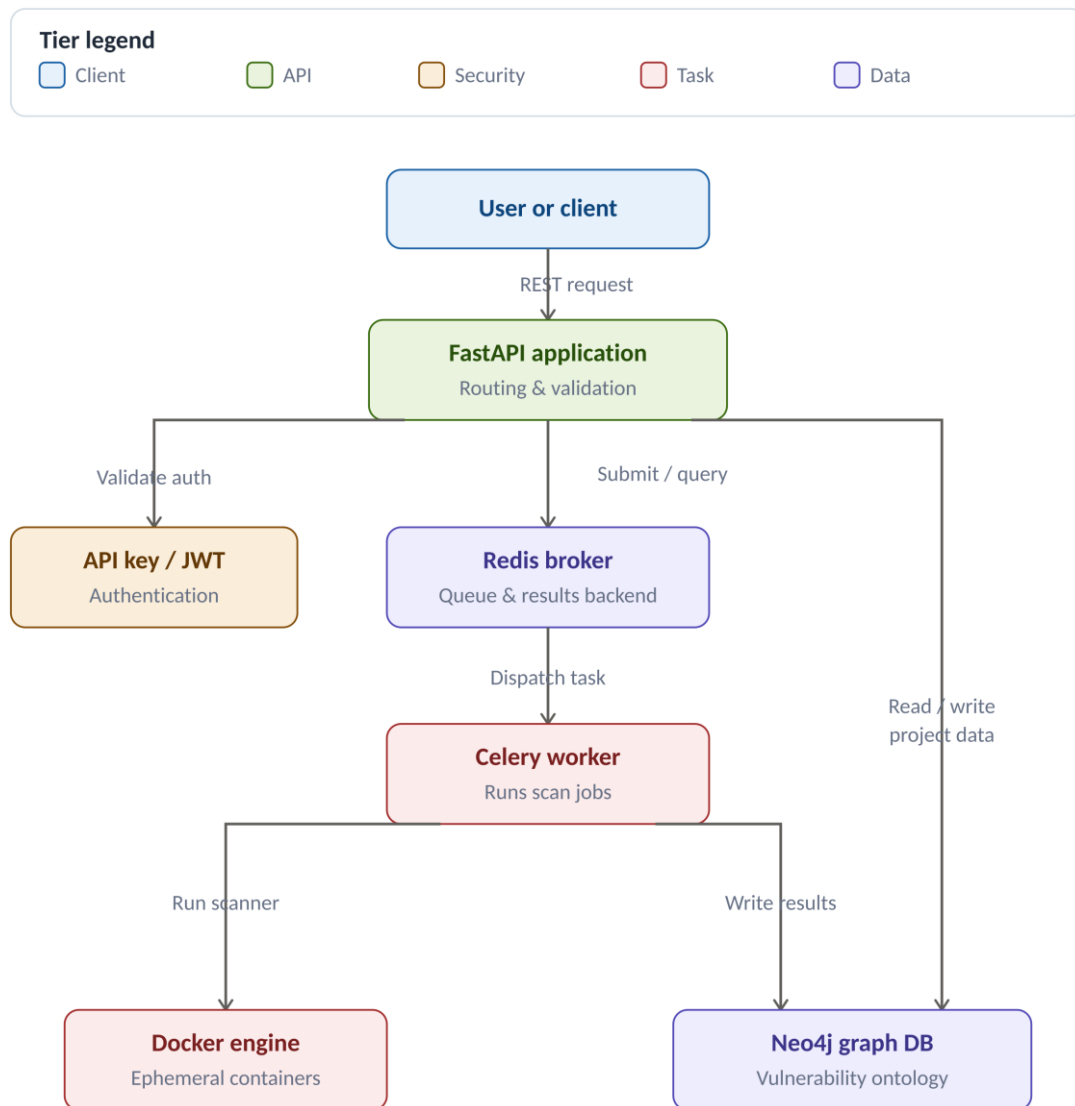


FIGURE 16. FIVE LAYERS OF PSTVA'S ARCHITECTURE

The production toolkit unifies five trusted open-source utilities directly into the centralized user interface, segmented by tactical application:

Infrastructure & Network Security

- Nmap: Executes high-speed host discovery, port scanning, and service fingerprinting across target subnets.
- ADEnum & Kerbrute: Handles Active Directory for reconnaissance, mapping out users, groups, and assets while conducting safe Kerberos account enumeration to expose privilege flaws.

Web Application Security

- Nikto: Scans target web servers for dangerous files, misconfigurations, outdated server software, and software vulnerabilities.

Static Application Security Testing (SAST)

- Horusec: Analyzes source code repositories directly through the pipeline to catch security vulnerabilities, hardcoded secrets, and compliance flaws prior to deployment.

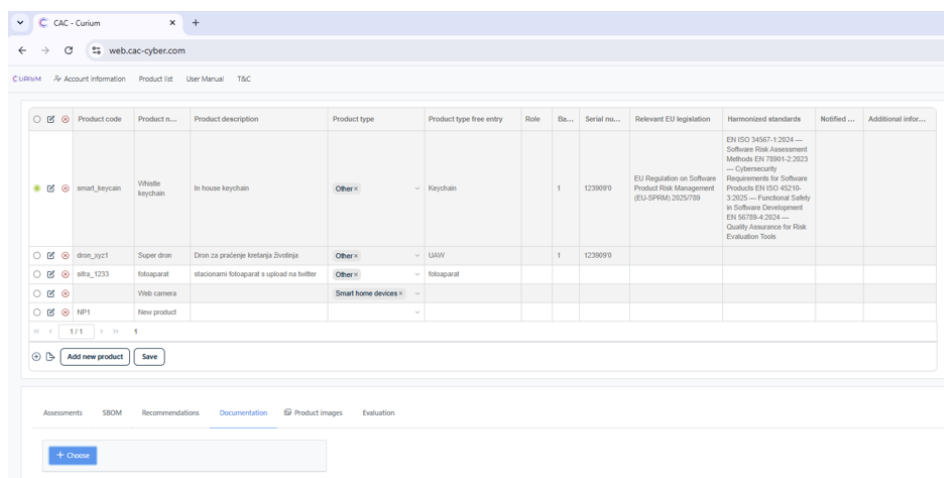
User Workflow

The operational workflow within the PSTVA dashboard follows a seamless, data-driven cycle designed to take an engineer from initial authentication to compliance-ready reporting:

1. **Authenticate & Access:** The user signs into the secure dashboard via JWT-authenticated credentials or API keys, granting scoped access based on their RBAC profile.
2. **Establish Project Scope:** Users define a project workspace to encapsulate related assets, compliance boundaries, and target scopes.
3. **Select UI Tooling:** The operator selects the required tool directly from the graphical interface—ranging from rapid network mapping (Nmap) to code scanning (Horusec) or directory fuzzing.
4. **Configure Parameters:** Target scopes, ports, and scan profiles are customized with built-in parameter validation before being pushed to the distributed Redis broker queue.
5. **Monitor via Celery Tab:** The dashboard provides real-time tracking of asynchronous task states, worker performance metrics, and `stdout` logs parsed on the fly.
6. **Explore the Smart Graph:** Upon completion, the normalized results are written to Neo4j. Users can visually traverse structural dependencies, viewing how a single vulnerability maps across multi-hop asset connections.
7. **Generate Enriched Report:** Automated reporting compiles findings into heavily structured JSON or polished PDF formats. These reports highlight prioritized remediation roadmaps (patches, secure configurations) and use schemas engineered for easy ingestion by Large Language Models (LLMs).
8. **Verify Regulatory Compliance:** Organizations audit the finalized PDF reports and CVE/CWE data to satisfy technical testing audit requirements, explicitly closing out compliance obligations under Article 31 of ANNEX VII.

4.6 Conformity Assessment and Compliance (CAC)

The Conformity Assessment and Compliance (CAC) tool has transitioned from its iterative development phase (v0.9, TRL 6) to a stable, production-ready module (v1.2) within the CURIUM Compliance Continuum. As of June 2026, the service has reached Technology Readiness Level (TRL) 7-8, indicating it is fully operational in a web-based environment and has been rigorously demonstrated through real-world validation. The tool serves as the final step in the CURIUM journey, transforming technical evidence into mandatory CE marking documentation (Figure 17).



The screenshot displays the 'CAC - Curium' web application. The main area features a table with columns: Product code, Product n..., Product description, Product type, Product type free entry, Role, Ba..., Serial no..., Relevant EU legislation, Harmonized standards, Notified ..., and Additional info... The table contains four rows of data, including products like 'smart_keychain', 'dron_vy1', 'sifa_1233', and 'NP1'. Below the table are buttons for 'Add new product' and 'Save'. On the left, a sidebar contains navigation links: Assessments, SBOM, Recommendations, Documentation (active), Product images, and Evaluation. At the bottom of the sidebar is a '+ Upload' button.

FIGURE 17. TECHNICAL DOCUMENTATION AND REPORTS

The development team focused on production hardening and resolving usability barriers identified during validation workshops in Athens (March 2026) and Zagreb (April 2026).

Key achievements include:

- **Unified SSO & IAM Integration:** We resolved initial access friction by integrating a centralized Identity and Access Management (IAM) layer, allowing users to transition seamlessly between the CURIUM Portal and the CAC tool without redundant logins.
- **Mobile Responsiveness:** Based on feedback from the Zagreb workshop, we enabled responsive frontend library features to ensure the tool renders effectively on tablets.
- **Contextual Regulatory Guidance:** To assist non-expert users, we introduced contextual help texts and tooltips linked directly to CRA Annex VII provisions, explaining why specific documentation artifacts are required (FDBK-001).
- **UI/UX Refinements:** Following the Athens workshop, where users reported difficulty navigating instructions, we relocated the User Manual and Terms & Conditions to the top-level menu for persistent visibility (FDBK-008).
- **Post-Market Monitoring Activation:** We finalized the implementation of the post-market analysis capability, which provides automated alerts to SMEs regarding new vulnerabilities or regulatory updates affecting their products already on the market.

CAC - User Interaction Flow

The operational user flow of the CAC application is designed to guide an SME manufacturer through a structured trajectory from initial product registration to the generation of a legally required EU Declaration of Conformity (DoC):

- **Authentication & Entry:** Users access the tool via the CURIUM Portal using Single Sign-On (SSO).
- **Product Onboarding:** By selecting "Add new product," the user completes a form for mandatory metadata, including product code, type, class, and relevant EU legislation.
- **Automated Self-Assessment:** The user completes a questionnaire wizard covering cybersecurity requirements. The system automatically calculates a KPI score (e.g., "Excellent," "Good"). Users can manually override results if a documented justification is provided for transparency.
- **Technical Documentation Management:** The user uploads required evidence of artifacts—as defined in CRA Annex VII—into a centralized workspace. This includes design information, vulnerability management plans, and user instructions.
- **SBOM Import and Analysis:** Users import a Software Bill of Materials (SBOM) into SPDX 2.3 format. The CAC tool automatically triggers a file evaluation to identify third-party components and highlight known vulnerabilities.
- **Gap Analysis & Recommendations:** The Recommendations tab aggregates gaps identified from the questionnaire and SBOM analysis. The user must select an action for every recommendation (e.g., "Implemented," "Acknowledged," or "Deferred") to satisfy compliance.
- **Final Evaluation & DoC Generation:** Once all steps—Assessment, Recommendations, and Documentation—are marked as "Passed," the user initiates the final check. Upon success, the tool automatically generates the EU Declaration of Conformity template, incorporating the company's logo and signature stored in the profile.

This structured flow ensures that SMEs can manage the complete CE marking documentation process accurately (target ≥98%) without requiring deep external legal expertise.

5 Final Deployment and Operations

5.1 Final Production Environment

The final deployment and operations phase represent the transition of the CURIUM Compliance Continuum from an iterative development framework to a fully operational, stable ecosystem (v1.2). This stage ensures that the

suite of tools is hardened for production use, enabling European micro-enterprises and SMEs to meet the mandatory requirements of the Cyber Resilience Act (CRA) through a unified and reliable infrastructure.

The CURIUM final production environment is established as a centralized, hardened infrastructure designed for high availability and session continuity. The architecture utilizes containerization (Docker/Kubernetes) to ensure that individual services are modular, scalable, and can be maintained independently without disrupting the overall compliance journey.

To maintain the resilience and regulatory alignment of the production environment, CURIUM employs a DevOps-driven update strategy:

- **CI/CD Pipeline:** Automated builds, testing, and deployment are managed through GitLab CI/CD, ensuring rapid iteration and security patching.
- **Service Disruption Mitigation:** Containerized services allow for regular release cycles and the deployment of new features or bug fixes without interrupting active SME compliance sessions.
- **Regulatory Updates:** The tools are maintained against a traceability matrix, ensuring technical checks are updated as new harmonized standards, or delegated acts emerge from European policymakers.

The Feedback-to-Action Tracker (Figure 18) is a central, shared repository and the primary tool for implementing the CURIUM project's Feedback Management Framework. It serves as the critical link between the validation activities in Work Package 4 (WP4) and the technical development in Work Package 3 (WP3), ensuring that the Compliance Continuum is user-driven and continuously refined based on real-world SME testing.

Description of the Feedback-to-Action Tracker

The tracker provides a transparent and traceable log for all stakeholder input collected through validation workshops, hands-on sessions, and online surveys. It systematically captures, analyses, and prioritizes feedback to convert qualitative insights into actionable technical tasks.

The tracker is structured with several key fields to ensure comprehensive management, among which are:

- **Feedback ID:** A unique code (e.g., FDBK-001) for referencing specific items.
- **CURIUM Component:** Identifies the specific tool (CAC, CyReA, etc.) or resource (User Manual, Portal) the feedback applies to.
- **Categorization:** Classifies inputs into types such as Usability, Functionality, Performance, or Documentation.
- **Priority:** Determines the urgency (High, Medium, Low) based on criticality to compliance goals and technical feasibility.
- **Target Release:** Specifies the planned version (e.g., v1.1, v1.2, or "Hot Fix") in which the resolution will be deployed.

Feedback ID (Unique Identifier)	Date Reported (The date of the release update)	Source (The stakeholder that generated the feedback)	Stakeholder Group (The type of user e.g. Dev, Consultant, etc.)	CURIUM Component (The specific tool the feedback applies to)	Feedback Summary (A short summary of the feedback)	Feedback Category (The type of feedback e.g. Usability, Performance, Usability, etc.)	Priority (The severity of the feedback e.g. Low, High)	Action Type (The nature of the action e.g. Documentation Change, Technical Refinement, etc.)	Assigned To (Developer/Partner)	Action Description (A short description of the action)	Status (The current status of the action e.g. Done, In Progress, Cancelled)	Target Release (The release to which the feedback is planned)	Resolution Notes (A brief note on how the feedback was addressed)
FDBK-004	23/01/23	Internal Workshop	Consultant	PSTVA	Scan code written in the user manual	Functionality	Low	Technical Refinement	ADDS	Add corresponding functionality to PSTVA service, for the programming language	In Progress	v1.2 (Mar 2023)	
FDBK-005	23/01/23	SEC Forum 2023	Dev	CyReA Portal	Redirection to CyReA is working but the user has to sign again	Usability	High	Technical Refinement	ADDS/TLG	Check CURIUM Portal and CyReA connection flow	Done	Hot Fix	ADDS and TLG collaborated to identify the bug and fix it
FDBK-006	23/01/23	SEC Forum 2023	N/A	DPMA	Documentation: Operational Search input the UI is not clear when using the search	Documentation	Low	Documentation update	ADDS/DPMA	Update the DPMA User Manual	Done	v1.2 (Mar 2023)	Reviewed if the improvements that weren't aligned with the current state, aligned with new state
FDBK-007	23/01/2023	Technical Forum 2023		CAC	Why specific documentation artifacts are required	Functionality	Medium	Technical Refinement	CIS	Introduction of contextual help texts and tooltips			
FDBK-008	23/01/2023	Technical Forum 2023		CAC	How guidelines are created and validated	Functionality	Medium	Technical Refinement	CIS	Introduction of contextual help texts and tooltips			
FDBK-009	23/01/2023	Technical Forum 2023		CAC	How assessment results translate into compliance measures	Functionality	Medium	Technical Refinement	CIS	Improved visual explanations of assessment scoring, test categories, and evidence mechanisms			
FDBK-004	23/01/2023	Technical Forum 2023	Developer	PSTVA	Complexity of user configuration parameters for non-expert users	Usability	High	Technical Refinement	ADDS	Add more pre-configured scan profiles	Done	v1.2 (Mar 2023)	
FDBK-005	05/12/2023	Nickova Workshop	Consultant	PSTVA	Add Directory vulnerability scanning feature accessibility through GUI	Usability	Medium	Technical Refinement	ADDS	Update the User Manual to include Directory vulnerability scanning option	Done	v1.2 (Mar 2023)	
FDBK-006	05/12/2023	Nickova Workshop	Consultant	PSTVA	User Scanning feature accessibility through GUI	Usability	Medium	Technical Refinement	ADDS	Update the User Manual to include the Code Analysis option	Done	v1.2 (Mar 2023)	
FDBK-007	05/12/2023	Nickova Workshop	Developer	PSTVA	Unlinked OS, a windows version would be nice to have	Documentation	High	Documentation update	ADDS	ADP guidelines for deployment on systems that run Windows	Done	v1.2 (Mar 2023)	
FDBK-008	05/09/2023	Athens NTUA Validation Workshop	Developer	CAC	User Find it difficult to add new products	Usability	High	Training material update	CIS	Add User Manual and Terms and conditions to the UI menu for better visibility	Done	Hot Fix	
FDBK-009	05/09/2023	Athens NTUA Validation Workshop	Developer	PSTVA	The flow of scanning output was not clear	Usability	Medium	Technical Refinement	ADDS	Use different color updates and font size	Cancelled	v1.2 (Mar 2023)	
FDBK-010	05/09/2023	Athens NTUA Validation Workshop	Developer	PSTVA	Add refresh the main page whenever user action triggered on the page	Usability	Medium	Technical Refinement	ADDS	Update the User Manual to include the Directory vulnerability scanning option	Done	v1.2 (Mar 2023)	
FDBK-011	4/12/2023	Zagreb Validation Workshop	Consultant	PSTVA	Make the workflow accessible	Functionality	Low	Technical Refinement	ADDS	Provide a general workflow with API with a general workflow	Cancelled	v1.2 (Mar 2023)	
FDBK-012	4/12/2023	Zagreb Validation Workshop		PSTVA	Create a MCP help user with assessment	Functionality	Low	Technical Refinement	ADDS	Create an MCP server and hosted on ADDS server, with a general workflow with API with a general workflow	Cancelled	v1.2 (Mar 2023)	
FDBK-013	4/12/2023	Zagreb Validation Workshop	Developer	PSTVA	Add checkbox to the UI, under the scope of guide user with functionalities	Functionality	Low	Technical Refinement	ADDS	Add a light activation module inside the main console, and new feature on UI for the checkbox, text and text for documentation	Cancelled	v1.2 (Mar 2023)	
FDBK-014	4/12/2023	Zagreb Validation Workshop	Consultant	CyReA Portal	The UI has to be more mobile friendly	Usability	Medium	Technical Refinement	ADDS	Enable Formatted Binary Native for more efficient loading of mobile (phones and tablets)	Done	v1.2 (Mar 2023)	
FDBK-015	4/12/2023	Zagreb Validation Workshop		CyReA Portal	Implement an interactive chatbot within the application to assist users in navigating, understanding tools, and completing workflows related to the UI	Functionality	Medium	Technical Refinement	ADDS	Implement and integrate a chatbot within the application (e.g., providing guidance, real-time guidance to users across tools)	Cancelled	v1.2 (Mar 2023)	
FDBK-016	4/12/2023	Zagreb Validation Workshop		CyReA Portal	Create and implement a consistent, structured tool set representing each tool within the portal UI	Usability	High	Documentation update	ALL	Create usage, and integrate consistent user for each in the UI, ensuring alignment with the design system and ensuring readability across all components	Pending	v1.2 (Mar 2023)	
FDBK-017	4/12/2023	Zagreb Validation Workshop		DPMA	The DPMA tool could be improved by making it more user-friendly, adding clearer guidance, and including more practical examples for easier implementation	Documentation	Low	Documentation update	ADDS	Manual for DPMA has been updated in previous version	Done	v1.2 (Mar 2023)	
FDBK-018	4/12/2023	Zagreb Validation Workshop		DPMA	Notes on valid tool with some tool, using GUI that will guide users through the process	Usability	Medium	Technical Refinement	ADDS	ADDS point has decided that we are not planning to make any changes to the tool	Cancelled	v1.2 (Mar 2023)	
FDBK-019	05/09/2023	Athens NTUA Validation Workshop		DPMA	Functionality of creating the implemented controls to better monitor vulnerability and risks	Functionality	Low	Technical Refinement	ADDS	ADDS point has decided that we are not planning to make any changes to the tool	Cancelled	v1.2 (Mar 2023)	

FIGURE 18. FEEDBACK_TO_ACTION TRACKER

Role in the CI/CD Pipeline and DevOps Strategy

The tracker is integral to CURIUM’s DevOps-driven update strategy, which emphasizes rapid iteration and maintenance of regulatory alignment with the Cyber Resilience Act (CRA):

- Iterative Refinement Loop: Feedback logged in the tracker is translated into technical improvement requests passed to Task 3.2 (Deployment). This ensures that each release cycle (Alpha, Beta, Final) incorporates specific fixes derived from user needs.
- Automated CI/CD Integration: Refinements identified in the tracker are fed into a pipeline using GitLab CI/CD for automated builds, testing, and deployment. This allows the consortium to deliver bug fixes and new features — such as the v1.2 interface optimization for mobile devices (FDBK-014) — without service disruption.
- Deployment via Containerization: The DevOps strategy utilizes Docker and Kubernetes to ensure that tool updates are portable and scalable. For example, technical refinements for the PSTVA toolkit (like FDBK-004 to add pre-configured scan profiles) are deployed as updated images within the production environment.
- "Hot Fix" Capability: The tracker enables the team to identify high-priority issues that require immediate attention outside of major releases. A notable example is FDBK-008, where users found it difficult to add new products; this was resolved via a "Hot Fix" that relocated the User Manual to the top-level menu for better visibility.
- Traceability and Accountability: By assigning items to specific partners and recording Resolution Notes, the tracker ensures that all technical refinements are verified and mapped back to the initial stakeholder requirement, maintaining a ≥98% accuracy in compliance documentation.

5.1.1 CURIUM Portal (Landing Page)

The final production deployment of the Curium Continuum portal marks its transition from an iterative development framework to a fully operational, stable ecosystem. Deployed in its final v1.2 release as of June 2026, the portal establishes a centralized, hardened environment hosting the core cybersecurity toolsets (DPRA, DPMA, CyReA, CAC, and PSTVA) alongside the newly integrated training modules, compliance layers, and localized manual download infrastructures. The operational environment is optimized for high availability, secure session continuity via continuous token propagation, and seamless user lifecycle management. To ensure long-term sustainability, operational workflows include structured telemetry monitoring and an active

maintenance pipeline capable of absorbing technical refinements driven directly by stakeholder validation activities.

Operational optimization and post-deployment refinements are systematically guided by insights gathered during end-user validation workshops. This feedback loop ensures that the portal's production state remains aligned with practical deployment realities and user experience standards. A critical component of this operational evolution involved addressing specific technical refinements logged by domain experts during live validation trials. The table below details a specific high-priority usability refinement capturing end-user feedback from the field and its subsequent resolution within the final v1.2 deployment footprint.

TABLE 1. ZAGREB WORKSHOP USER FEEDBACK LOOP

Validation Event	Feedback Summary	Technical Resolution	Status
Zagreb Workshop (April 2026)	Interface optimization required for mobile and tablet devices.	Enabled responsive frontend library features for efficient cross-platform rendering.	Completed (v1.2)

5.1.2 Cyber Resilience Assessment (CyReA)

The CyReA tool has progressed from iterative development to a stable and ready to use service for supporting to determine the scope of product with digital element by following the Cyber Resilience Act (CRA). The final phase has focused on aligning classification logic with CRA requirements, incorporating structured user feedback, and preparing the tool for the deployment.

The Product Classification service of CyReA has achieved full functionality, demonstrating full operational capability through the portal. Key advancements include enhanced classification workflows aligned with CRA criteria, improved usability for non-expert users, detailed information at each stage of the product classification and strengthened system integration for seamless deployment to the portal as a part of final release. Following Features are enhanced for the final release by following the feedback from the validation activities.

Technical and Functional Enhancement

From a technical perspective, the enhancements were introduced to align the tool with CRA requirements for product classification and improve usability. Product classification logic has been refined so that users can more clearly map their products to the appropriate categories and obligations. These include the integration of CRA-aligned product classification, enabling structured identification of product categories and associated necessary competence such as risk assessment and awareness. Moreover, an overview of the CRA framework and product class definitions has been embedded within the tool to support user understanding. At the end of each question set, users are now provided with automated summaries and detailed guidance based on their responses. Finally, Improvements have been made to the presentation and transparency of classification results. The tool now clearly presents product classification outcomes, ensuring that users can easily understand how their inputs map to CRA requirements.

Validation and User Feedback

The tool has been validated through the series of validation session for obtaining structured feedback sessions. Feedback highlighted the need for clearer definitions, practical examples, and transparent outcomes. These insights directly informed the integration of enhanced explanatory content and improved response summaries. Validation activities confirmed that the updated workflows are accessible to non-expert users while maintaining alignment with regulatory expectations.

5.1.3 Digital Product Risk Management (DPRA)

The Digital Product Risk Assessment (DPRA) tool has reached to the final deployment-ready stage, with recent efforts focused on improving usability, strengthening risk modelling capabilities, and aligning outputs for informed decision making for managing the risks. The latest updates reflect both technical refinements and user-driven enhancements identified during validation activities.

Technical and Functional Enhancement

From a technical perspective, several improvements have been introduced to enhance both functionality and user interaction. The graphical user interface has been redesigned to provide a clearer and more intuitive layout, improving overall navigation and user experience. It also includes customization options, such as selectable background themes, have been included to accommodate user preferences and accessibility needs. The DPRA also incorporates a more structured approach for defining security objectives and mapping corresponding security requirements for ICT products. The Identified ICT products are systematically decomposed to establish a detailed product-based asset inventory, forming the foundation for more accurate risk assessment. Furthermore, vulnerabilities associated with specific ICT products are now explicitly identified and prioritised, enabling more consistent and transparent risk level calculations. From functionalities context, DPRA now provides a more coherent risk management process, ensuring that ICT product decomposition, vulnerability prioritisation, and risk calculation are consistently linked. In addition, the enhanced visual design and structured outputs support clearer interpretation of results, improving both usability and auditability. These improvements position the DPRA tool as a reliable component within the broader compliance framework, ready for deployment in real-world risk management scenarios.

Validation and User Feedback

User feedback is obtained through the series of validation workshops to enhancement of the DPRA tool before final release. Users highlighted the importance of improved usability, clearer visual structure, and better alignment between identified assets, vulnerabilities, and calculated risks. The updated interface and enhanced workflows directly address these needs, making DPRA more accessible for all user groups. Validation results indicate that users are now better able to understand the relationship between product components, associated vulnerabilities, and resulting risk scores.

5.1.4 Digital Product Maturity Assessment (DPMA)

The DPMA tool's final production environment reflects its integration into the wider CURIUM ecosystem. Users access the tool through the Curium platform via Single Sign-On (SSO), so authentication is handled entirely by Curium's identity and access management rather than by a separate login system within DPMA. This reduces the deployment's attack surface and avoids duplicating access controls across tools.

One point worth clarifying: the RAG-based platform used to prepare and consolidate the underlying dataset is not part of DPMA and does not exist within its production environment. It's a separate, standalone application used earlier in the workflow, solely to review and de-duplicate the standards and framework documentation feeding into DPMA's content. Once that preparatory work is done, the output becomes a static, curated dataset that gets integrated into DPMA. The production application itself never connects to, queries, or depends on the RAG platform at runtime — the two are fully decoupled, and RAG plays no role in DPMA's live operation.

What end users actually interact with is a lightweight system: a web application that authenticates via Curium SSO and serves the pre-prepared dataset for search, navigation, and export. Keeping the more sensitive data-processing work — ingesting and de-duplicating standards documentation — confined to an earlier offline stage means the production environment stays small, predictable, and isolated from that process entirely.

Before reaching this final state, DPMA went through a structured validation process, with feedback gathered from several stakeholder events: the SEC Forum 2025, the Zagreb Validation Workshop, and the Athens NTUA Validation Workshop. Feedback from these sessions was logged, categorised (Documentation, Usability, Functionality), prioritised, and assigned to APIROPLUS SERVICE Ltd. for review.

This led to an update of the DPMA User Manual, bringing the documentation back in line with the actual tool interface. Suggestions around further UI/UX improvements — for example, using LLM-guided navigation to help users through the tool — were also reviewed, and the decision was made not to pursue further UI changes at this stage of the project. Requests to extend DPMA into risk management, or to integrate it directly with DPRA, were assessed and closed as out of scope since DPMA is designed to help identify applicable security measures, not to perform risk management, and direct DPRA integration sits outside the current project's boundaries.

Overall, this feedback cycle confirmed that the final production version of DPMA meets its intended purpose and stakeholder expectations, while keeping its functional boundaries clearly defined.

5.1.5 Penetration Self-Testing & Vulnerability Assessment (PSTVA)

The final development milestones, operational strategies, and consolidated core optimizations of the PSTVA (Platform for Self-Testing and Vulnerability Assessment) toolkit represent the culmination of an iterative, data-driven development lifecycle heavily informed by formal end-user validation activities.

The transition from a raw orchestration utility to a finalized production ecosystem involved merging architectural optimizations with tactical fixes derived from end-user feedback. The table below outlines how specific validation logs from action tracker map directly to the core enhancements deployed in the final release.

TABLE 2. VALIDATION LOGS FOR PSTVA FROM THE FEEDBACK-TO-ACTION TRACKER

Feature Area / Enhancements	Technical Implementation & Changes	Driver / Validation Activity Source
Predefined Configuration Profiles	Implemented pre-configured scan profiles within the UI. Users can now execute rapid vulnerability assessments without adjusting complex underlying CLI arguments.	High-Priority Usability Fix: Addressed developer feedback stating that command execution parameters were too complicated for novice operators.
Standalone Active Directory Scans	Updated the front-end dashboard to display the Active Directory Scan Flow (using ADEnum and Kerbrute) as an independent, standalone testing option.	Medium Priority Usability Fix: Responded to consultant requests to execute directory enumeration separately from broad network sweeps.
Integrated SAST Control Center	Developed a direct front-end interface for static application security testing, embedding Horusec analysis options smoothly into the central dashboard.	Medium Priority Usability Fix: Incorporated developer feedback requiring explicit UI-driven code scanning controls alongside DAST options.
"Smart Graph" Visualization Engine	Refactored the data layer and integrated a custom visualization engine to render Neo4j graph	High-Priority Visualization Update: Replaced cluttered, text-heavy scan formats with a reader-

	nodes dynamically, detailing asset-vulnerability links cleanly.	friendly, intuitive graphical overview.
Real-Time Interface Synchronicity	Optimized UI rendering with auto-scroll data capabilities that display background pipeline logs in real time as elements register on the graph database.	Medium Priority Usability Fix: Fixed visual lag and interface synchronization bottlenecks during high-volume scans.
Docker Layer Environment Optimization	Restructured container layers, minimized base image footprints, and streamlined ephemeral container lifecycles to minimize CPU/RAM overhead.	Performance Refinement: Applied structural optimizations to shorten scanning task execution timelines.

5.1.6 Conformity Assessment and Compliance (CAC)

The Conformity Assessment and Compliance (CAC) tool has transitioned from an iterative development phase to a stable, production-ready module within the CURIUM Compliance Continuum (v1.2).

The focus of development during this period has been on enhancing UI/UX accessibility for non-experts, integrating a unified Single Sign-On (SSO) architecture, and refining the tool based on structured feedback from validation workshops in Athens and Zagreb.

Development Progress (January – June 2026)

The CAC service has reached Technology Readiness Level (TRL) 7-8, indicating it is fully operational in a web-based environment and has been demonstrated through real-world validation.

Key technical enhancements included:

- SSO and IAM Integration: Resolution of access friction through a centralized Identity and Access Management (IAM) layer, enabling seamless transitions between the CURIUM Portal and the CAC tool.
- Production Hardening: The environment has been optimized for high availability, continuous propagation for session continuity.

Validation Insights

Athens Workshop (March 2026)

The Athens workshop provided critical data on the tool's usability for its primary target group, i.e., SMEs and non-cybersecurity experts:

- Usability (NFR-002): Respondents strongly agreed they could use the CAC tool without hiring an external expert (avg. score 5.0/5.0).
- UI Quality (NFR-005): The tool achieved a 100% satisfaction rate for UI cleanliness and label clarity.
- Critical Feedback: Despite high scores, users reported moderate difficulty in the initial step of "Adding a new product" (avg. difficulty 3.0/5.0). Stakeholders specifically requested more immediate access to instructional materials to guide them through complex product data entry.

Zagreb Workshop (April 2026)

The Zagreb workshop demonstrated the effectiveness of the iterative improvements implemented after the Athens event:

- **Improved Workflows:** The perceived difficulty of adding a new product dropped to 2.3/5.0, showing that UI refinements made the process more intuitive. (1- being easy and 5 – being hard to add new products)
- **Recommendation Likelihood (KPI 5):** The tool maintained a strong recommendation score of 8.3/10, with 100% of respondents finding labels, buttons, and instructions easy to understand.
- **User Intent:** A significant percentage of participants (26%) identified CAC as the most relevant tool for their organization’s CRA journey, particularly for automated EU Declaration of Conformity (DoC) generation.

Feedback-to-Action Tracker Implementation

Refinement actions for the CAC tool have been systematically logged and resolved through the Feedback-to-Action Tracker.

Key entries since January 2026 include:

TABLE 3. KEY ENTRIES TO THE FEEDBACK-TO-ACTION TRACKER

Feedback ID	Source	Feedback Summary	Technical Resolution	Status
FDBK-001	Techritory/Athens	Need for clarity on why specific documentation artefacts are requested.	Introduction of contextual help texts and tooltips linked directly to CRA Annex VII provisions.	Done
FDBK-008	Athens	Users found it difficult to add new products due to buried instructions.	Relocated User Manual and Terms & Conditions to the top-level menu for persistent visibility.	Done (Hot Fix)

These refinements ensure that the CAC tool not only meets the functional requirements for CRA compliance (e.g., FR-004 for automated DoC generation) but also remains accessible to the small and micro-enterprises the CURIUM project aims to support.

5.2 Data Management and Privacy

CURIUM handles sensitive data security and GDPR compliance through a structured framework of technological safeguards, organizational policies, and dedicated oversight. The project’s approach is detailed in its Data Management Plan (DMP), which prioritizes the confidentiality, integrity, and availability of all research and personal data.

GDPR Compliance Framework

CURIUM is fully committed to the General Data Protection Regulation (GDPR) and other European legal standards. Key elements of this compliance include:

- **Data Protection Officer (DPO):** The project has appointed a central DPO to oversee compliance, monitor adherence to laws, and liaise with supervisory authorities. Each consortium partner also maintains their own DPO for organization-specific matters.
- **Roles and Responsibilities:** Partners processing personal data act as independent data controllers, responsible for maintaining internal records and ensuring their staff are informed of GDPR obligations.

- **Privacy-Enhancing Measures:** Although large-scale personal data processing is not foreseen, any such data collected is protected via encryption, pseudonymization, and anonymization where feasible. Techniques like anonymous micro-aggregation and statistical disclosure control are used to balance usability and privacy.
- **Data Principles:** The project adheres to data minimization and purpose limitation, ensuring that only the minimum necessary information is collected or exchanged.
- **Data Classification Scheme**
- To ensure appropriate handling, CURIUM categorizes information into three levels:
- **PUBLIC:** General project information that can be circulated freely.
- **CONFIDENTIAL:** Data belonging to the project that is not public; access is restricted based on the "need to know" principle.
- **CONFIDENTIAL / Partner Proprietary:** Sensitive material belonging to a specific partner that requires explicit permission from the owner for any use or dissemination.

Technical Security Measures

The project implements a layered cybersecurity strategy to protect sensitive data:

- **Secure Storage:** The primary repository is a secure Microsoft SharePoint environment within a trusted institutional Microsoft 365 infrastructure.
- **Access Control:** Access is strictly role-based (RBAC), ensuring users only see data relevant to their responsibilities.
- **Encryption:** Data is protected by TLS encryption in transit and standard encryption at rest.
- **Monitoring and Defense:** The system maintains comprehensive audit logs, real-time access monitoring, and defenses against brute-force and phishing attacks.
- **Secure Transfers:** Any transfer of sensitive information between partners occurs through encrypted channels.

Retention and Breach Response

- **Data Retention:** Project information and confidentiality obligations are maintained for five years after the final payment, as defined in the Grant Agreement.
- **Open-access data** also remains available for at least five years post-project.
- **Breach Response:** In the event of a suspected breach, partners must activate internal incident response plans compliant with GDPR and national laws. This includes immediate containment, investigation, and mandatory notification to relevant Data Protection Authorities (DPAs), the Project Coordinator, and the DPO.

6 Feedback-Driven Refinements (AEGIS)

This section presents the final outcomes of the feedback-driven refinement process applied to the CURIUM Compliance Continuum during the last phase of the project. Building on the framework established in the earlier version of this deliverable (namely D3.1 “Continuous release of tools and services and support for training, knowledge, and capacity building”), the refinement process ensured the continuous integration of insights gathered from WP4 validation activities into the final version of the tools and services.

In this phase, feedback collected through structured validation workshops, user evaluations, and pilot usage sessions was consolidated, prioritised, and translated into concrete technical and usability improvements across the CURIUM services and the CURIUM Portal. Emphasis was placed on improving usability, clarity of workflows, consistency across tools, and alignment with end-user expectations, especially for SMEs and micro-enterprises.

The refinement activities supported the transition of the CURIUM Compliance Continuum from iterative development to final release, ensuring that the system reflects validated user needs, addresses identified usability and functional gaps, and delivers a stable and coherent end-to-end experience. The following subsections provide an overview of the feedback management approach, a synthesis of key findings from WP4 validation rounds, and a summary of the final refinements implemented in the CURIUM tools and services.

6.1 Overview of the Feedback Management Framework

The feedback management approach applied in the final phase of the CURIUM project builds upon the framework defined and described in D3.1. In particular, the **Feedback-to-Action Tracker** introduced in D3.1 remains the central mechanism for the structured collection, tracking, and management of stakeholder feedback throughout the WP4 validation activities.

This framework ensures traceability between feedback items and the corresponding CURIUM components, as well as consistent categorisation, prioritisation, and assignment of corrective or improvement actions. It has continued to support the systematic processing of feedback from validation workshops, pilot activities, and user evaluations, enabling a controlled flow of information from external stakeholders to WP3 implementation activities.

For a detailed description of the framework and the structure and fields of the Feedback-to-Action Tracker, including categorisation and prioritisation criteria, please refer to Section 6 of D3.1.

In the context of D3.2, this established framework has been used to consolidate final validation results and ensure that all relevant feedback has been appropriately addressed or documented as part of the final refinement cycle of the CURIUM Compliance Continuum.

6.2 Synthesis of Feedback from WP4 Validation Rounds

6.2.1 Riga Validation workshop

The first validation workshop was conducted in Riga, Latvia, in October 2025 as part of the TECHRITORY Digitalization & Connectivity Forum. The event represented the first opportunity to collect structured feedback from external stakeholders regarding the initial release of the CURIUM Compliance Continuum. At the time of the workshop, only two components of the Continuum were available for demonstration and evaluation: the Conformity Assessment and Compliance (CAC) tool and the Penetration Self-Testing and Vulnerability Assessment (PSTVA) toolkit. A detailed description of the event, validation methodology, participant profile, and KPI assessment is provided in Deliverable D4.1 - Section 4.3.1.

The workshop marked the initial operationalisation of the CURIUM Feedback Management Framework in a real-world validation setting. Feedback was collected through direct user interaction during demonstrations and hands-on exploration activities and subsequently recorded in the Feedback-to-Action Tracker for structured analysis, prioritisation, and follow-up actions.

A total of four feedback items were recorded during this workshop. Three feedback items were related to the CAC tool and one to the PSTVA toolkit. The CAC-related feedback primarily focused on the need for improved transparency and interpretability of the compliance assessment process. Participants requested clearer explanations regarding:

- (i) the rationale behind required technical documentation artefacts
- (ii) the methodology used for scoring questionnaire responses, and
- (iii) the relationship between intermediate assessment outputs and final conformity readiness results is important. While the tool was generally perceived as useful and relevant, these comments highlighted

the importance of strengthening contextual guidance and explanatory support within the user interface, particularly for SMEs and non-expert users.

The single PSTVA-related feedback item concerned the complexity of scan configuration parameters. Participants indicated that certain configuration options were not sufficiently intuitive for non-specialist users, which could limit accessibility for SMEs without dedicated cybersecurity expertise. This observation was directly relevant to the project objective of ensuring usability and adoption across organisations with varying technical maturity levels.

Although the feedback volume at this early stage was limited, a clear concentration pattern emerged. Feedback was exclusively focused on the two tools available at this stage - CAC and PSTVA - which also represent the most interaction-intensive components of the Continuum. These tools require either interpretation of regulatory and compliance logic (CAC) or direct configuration of technical security operations (PSTVA), which naturally generates a higher level of user interaction and clarification needs compared to other, more structured assessment-oriented services introduced in later phases.

Two main thematic areas of improvement were identified across the feedback set: (i) enhanced contextual guidance and explanation of compliance logic, assessment scoring, and result interpretation; and (ii) simplification of technical configuration steps to improve accessibility for non-expert users.

Overall, the Riga workshop provided the first structured validation input for the CURIUM Compliance Continuum and confirmed the relevance of both evaluated tools. The feedback collected was systematically recorded in the Feedback-to-Action Tracker and fed into the WP3 refinement cycle, informing subsequent iterations of usability improvements and interface enhancements across the Continuum.

6.2.2 Nicosia Validation workshop

The second CURIUM validation workshop took place in Nicosia, Cyprus, in December 2025 and represented a major milestone in the validation activities, as it was the first event where the full set of CURIUM Compliance Continuum tools (CyReA, DPRA, DPMA, CAC, and PSTVA) were presented and tested in an integrated manner. A detailed description of the event setup, validation methodology, KPI evaluation, and user feedback is provided in Deliverable D4.1 – Section 4.3.2.

This workshop marked the transition from individual tool validation (as performed in the first workshop) to end-to-end Continuum validation, allowing stakeholders to evaluate not only standalone functionalities but also the coherence of the overall compliance journey across tools.

Overall feedback confirmed a strong positive perception of the integrated Compliance Continuum approach, with participants highlighting the value of combining cyber resilience assessment, risk management, maturity evaluation, vulnerability testing, and compliance documentation within a single ecosystem. The results reinforced the relevance of the modular design, while also providing insights into cross-tool usability and operational consistency.

The feedback collected indicated that users particularly appreciated:

- The ability to navigate between different compliance stages within a unified framework
- The perceived efficiency gains in managing CRA-related tasks through automation
- The overall usability and accessibility of the tools for SME-oriented use cases
- The value of structured guidance across compliance workflows

At the same time, the workshop identified several areas for refinement, primarily related to usability and accessibility of specific advanced functionalities, particularly within PSTVA. Feedback highlighted the need to

simplify access to more technical features, improve clarity of available scanning options, and enhance deployment guidance for heterogeneous environments.

The Feedback-to-Action Tracker captured a set of concrete improvement actions arising from this workshop. Key refinements included improving GUI accessibility for advanced PSTVA modules (e.g. Active Directory scanning and code analysis features) and extending deployment documentation to support Windows-based environments, addressing a previously identified limitation in the tool onboarding process.

These feedback-driven improvements demonstrate the increasing maturity of the PSTVA component, shifting from initial usability validation towards broader deployment readiness and environment compatibility. All identified actions were assigned, implemented, and scheduled for inclusion in subsequent releases, contributing to the progressive stabilization of the CURIUM Compliance Continuum.

Finally, the workshop confirmed the importance of maintaining a strong focus on usability and deployment flexibility, particularly for SME and consultant stakeholders, as the platform evolves from demonstration-level tools to more operationally deployable solutions.

6.2.3 Athens Validation workshop

The third CURIUM validation workshop was held in Athens, Greece, in March 2026 and represented a further step in the maturation of the CURIUM Compliance Continuum. Unlike the previous validation rounds, the workshop adopted a more granular, tool-specific feedback approach, enabling participants to assess each of the five Continuum components individually following hands-on interaction. A detailed description of the event setup, validation methodology, participant profile, KPI assessment, and complete validation results is provided in Deliverable D4.1 - Section 4.3.3.

The Athens workshop provided more detailed and actionable feedback on the usability, interface quality, and practical operation of the individual CURIUM tools. The use of dedicated questionnaires for each tool enabled feedback to be collected immediately after user interaction, providing a more focused view of strengths, usability barriers, and potential areas for refinement.

Overall, the feedback confirmed a positive perception of the CURIUM tools, with all five components receiving high recommendation scores. Participants also demonstrated strong engagement with the tools, while the workshop generated additional interest from potential users wishing to arrange dedicated sessions for testing CURIUM tools with their own products or organisational environments. The feedback therefore provided not only technical and usability insights but also indications of potential future adoption and exploitation interest.

The Feedback-to-Action Tracker captured several concrete improvement actions arising from the workshop. For the **CAC tool**, participants identified some difficulty in the process of adding a new product and requested improved visibility of supporting information. This resulted in adjustments to the interface structure, including the relocation of the User Manual and Terms & Conditions to the top-level menu (FDBK-008). For **PSTVA**, users highlighted the need for more immediate visibility of newly generated scan results, leading to the implementation of an automatic page refresh mechanism for the relevant graphical modules (FDBK-010).

Additional feedback concerned the need for stronger guidance and clearer explanations within the tools. Participants requested more examples and explanatory content in **CyReA**, while feedback on **CAC** reinforced the need for contextual help explaining why specific CRA-related documentation artefacts are requested. These observations were consistent with the guidance and interpretability requirements already identified in the earlier validation rounds and further reinforced their importance for non-specialist users.

The workshop also generated broader architectural feedback concerning the relationship between the **DPRA** and **DPMA** components. Participants expressed interest in a more closely integrated risk-to-maturity workflow, highlighting the potential value of a smoother transition between risk identification, treatment, and maturity assessment. This feedback was considered in the further refinement of the overall Compliance Continuum and its cross-tool user journey.

Overall, the Athens workshop demonstrated a higher level of maturity in the validation process, moving beyond the identification of basic usability issues towards more granular optimisation of individual tools and consideration of cross-tool integration. The feedback collected was systematically recorded in the Feedback-to-Action Tracker and used to guide subsequent refinements, while also providing valuable input for the finalisation of the CURIUM Compliance Continuum.

6.2.4 Zagreb Validation workshop

The fourth CURIUM validation workshop was held in Zagreb, Croatia, in April 2026 and represented an important validation step towards the finalisation of the CURIUM Compliance Continuum. The workshop extended the tool-specific validation approach established in Athens by introducing the **CURIUM Portal** as an additional validation target, alongside the five core tools (CyReA, DPRA, DPMA, CAC, and PSTVA). A detailed description of the event setup, validation methodology, participant profile, KPI assessment, and complete validation results is provided in Deliverable D4.1 - Section 4.3.4.

The Zagreb workshop provided particularly valuable feedback on the **overall user experience and accessibility of the CURIUM environment**, complementing the more tool-specific feedback collected during previous validation rounds. The inclusion of the Portal enabled stakeholders to assess not only individual services but also the way in which users discover, access, and navigate between the different components of the Compliance Continuum.

Overall, the feedback confirmed a positive perception of the CURIUM environment, with strong recommendation scores across most tools and particularly positive assessments of the Portal's navigation between services and overall user experience. The results also indicated that the usability improvements introduced following earlier validation rounds, particularly for CAC, had a measurable positive effect. The reduced perceived difficulty of adding a new product in CAC provided evidence that feedback collected in previous rounds had been effectively translated into usability refinements.

At the same time, the workshop identified several areas requiring further attention before the final release. For the **CURIUM Portal**, participants generally found navigation and the overall user experience positive, while interface intuitiveness received comparatively lower scores. This indicated a need to further simplify the presentation and strengthen the guidance provided to users when moving through the Compliance Continuum. Participants also suggested the use of a more explicit **customer journey representation**, clearer tool-specific visual cues, and additional guidance to help users understand which service should be selected at different stages of their compliance process.

Accessibility across different device types was another concrete area of improvement. Feedback identified limitations in the rendering of the CURIUM Portal on mobile and tablet devices. This resulted in a technical refinement to enable responsive front-end functionality, incorporated into release v1.2 (FDBK-014). This action extended the accessibility of the Portal beyond desktop environments and supported the project's objective of providing an easily accessible solution for a broad SME user base.

Feedback concerning **PSTVA** continued to highlight usability challenges associated with more technically advanced functionality. The comparatively lower recommendation score for the toolkit, together with requests

for simplified scan configuration and more intuitive navigation, reinforced the usability concerns identified during the earlier Riga and Nicosia workshops. This recurring feedback pattern further confirmed the importance of simplifying technical workflows and providing appropriate guidance for users without specialised cybersecurity expertise.

The workshop also generated several forward-looking suggestions, including AI-supported guidance, clearer tool-specific icons, and a more prominent visual representation of the customer journey on the Portal landing page. While not all such suggestions were considered within the scope of the final project release, they provide useful input for the future evolution and exploitation of the CURIUM platform.

Overall, the Zagreb workshop demonstrated that the validation process had progressed from the assessment of individual tool functionality towards a broader evaluation of **platform-level usability, accessibility, navigation, and user journey design**. The feedback collected was systematically recorded in the Feedback-to-Action Tracker and used to guide final technical refinements and prioritisation decisions for the CURIUM Compliance Continuum.

6.2.5 Nicosia “Skills” validation workshop

The fifth CURIUM validation activity was conducted in Nicosia, Cyprus, in June 2026 as part of the high-level *Skills for Digital Autonomy: Empowering a Resilient Society* conference. Unlike the preceding structured validation workshops, the activity took the form of a dedicated CURIUM stand at a policy-oriented European event, where visitors could voluntarily interact with the tools according to their interests. A detailed description of the event setup, validation methodology, participant profile, KPI assessment, and validation results is provided in Deliverable D4.1 -Section 4.3.5.

The activity provided an opportunity to extend the validation campaign beyond the predominantly technical, product-oriented, and SME audiences engaged through the previous workshops. The conference brought together policymakers, institutional stakeholders, academia, industry, and other actors concerned with digital resilience and skills. The two external respondents who completed tool-specific questionnaires were both representatives of micro-enterprises in non-IT/IS management roles, providing an additional perspective on the accessibility of the CURIUM tools for users without a specialised cybersecurity background.

Validation was conducted through informal, hands-on demonstrations at the CURIUM stand, with visitors selecting the tools of greatest relevance to their interests. Two tool-specific questionnaires were subsequently completed, covering CyReA and DPMA. Given the voluntary and informal nature of the stand-based interaction and the limited number of responses, the results should be interpreted as indicative validation feedback rather than as statistically representative evidence.

Despite the limited sample, the feedback provided a positive signal regarding usability and interface accessibility. The DPMA respondent rated both navigation through controls and measures and identification of the organisational maturity level at the maximum score of 5/5, successfully identified relevant organisational threats, and rated the overall UX at 5/5. Navigation and labels were also assessed positively, while the tool received a recommendation score of 10/10. These results are consistent with the strong usability performance observed for DPMA during the structured Athens and Zagreb validation workshops and provide additional confirmation that the tool can be understood and operated by users without specialised cybersecurity expertise.

CyReA also received positive usability feedback, with the respondent rating navigation as extremely easy, labels and buttons as easy to understand, and overall UX at 4/5. The respondent indicated willingness to adopt the tool and provided contact details for potential future testing. The product-classification task itself was not completed during the stand interaction because of the limited time available. This should not be interpreted as

a functional usability failure, particularly given the informal nature and short duration of exhibition-based interactions, but rather as an indication of the importance of providing concise and immediately accessible user journeys for such engagement formats.

From a feedback-management perspective, the activity therefore provided additional confirmation of the accessibility of the CURIUM tools for non-specialist and management-oriented users, while also highlighting the value of short, self-contained interaction flows when validation takes place outside a structured workshop environment. The positive results for DPMA reinforced the usability improvements and design choices emerging from the previous validation rounds, while the CyReA adoption signal provided an additional indication of potential user interest and exploitation relevance.

Overall, the Cyprus “Skills” Validation activity complemented the four structured workshops by broadening the stakeholder base exposed to the CURIUM Compliance Continuum and by testing its accessibility in a less formal, exhibition-based setting. Although the limited number of responses restricts the strength of quantitative conclusions, the feedback was consistently positive and reinforced the broader validation finding that the CURIUM tools can be understood and used by non-cybersecurity specialists. The activity also generated an additional lead for future product-level testing, supporting the continuation of the validation and exploitation pathway beyond the project demonstration events.

6.2.6 BEYOND validation workshop

The sixth CURIUM validation activity was conducted in Athens, Greece, in June 2026 as part of the BEYOND 2026 international technology and innovation exhibition. The activity extended the validation campaign into an exhibition environment, where CURIUM was showcased at the APIROPLUS SERVICES stand and visitors could voluntarily interact with the Compliance Continuum tools according to their interests. A detailed description of the event setup, validation methodology, participant profile, KPI assessment, and validation results is provided in Deliverable D4.1 - Section 4.3.6.

The BEYOND activity provided an opportunity to engage directly with a broad technology-oriented audience, including digital providers, research organisations, and other product-oriented stakeholders. This complemented the more structured SME and institutional validation activities conducted during the previous workshops and enabled the CURIUM tools to be evaluated in a more informal setting closely resembling a real-world technology demonstration or exploitation environment. The exhibition context also resulted in visitors selecting individual tools according to their perceived relevance, rather than following a predefined validation sequence.

Validation was conducted through live, hands-on demonstrations tailored to the interests and products of individual visitors, followed by completion of the corresponding tool-specific questionnaire. Eleven questionnaires were collected across four tools: CyReA (6), CAC (3), DPRA (1), and DPMA (1). No questionnaire was collected for PSTVA. As with the Cyprus Skills Validation activity, the voluntary and exhibition-based nature of the interaction and the uneven distribution of responses mean that the results should be interpreted as complementary and indicative evidence rather than as statistically representative validation results.

The feedback nevertheless provided strong additional confirmation of the usability and accessibility of the CURIUM tools. CyReA, which serves as the entry point to the Compliance Continuum, achieved particularly positive results: all six respondents confirmed that they were able to obtain information on the classification of their product, while labels and buttons were considered easy to understand by all respondents. Navigation was rated positively by all six participants, with four finding it extremely easy and two somewhat easy. Overall UX

reached 4.4/5 and recommendation likelihood 9.1/10, providing further evidence that the tool can support the initial product-classification step of the CRA compliance journey in an accessible manner.

CAC also demonstrated very strong usability results. All three respondents strongly agreed that they could use the tool without hiring a cybersecurity expert, while the task of adding a new product was rated at only 1.3/5 in perceived difficulty, representing the strongest result for this task across the validation activities. All respondents considered the interface clean and the labels and buttons easy to understand, while navigation was rated either very easy or extremely easy. The overall UX score was 5/5, and recommendation likelihood reached 29/30. These findings further reinforce the positive usability evolution already observed for CAC following the refinements introduced after earlier validation rounds.

DPMA received similarly strong feedback, with the single respondent rating navigation through controls and measures and identification of the maturity level at 5/5. Labels and buttons were considered easy to understand, navigation was rated extremely easy, overall UX reached 5/5, and recommendation likelihood was 10/10. Although the single-response sample limits the generalisability of these results, they are consistent with the positive DPMA usability results observed in the structured Athens and Zagreb workshops and provide additional confirmation of the tool's accessibility for non-specialist users.

The single DPRA response also confirmed positive usability characteristics. Navigation through controls and measures was rated 5/5, identification of the maturity level 4/5, and labels and buttons were considered easy to understand. The respondent successfully identified relevant threats and corresponding mitigation controls, while overall UX was rated 4/5 and recommendation likelihood 8/10. Given the single respondent, these results are considered indicative, but they remain consistent with the generally positive DPRA results recorded during previous validation events.

No new improvement requests were recorded during the BEYOND activity. This is notable when considered alongside the feedback-driven refinement cycle implemented throughout WP3: by this stage of the validation campaign, the tools had undergone several rounds of usability and interface improvements, and the absence of additional concrete issues in this exhibition-based setting provides a positive indication of their increasing maturity. At the same time, the lack of improvement requests should not be interpreted as evidence that no further refinement is required, particularly given the limited sample sizes for three of the four evaluated tools.

Overall, the BEYOND validation activity complemented the structured CURIUM workshops by testing the tools in an informal, real-world exhibition environment and exposing them to a broader technology and innovation audience. The consistently positive results, particularly for CyReA and CAC, reinforced the validation findings accumulated across the preceding events and provided additional evidence that the Compliance Continuum tools can be understood and operated by users without specialised cybersecurity expertise. The activity also strengthened the project's validation and exploitation evidence by demonstrating that the tools can generate positive engagement when presented directly to potential users in an open technology ecosystem.

7 Final Capacity Building and Support Outcomes

Section 7 presents the final outcomes of Task 3.4, which focuses on knowledge and capacity-building activities supporting the CURIUM Compliance Continuum. In accordance with the Grant Agreement, T3.4 covers the creation and integration of training and knowledge resources, as well as experimentation, testing, training, consulting and other activities aimed at strengthening stakeholder capacity and supporting the effective use of the CURIUM services.

7.1 Cyber Range CRA Training

An interactive online training programme has been designed with the aim to provide structured awareness and practical understanding of the EU Cyber Resilience Act (CRA), focusing on scope determination, essential cybersecurity requirements, vulnerability handling, incident reporting obligations, and lifecycle responsibilities. The programme titled Cyber Resilience Act (CRA) Compliance and Awareness is being delivered through the Sphynx Cyber Range platform. Through scenario-based training questions and a formal assessment, participants can strengthen their ability to interpret regulatory obligations and apply secure-by-design and secure-by-default principles in practical contexts.

The goal of this programme is to enable Small and Medium-sized Enterprises (SMEs), and other users to understand and apply key compliance obligations, strengthen vulnerability management and incident reporting practices, and support structured CRA adoption across the digital supply chain. The programme structure involves a scenario outline, associated roles and skills, and a comprehensive set of training and assessment questions.

The outlined scenario guides participants through the essential aspects of the EU Cyber Resilience Act (CRA). Using realistic examples, training questions, and a final assessment, participants explore how to determine whether their products, software, or activities fall within the scope of the CRA and understand key cybersecurity obligations. The scenario aims to raise CRA awareness among users and Small and Medium-sized Enterprises (SMEs), support informed compliance decisions, and strengthen the adoption of robust cybersecurity practices throughout the digital supply chain. The programme equips trainees with practical knowledge to identify CRA applicability, handle vulnerabilities responsibly, and ensure regulatory alignment.

The training material has been produced based on the EU Cyber Resilience Act (CRA) Official - <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act> and the European Commission CRA Implementation - <https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation>.

The material includes 26 Training Questions and 16 Assessment Questions structured in the following sections:

1. CRA Fundamentals
2. Products Classification and Scope
3. Essential Cybersecurity Requirements
4. Economic Operators and Obligations
5. Conformity Assessment
6. Technical Documentation
7. Vulnerability Handling
8. Product Lifecycle
9. Supply Chain and Third-Party Components
10. Regulatory Compliance and Market Surveillance.

Associated Roles include:

- Software Developer (NIST NICE)
- Information Systems Security Developer (NIST NICE)
- Cyber Instructor (NIST NICE)
- Information Systems Security Manager (NIST NICE)
- Vulnerability Assessment Analyst (NIST NICE)
- Level 2 Risk Management (ECF)
- Level 3 Risk Management (ECF)
- Level 2 Information Security Management (ECF)
- Level 3 Information Security Management (ECF)
- Level 2 Education and Training Provision (ECF)
- Level 3 Education and Training Provision (ECF)

Associated Skills

- Cybersecurity Fundamentals (Theoretical)
- Vulnerability Assessment and Management (Theoretical)
- Incident Response (Defensive)
- Security Policies and Standards (Theoretical)
- Software Development (Theoretical)
- Systems Analysis (Theoretical)
- Training, Education, and Awareness (Theoretical)

The programme has been promoted through the CURIUM validation workshops and stakeholder engagement activities conducted within the project. Following the workshops, participants were invited through email to access the training on the Sphinx Cyber Range platform. A total of 82 invitations were issued, of which 77 were successfully delivered to recipients. Each participant received a personal license key, along with detailed registration and platform access instructions. The training was offered through a 30-day license period, enabling participants to complete the programme within a defined timeframe following their workshop participation. Overall, 17 recipients actually registered in the Cyber Range Platform and completed the CRA Training Programme.

The programme is implemented within the Sphinx Cyber Range environment and delivered to registered trainees through a structured online process. Initially, a content creator designs the Cyber Resilience Act (CRA) awareness training scenario through the Sphinx Cyber Range graphical user interface (GUI), defining the learning objectives, associated roles and skills, training material, bibliography sources, and training/assessment content. The scenario is then incorporated into a dedicated training programme, where participants are assigned and granted access through individual license keys.

A shortened version of the Cyber Resilience Act (CRA) Compliance and Awareness training programme has been also integrated within the CURIUM Continuum Portal, <https://curium-project.eu/portal/>, and has become part of the CURIUM offering in the CRA domain, providing interested stakeholders with continuous access to selected training materials, which can be undertaken and revisited as often as required to support CRA awareness and knowledge development.

7.2 Capacity Building and Stakeholder Support Activities

The CURIUM's capacity building strategy and plan unfold along the pillars of a./ training, b./ experimentation and testing, c./ consulting and support activities, d./ awareness and knowledge transfer, e./ collaboration and sustainability. All relevant activities aimed at engaging a broad spectrum of stakeholders across the targeted ecosystem that includes SMEs, industry, security services/tools providers, policy makers, authorities, academia, general public. These activities contribute to raising awareness, strengthening competencies, and fostering knowledge exchange.

7.2.1 Training - Capacity Building Workshops and Webinars

CURIUM organized and/or contributed to the design and implementation of numerous workshops, webinars and innovation events, as the project's main modalities for training and capacity building in addition to the on-line interactive, cyber range, training on the CRA. Brief description of such workshops and webinars follow. Some of them were co-organised with sister projects because of the project's clustering efforts.

Workshops



The project was presented at the **Patras IQ 2026** with a workshop on the 28th of February 2026, titled **“CRA & CSA: Mandatory Cybersecurity Requirements for Digital Products in the EU - The Deadline is Approaching.”** The event was organized by partner p-NET and supported by the CURIUM, SAND5G and CUSTODES EU Projects. The session, led by Iro Chatzopoulou (API) and Kostas Lambropoulos (p-NET), addressed the evolving European regulatory landscape, including the Cyber Resilience Act (CRA) and Cybersecurity Act (CSA), and their implications for manufacturers, service providers, and digital product developers. It provided participants with practical insights into compliance requirements, risk management approaches, and the broader impact of cybersecurity regulation on innovation and market readiness. This event was attended by approximately 50 people.

Link to CURIUM website: <https://curium-project.eu/patras-iq-2026-cra-csa-mandatory-cybersecurity-requirements-for-digital-products-in-the-eu-the-deadline-is-approaching/>



On February 13th, 2026, an interactive workshop titled **“Risk Assessment & Incident Response”** was jointly organised with the SAND5G project. The session, led by experts from APIROPLUS SOLUTIONS Ltd., provided participants, mainly researchers and engineers from the University of Patras and p-NET, with practical guidance on conducting risk assessments, preparing for and managing cybersecurity incidents, and addressing real-world challenges through hands-on exercises. The workshop demonstrated how structured risk assessment and incident response practices

support organisations in navigating complex cybersecurity environments and contribute to the secure deployment of next generation 5G networks. The workshop was attended by 15 participants.

Link to CURIUM website: <https://curium-project.eu/risk-assessment-incident-response/>



The **“Preparing Stakeholders for CRA Compliance”** event was successfully hosted by the Office of the Commissioner of Communications – Digital Security Authority in Nicosia, Cyprus, on December 11th, 2025. The event introduced participants to the CURIUM Project, showcasing how it supports the implementation of the Cyber Resilience Act (CRA). Throughout the sessions, tools currently in development were presented. These tools are designed to help stakeholders Understand regulatory obligations, identify compliance gaps and take necessary steps to

align with the CRA. By leveraging these resources, organizations can start their preparations early, strengthen compliance strategies, and improve their approach to managing cyber resilience in practice. The event concluded with a live demonstration and hands-on session led by project partners, providing participants with the opportunity to explore and interact directly with the tools.

Link to CURIUM website: <https://curium-project.eu/preparing-stakeholders-for-cra-compliance/>



As part of the **Cyber Resilience and Security Workshop at Techritory 2025** in Riga, which was held on October 23rd, our team had the opportunity to present the CURIUM suite of innovative tools designed to support cybersecurity certification and compliance across Europe. During the workshop, Kristian Ravic, Project Manager at Cyber Security Ltd., provided an overview of the CURIUM Project, outlining its role in developing innovative platforms, tools, and services that guide businesses through the complexities of

cybersecurity certification. Dr. Admir Jukan, Senior Project Manager at Cyber Security Ltd., introduced the Conformity Assessment and Compliance (CAC) Tool, showcasing how it helps SMEs manage their compliance

journey – from initial readiness checks to ongoing post-market monitoring. The tool enables automated self-assessment with clear visualisation of requirements, helping users identify gaps and strengthen regulatory readiness. Christos Kargatzis, Software Engineer at AEGIS IT Research, presented the Penetration Self-Testing and Vulnerability Assessment (PSTVA) Tool, highlighting its contribution to CURIUM’s mission of supporting cybersecurity validation and assurance.

The workshop also featured contributions from the [NATWORK](#), [SAND5G](#), and [CUSTODES](#) EU projects, highlighting the importance of collaborative European research and innovation in building a trusted and secure digital future for Europe. This event was attended by approximately 30 participants.

Link to CURIUM website: <https://curium-project.eu/showcasing-the-curium-project-at-techritory-2025/>



The **“Prepare Your SME for EU Cyber Rules”** workshop, presented by Iro Chatzopoulou (Apiroplus Services) and Esther Garrido (28 Digital) was successfully held as a joint webinar with SME4DD. The session focused on raising awareness among SMEs about the Cyber Resilience Act (CRA) and its implications. While the event primarily aimed to inform participants about the

upcoming EU cyber regulations, it also served as a valuable training opportunity, helping businesses understand how to prepare for compliance and strengthen their cybersecurity frameworks.

Link to CURIUM website: <https://curium-project.eu/prepare-your-sme-for-eu-cyber-rules/>



The **Madrid TechConnect Funding Opportunities Workshop**, hosted by EIT Digital on 23 September 2025, was a training event focused on supporting startups and scaleups in Madrid in accessing European funding opportunities. Co-financed by the European Regional Development Fund and the Comunidad de Madrid, the workshop provided practical guidance on EU funding mechanisms, eligibility criteria, and strategies for securing financial support. The event reached key stakeholders across the Madrid innovation ecosystem, including entrepreneurs, startups, corporations, universities, and research centres. During the workshop, 28D presented the challenges introduced by the Cyber Resilience Act (CRA) and highlighted the opportunities offered by the CURIUM project, particularly in terms of training and support for organisations navigating the evolving cybersecurity regulatory landscape.

Link to CURIUM website: <https://curium-project.eu/madrid-techconnect-funding-opportunities-workshop/>



The interactive cybersecurity workshop **“Think Before You Click! To Hackers, the Easiest Target is You!”**, organized by partner p-NET on May 17th at the University of Patras Conference Center, was a great success. The workshop was organized with the support of the CURIUM Project, alongside fellow EU-funded initiatives [SAND5G EU project](#) and [CUSTODES EU Project](#). CURIUM’s mission to promote cybersecurity awareness and resilience in digital environments was strongly reflected throughout the session. In addition to the

workshop, p-NET hosted an interactive booth where visitors could ask questions and learn more about EU-funded cybersecurity efforts. The CURIUM Project’s flyers were distributed to interested attendees, offering insights into how the project is contributing to a more secure and resilient digital future.

Link to CURIUM website: <https://curium-project.eu/tedx-workshop-think-before-you-click/>

Webinars



“The EU AI Act & EU-Funded Research Projects: Implications, Challenges, and Good Practices” webinar was designed to provide an accessible introduction to the EU AI Act, while exploring its implications, key challenges, and good practices for EU-funded research projects developing or deploying AI systems. The webinar was held on-line on Thursday, 7 May 2026 at 13:30 – 16:05 CET. It was

organized by Eunomia Ltd in collaboration with Tilburg Institute for Law, Technology, and Society (TILT) and APIROPLUS SERVICES Ltd., and supported by the CURIUM, SYNAPSE, CONSENTIS, and PANDORA Horizon Europe Projects.

Link to CURIUM website: <https://curium-project.eu/curium-participates-in-online-workshop-the-eu-ai-act-and-eu-funded-research-projects/>



The “**Cybersecurity through the lens of EU Policies and Regulations**” webinar explored how the latest EU policies and regulations are reshaping cybersecurity, AI governance, digital identity, privacy, and trusted connectivity across Europe. It was held on-line on June 3rd, 2026. The webinar brought together an exceptional panel of leading experts and thought leaders: Prof. Dr. Eleni Kosta - Professor of Technology, Law & Human Rights at Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Prof. [Lilian Mitrou](#) – Professor - [University of the Aegean](#), Lawyer, Vice President of the National Commission for Bioethics and Technoethics, Argyro (Iro) Chatzopoulou - Senior Cybersecurity Advisor and Co-founder of APIROPLUS SERVICES, Dr. Thanassis Staveris - Senior Cybersecurity Specialist at p-NET Emerging Networks & Vertical Applications. Key topics included:

- EU Digital Identity Wallet & GDPR
- AI Act implications for organizations
- Cybersecurity Act (CSA) & Cyber Resilience Act (CRA)
- Turning EU Cybersecurity Policy into Operational Assurance

The session offered practical insights into the policies, obligations, risks, and opportunities shaping Europe’s digital future - highly relevant for cybersecurity professionals, legal and compliance experts, ICT stakeholders, researchers, policymakers, SMEs and organizations navigating the new regulatory environment, and to anyone else who may be interested. The webinar attracted 54 participants.

Link to CURIUM website: <https://curium-project.eu/cybersecurity-through-the-lens-of-eu-policies-regulations/>

Internal Trainings

Last but very important, the project organized and implemented a series of **internal trainings** aiming towards the awareness raising and up-skilling of partners’ staff. The internal trainings included:

1. A first introduction to the CURIUM tools to selected staff of the project partners took place on-line on the 4th of November 2025, whereby partners CYS and NLG presented their tools, CAC and CyReA/DPRA. Tool owners collected feedback from the participants towards further enhancing their tools in the best possible way. Its duration was 90 minutes and was attended by 10 members of the partners’ staff.
2. A follow up internal training was organized on-line on the 11th of November 2025, whereby partners AEGIS and APPS presented their tools, PSTVA and DPMA, to project partners. Tool owners collected feedback from the audience towards enhancing their tools. The duration of the internal training was 90 minutes and was attended by 10 members of the partners’ staff.

3. On the 10th of December 2025, all tool owners presented their tools to the members of staff of the DSA. The internal training took place physically at the ICT Academy Nicosia, in Cyprus. The training session lasted 90 minutes and there were 10 participants from the DSA.

7.2.2 Collaboration and Sustainability

CURIUM has joined the CyberHubs European Network as an Associated Project. CyberHubs, <https://cyberhubs.eu>, is a three-year Erasmus+ project coordinated by DIGITALEUROPE that has established a network of seven Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, bringing together industry, academia, policymakers, and training providers.

Each CyberHub has identified national cybersecurity skills needs and developed country-specific strategies to address them. Together, the Hubs are strengthening Europe's cybersecurity skills ecosystem and helping address the growing shortage of cybersecurity professionals through innovation, knowledge sharing, and talent development.

As an Associated Project, CURIUM has been exchanging expertise, promoting skills development initiatives, amplifying project results, and contributing to a stronger and more resilient European cybersecurity community.

7.2.3 CRA Guidance and Knowledge Transfer for Stakeholders

As part of the CURIUM project's knowledge and capacity-building activities, the DSA developed a practical guide on the CRA in collaboration with the Cyprus National Coordination Centre - Working Group 4: EU and National Legislations.

The guide supports the project's objectives by raising awareness and visibility of the CRA among relevant stakeholders, including businesses, software developers, importers, distributors, public bodies, consumers and conformity assessment bodies. It also contributes to knowledge transfer within the national cybersecurity ecosystem by translating key regulatory concepts into accessible, practical information.

Through this activity, the project strengthens stakeholder engagement, promotes early preparedness for upcoming CRA obligations, and supports the wider dissemination of cybersecurity knowledge and compliance-related resources. The guide has been made publicly available through the following webpages:

<https://ncca.cy/cyber-resilience-act-cra-guide-cyprus/>

[Cyber Resilience Act - Manufacturers | Shaping Europe's digital future](#)

[CRA Guide – Curium Project](#)

7.2.4 Experimentation and Testing

The project utilizes the p-NET Testing and Experimentation Facility (TEF), an integrated, fully functional smart network environment designed for comprehensive end-to-end validation of network functions, services, and performance. Operating under "Testbed as a Service" and "Bring Your Own Use Case" models, the TEF serves as a vital resource for knowledge transfer and capacity building among project stakeholders.

Key capabilities and supported experimental categories include:

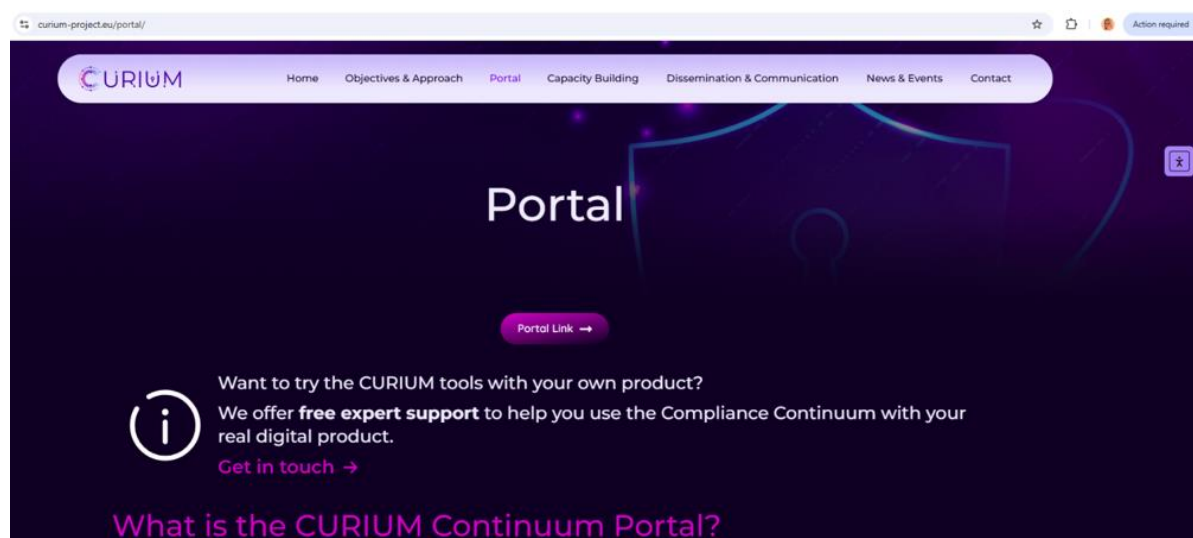
- **Core TEF Capabilities:** Vendor conformance and interoperability testing (aligned with 3GPP and EU cybersecurity guidelines), new feature/service development, KPI and cybersecurity assessments, and hands-on training for regulators, operators, and researchers.
- **Traffic & Anomaly Observation:** Monitoring workload patterns, system responses to congestion, usage deviations, and concurrent service interactions.

- **Resilience & Incident Handling:** Evaluating infrastructure recovery, fault tolerance under partial failures, misconfiguration responses, and alerting workflow validation.
- **Vertical & Multi-Stakeholder Testing:** Assessing sector-specific application requirements, real-time data services (telemetry/video), and shared resource dynamics in multi-actor digital environments.

The TEF is being promoted to the CURIUM ecosystem, as a complementary support service for testing and validation purposes. Relevant LinkedIn Post https://www.linkedin.com/posts/curium-project_curium-pnet-smes-activity-7475474257330958336-wOtE

7.2.5 Consulting and Support Services

CURIUM's consulting and support services mainly target the prospective users of the CURIUM Compliance Continuum Portal. They include on-line user manuals that provide a stepwise guide to the use of the tools of the continuum, relevant videos, as well as the capability of users to receive free consulting by tool experts on the use of the Compliance Continuum with the user's own real digital project. The relevant consulting and support services are being promoted through the project's website, social media and YouTube channels.



In addition, p-NET provides an Open-Door Consultation & Mentoring service for SMEs, start-ups, manufacturers, end users, and anyone else who is interested. The CURIUM Helpdesk is established at the Patras Science Park, where interested stakeholders are given the opportunity to:

1. Understand the scope of the CRA and when it applies to their products;
2. Learn the key requirements for compliance;
3. Explore how CURIUM tools and services can support their business;
4. Be connected with the right experts for further consultation.

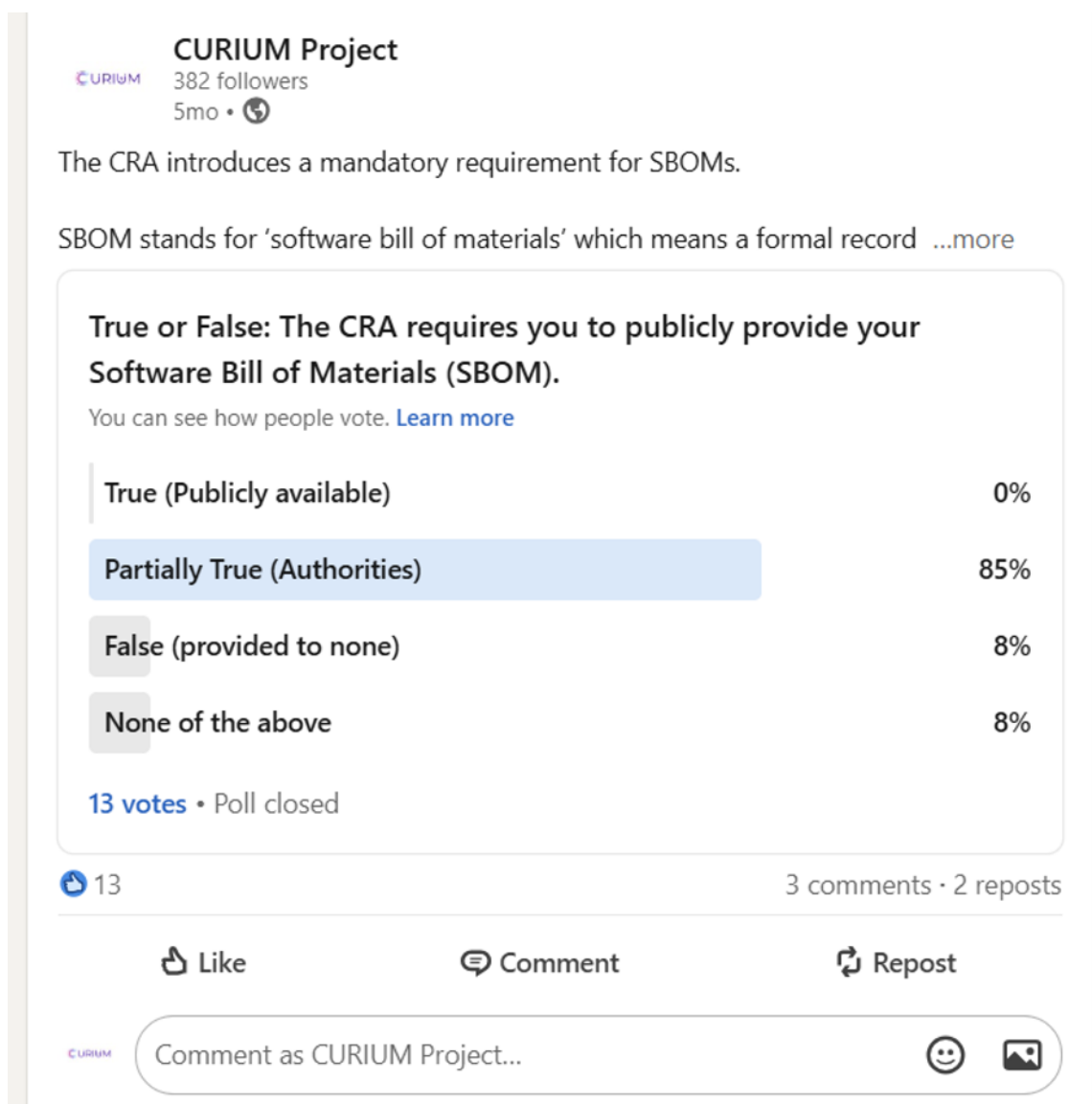
Link to CURIUM website: <https://curium-project.eu/helpdesk/>

7.2.6 LinkedIn Awareness Campaign

As part of its capacity-building activities, the CURIUM project implemented a structured LinkedIn awareness campaign based on interactive polls designed to promote understanding of the Cyber Resilience Act (CRA). From 27 January 2026 to date, 15 polls have been published, each presenting a practical regulatory question followed by an explanation of the correct answer and its implications.

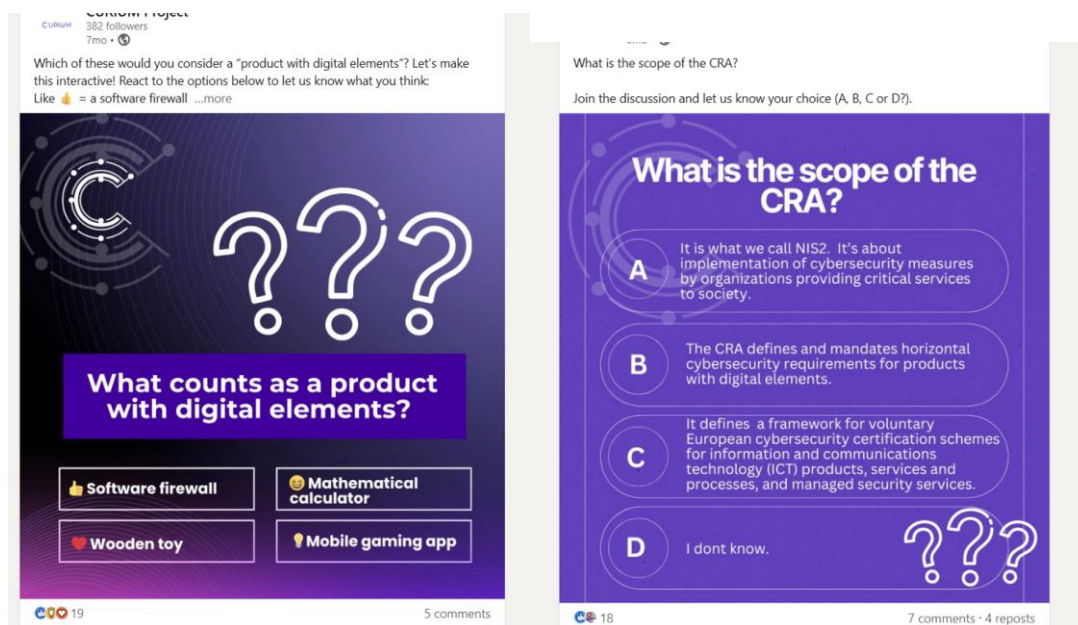
To ensure relevance for different stakeholder groups, the campaign was organised into three thematic segments: Developers & Product Managers, focusing on technical implementation; C-Level Executives & Founders, addressing business and strategic implications; and Legal & Compliance Officers, covering regulatory interpretation and compliance obligations. This segmented approach enabled the delivery of targeted knowledge to audiences with different roles and responsibilities.

One illustrative example focused on Software Bills of Materials (SBOMs). The poll asked participants whether the CRA requires manufacturers to publicly provide their SBOMs. While many practitioners assume that public disclosure is mandatory, the explanation clarified that the SBOM forms part of the technical documentation made available to market surveillance authorities and conformity assessment bodies, while manufacturers may decide whether to share it with users. The post also highlighted additional considerations relating to open-source software, demonstrating the complexity of applying the regulation in practice.



The LinkedIn poll series provided an effective mechanism for translating complex regulatory requirements into concise, practical learning opportunities. By encouraging participation and then explaining the correct interpretation, the campaign supported continuous knowledge transfer, raised awareness of the CRA, and complemented CURIUM's wider dissemination and capacity-building activities.

In addition to the LinkedIn polls, CURIUM also published a series of question-based awareness posts designed to test stakeholders' understanding of key CRA concepts. These posts encouraged reflection and discussion by presenting practical compliance scenarios and multiple-choice questions, helping to reinforce knowledge and stimulate engagement with the regulation in an accessible format.



Activities related to the capacity building pillars of awareness and knowledge transfer, and collaboration and sustainability, given their alignment with dissemination, stakeholder engagement, and outreach objectives, have been implemented in close collaboration with the impact maximization activities of WP5 and are reported in deliverable D5.2.

7.3 Evaluation of Capacity Building KPIs

In the present section we provide an evaluation of the status of Capacity Building KPIs.

TABLE 4. EVALUATION OF CAPACITY BUILDING KPIs #1

KPI-ID	Capacity Building KPI #1
Name	Internal Trainees
Description	Number of internal trainees trained within partner organizations to become familiar with the CURIUM training tools.
Responsible partner(s)	PNET
Goal	≥10
Means of verification	3 internal training sessions organized, each involving 10 trainees, as reported in Section 7.2.1.
Status	Completed
What is missing	No further actions required

TABLE 5. EVALUATION OF CAPACITY BUILDING KPIs #2

KPI-ID	Capacity Building KPI #2
--------	--------------------------

Name	Training provided
Description	Number of trainings provided by CURIUM (external, from consortium members or developed inside the project)
Responsible partner(s)	PNET
Goal	>10
Means of verification	1 on-line, interactive training course through the cyber-range environment, 1 on-line interactive training course through the compliance continuum portal (presented in Section 7.1), 7 workshops, 2 webinars (presented in sub-section 7.2.1). Evidence for the delivery of each of the above includes the course syllabus, workshop and webinar agendas, recordings, presentations, photos, promotion material and lists of participants. Additional training activities include the CRA Guide (subsection 7.2.3), and the continuous LinkedIn awareness campaigns (subsection 7.2.6),
Status	Completed
What is missing	No further actions required.

TABLE 6. EVALUATION OF CAPACITY BUILDING KPIs #3

KPI-ID	Capacity Building KPI #3
Name	Workshops, training sessions and events for European SMEs
Description	Number of workshops, training sessions, and events that facilitate interaction and CRA compliance among European SMEs; 25-100 participants each; ≥40% of the participants in each event attracted and registered as contacts.
Responsible partner(s)	PNET
Goal	≥3
Means of verification	Such events and workshops relate to the project's validation activity and are described in detail in deliverable D4.1. They are also described in subsection 6.2 of the present document and include: • The Riga Validation Workshop (10/2025) • The Nicosia Validation Workshop (12/2025) • The Athens Validation Workshop (3/2026) • The Zagreb Validation Workshop (4/2026) • Nicosia "Skills" validation workshop (6/2026) • BEYOND validation workshop (6/2026)

Status	Completed
What is missing	No further action required.

8 Conclusions (AEGIS)

This deliverable presents the final release and operational outcomes of the CURIUM Compliance Continuum and reports the results achieved across the activities of WP3. It documents the transition of the CURIUM ecosystem from successive development and validation iterations towards a stable, integrated and operational solution supporting organisations, and in particular SMEs and micro-enterprises, in addressing the requirements of the Cyber Resilience Act (CRA).

The final release consolidates the five core CURIUM services — CyReA, DPRA, DPMA, PSTVA and CAC — within the CURIUM Portal, supported by a common production environment, centralised authentication, containerised deployment and established mechanisms for maintenance and future updates. The final v1.2 environment incorporates the technical and functional improvements implemented throughout the project, strengthening the usability, accessibility, consistency and operational robustness of the individual tools and their overall integration within the Compliance Continuum.

A key outcome of the final development phase has been the systematic integration of stakeholder feedback into the evolution of the CURIUM services. Through the Feedback-to-Action Tracker, observations collected during the WP4 validation activities were systematically recorded, prioritised, assigned and translated into concrete technical and usability actions. This process ensured traceability between identified user needs, implemented refinements and final releases. The resulting improvements addressed recurring requirements for clearer guidance, simplified workflows, improved visualisation, greater accessibility for non-expert users, enhanced deployment flexibility and improved cross-tool usability. The progressive refinement of the tools demonstrates that validation was used as an active input to development rather than solely as a final assessment activity.

In parallel, the CURIUM ecosystem established the knowledge and capacity-building dimension. Training resources, including the CRA Compliance and Awareness programme delivered through the Sphynx Cyber Range and the training content integrated into the CURIUM Portal, complement the technical services by providing users with the knowledge required to understand CRA obligations and make effective use of the Compliance Continuum. The broader programme of workshops, webinars, experimentation and testing, consulting and support activities, knowledge-transfer initiatives and stakeholder engagement further contributed to strengthening CRA awareness and practical cybersecurity capabilities among SMEs, industry stakeholders, researchers, policymakers and other relevant actors. The achievement of the capacity-building KPIs confirms the successful implementation of the relevant planned activities.

The final WP3 outcomes also establish the foundations for the continued operation and evolution of the CURIUM ecosystem beyond the project lifetime. The DevOps-oriented production approach, supported by automated CI/CD processes and containerised services, facilitates controlled maintenance, security updates and future functional enhancements. At the same time, the availability of training, documentation, support mechanisms and reusable knowledge resources supports continued adoption and exploitation of the CURIUM services by external stakeholders.

Overall, the activities reported in this deliverable demonstrate that CURIUM has progressed from the development of individual compliance and cybersecurity tools to a coherent and operational Compliance

Continuum combining **technical assessment, risk management, maturity assessment, vulnerability testing, conformity assessment, training and stakeholder support** within a unified ecosystem. The final release reflects the lessons learned through iterative stakeholder engagement and validation, while the operational and capacity-building foundations established through WP3 provide the basis for continued use, maintenance, exploitation and future evolution of the CURIUM solutions beyond the end of the project.