Cra s**U**ppo**R**t cont**I**nu**UM**

D3.1 - Continuous release of tools and services and support for training, knowledge, and capacity building

Document Summary Information

Grant Agreement No	101190372	**Acronym**	CURIUM
Full Title	Cra sUppoRt contInuUM		
Start Date	01.01.2025	**Duration**	18 months
Project URL	www.curium-project.eu		
Deliverable	D3.1: Continuous release of tools and services and support for training, knowledge, and capacity building.		
Work Package	WP3: Development and release of CURIUM Compliance Continuum.		
Contractual due date	31.12.2025	**Actual submission date**	29.12.2025
Nature	DEM	**Dissemination Level**	PU - Public
Lead Beneficiary	Cyber-security, d.o.o. ZA SAVJETOVANJE		
Responsible Author	Miroslav Baca, Cyber-security, d.o.o. ZA SAVJETOVANJE		
Contributions from	All partners		

The project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre ('granting authority'), under the powers delegated by the European Commission ('European Commission'). under the Grant Agreement No. 101190372. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Revision history (including peer reviewing & quality control)

Version	Date	Author	Notes
0.1	12/07/2025	CYS	Initial Table of Contents and assignment of activities and sections to partners
0.2	02/09/2025	CYS	Executive Summary, Introduction, Chapter 3, Abbreviation
0.3	10/12/2025	All partners	All partners contribution to all chapters
0.4	13/12/2025	All partners	All partners contribution to all chapters
1.0	19/12/2025	CYS	Final Draft – most of comments are solved, missing input added
1.1	19/12/2025	AEGIS	Review
1.2	28/12/2025	CYS	Quality Assurance and Final Version

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Table 1 Abbreviations

Abbreviation	Description
CRA	Cyber Resilience Act
CyReA	Cyber Resilience Assessment
DPRA	Digital Product Risk Management
DPMA	Digital Product Maturity Assessment
CAC	Conformity Assessment and Compliance
PSTVA	Penetration Self-Testing and Vulnerability Assessment
DoC	Declaration of Conformity
SSO	Single Sign-On
CI/CD	Continuous Integration / Continuous delivery/deployment
CVE	Common Vulnerability Exposure
NVD	National Vulnerability Database
MISP	Malware Information Sharing Platform
SME	Small and Medium Enterprises
CE	Conformité Européenne
CC	Common Criteria
SBOM	Software Bill of Material
EAL	Evaluation Assurance Level
TRL	Technology Readiness Level

1. Executive Summary

Deliverable D3.1, "Continuous Release of Tools and Services and Support for Training, Knowledge, and Capacity Building", reports on the outcomes of WP3 during the initial development and release phase of the CURIUM Compliance Continuum.

The objective of WP3 is to prepare, deploy, refine, and support a comprehensive set of tools and services that enable European SMEs and micro-enterprises to achieve compliance with the Cyber Resilience Act (CRA).

The deliverable documents describe implementation of four major tasks:

- **T3.1 Adaptation of mature tools and systems to include in the CURIUM Compliance Continuum** to form the core services of the CURIUM Compliance Continuum, including 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). These tools have been customized and aligned with CRA essential requirements, focusing on usability for SMEs.
- **T3.2 Deployment of CURIUM services and tools to support CRA implementation**, ensuring availability of the tools in a unified framework and setting up the release processes that allow continuous integration and incremental improvements.
- **T3.3 Continuous feedback collection and refinements for CURIUM Compliance Continuum**, establishing the mechanisms to gather structured feedback from validation activities (WP4) and SMEs, and translating these into iterative refinements of the tools and overall Continuum.
- **T3.4 CURIUM support, knowledge and capacity building**, developing the necessary non-technical resources, including training material, user guides, and support services to facilitate the adoption of the CURIUM tools.

The deliverable is linked to MS 9, MS 10 and MS 11. The outcomes presented in this deliverable include the first consolidated release of the CURIUM Compliance Continuum, the definition of the implemented requirements, Curium portal (landing page), a set of SME-tailored training and support resources, and the establishment of a feedback loop for continuous improvement. The deliverable demonstrates how CURIUM contributes to the strengthening of cyber resilience in Europe, by providing practical instruments for compliance and building the capacities of SMEs to manage cybersecurity risks effectively.

2. Introduction

This deliverable, D3.1 Continuous Release of Tools and Services and Support for Training, Knowledge, and Capacity Building, provides the first consolidated report of the work performed under Work Package 3 (WP3) of the CURIUM project. It presents the methodology, results, and outputs achieved so far in the development and release of the CURIUM Compliance Continuum, as well as the supporting training and knowledge resources aimed at enhancing the cybersecurity capacities of European SMEs and micro-enterprises.

WP3 represents the core technical implementation phase of the project, where the various tools and services developed and adapted by consortium partners are progressively aligned, deployed, and continuously improved in response to stakeholder needs and regulatory requirements. This deliverable marks an important milestone

by documenting the first release of the tools and related services, along with the foundations for feedback-driven refinement and capacity-building activities.

2.1 Objective of WP3

The primary objective of WP3 is to design, deploy, and refine the CURIUM Compliance Continuum, a set of services and resources that support SMEs in achieving compliance with the Cyber Resilience Act (CRA). Specifically, WP3 aims to:

- Define and adapt the components/modules of the Compliance Continuum and prepare them for validation (O3.1).
- Identify and incorporate missing elements, ensuring future possible interoperability with both internal modules and external services (O3.2).
- Build the technical backbone of the Continuum, enabling its deployment and use for training, knowledge, and capacity-building activities (O3.3).
- Develop non-technical resources such as training materials, courses, helpdesk services, and support tools to ensure adoption by SMEs (O3.4).
- Through these objectives, WP3 ensures that the project delivers not only innovative technical solutions but also practical resources that enhance user capacity to meet CRA compliance obligations.

Table 2 Objective mapping with the Chapters in deliverable

WP3 Objective	Coverage in D3.1
O3.1 – Define/adapt Continuum components	Chapters 3,4
O3.2 – Interoperability & missing elements	Chapters 3, 5
O3.3 – Technical backbone & deployment	Chapter 5
O3.4 – Training, support, capacity building	Chapter 7

2.2 Relation to overall CURIUM goals and CRA compliance (to the WP2)

WP3 plays a pivotal role in operationalizing the overall vision of CURIUM: providing SMEs with a compliance continuum that simplifies regulatory alignment, strengthens resilience, and fosters trust in digital products and services. While WP2 focuses on mapping legal and regulatory requirements and translating them into functional and technical requirements, WP3 transforms these insights into concrete tools and services.

The outputs of WP3 ensure:

- Alignment with CRA Annexes (technical documentation, DoC, fulfilling the requirements, etc.).
- Practical implementation supports SMEs, turning regulatory requirements into actionable, tool-driven processes.
- Synergy with WP4 validation activities, ensuring that the tools meet real-world compliance needs as tested by external stakeholders.

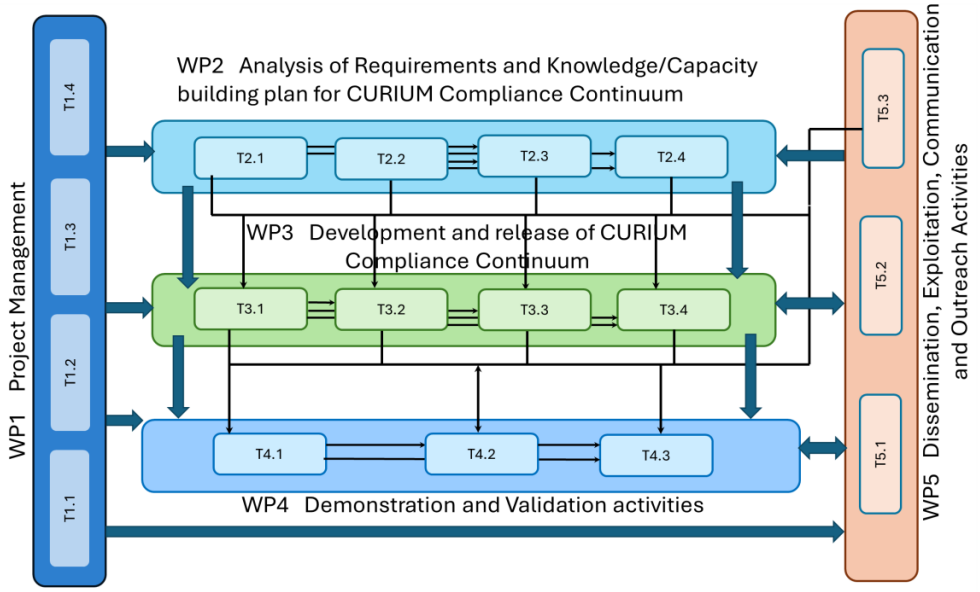


Figure 1 CURIUM PERT

Figure 1 shows a connection between WPs, where WP3 acts as the bridge between regulatory analysis (WP2) and real-world deployment and validation (WP4), ensuring that CURIUM contributes effectively to Europe's cybersecurity resilience and the adoption of the CRA. Figure 2 depicts an interplay between stakeholders.

WP2 legal requirements were translated into functional requirements directly implemented in the CURIUM tools.

The system requirements defined in Deliverable D2.2, Section 5.3 (Table 7 – Curium Requirements), are implemented through the CURIUM tools released under WP3. A detailed requirement-to-tool traceability table is provided in Annex II.

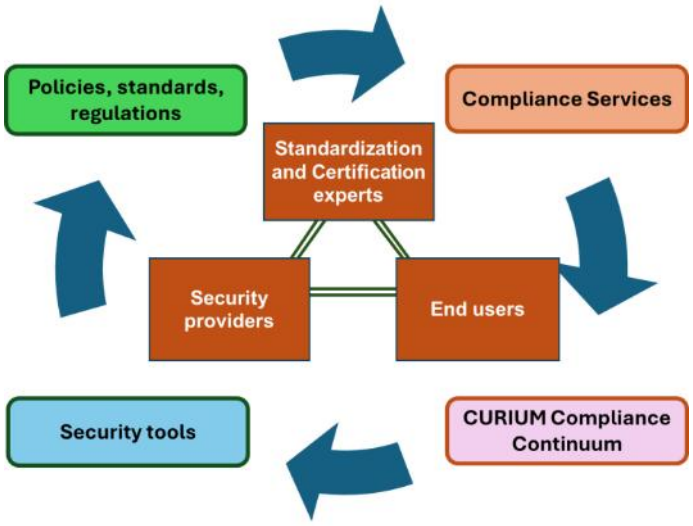


Figure 2 Triangle of the key actors in the project

2.3 Structure of the deliverable

This deliverable is structured as follows:

- Chapter 1 introduces the objectives and scope of the deliverable.
- Chapter 2 provides background information on the project context, WP3 objectives, and the relationship of this deliverable with other work packages.
- Chapter 3 describes the adaptation and integration of the CURIUM Compliance Continuum components.
- Chapter 4 presents the implemented tools and services that constitute the Compliance Continuum.
- Chapter 5 outlines the deployment strategy, release process, and mapping of deployed tools to the relevant Cyber Resilience Act (CRA) annexes.
- Chapter 6 describes the framework for continuous feedback collection and refinement.
- Chapter 7 presents the capacity-building, training, and support activities carried out under WP3.
- Finally, the conclusion summarizes the main outcomes of the deliverable and outlines the next steps.
- Annex I and Annex II provides a detailed mapping between the CURIUM tools and the relevant CRA requirements, as well as requirements described in D2.2.

3. CURIUM Compliance Continuum

3.1 Definition and rationale of the Compliance Continuum

The **CURIUM Compliance Continuum** is defined as a modular, end-to-end framework designed to enable European SMEs to achieve, demonstrate, and sustain conformity with the **Cyber Resilience Act (CRA)** and related EU regulatory obligations. The Continuum integrates risk-based methodologies, modular technical tools, and capacity-building services into a coherent compliance pathway, while preserving flexibility to adapt to diverse SME contexts and sectoral needs.

The rationale for establishing the Compliance Continuum stems from the increasing complexity of cybersecurity regulations and the disproportionate burden these impose on SMEs with limited resources. By providing a structured yet adaptable compliance pathway, the Continuum enables organizations to:

- **Systematically address CRA requirements** across the entire digital product lifecycle.
- **Facilitate CE marking** by documenting conformity with essential cybersecurity requirements.
- **Ensure proportionality and scalability**, allowing SMEs to select relevant tools and modules based on product criticality, organizational maturity, and regulatory exposure.
- **Support regulatory coherence**, ensuring alignment with CRA
- **Promote trust and transparency** by generating verifiable compliance evidence and reporting outputs suitable for both internal governance and external auditing processes.

Thus, the Compliance Continuum represents both a **conceptual compliance pathway** and a **practical ecosystem of tools and services**, designed to bridge the gap between legal obligations and SME operational capabilities.

3.2 Final components, modules, and structure

The finalized Compliance Continuum is structured around three interdependent layers:

1. **Core Technical Assessment Tools**
    a. **CyReA (Cyber Resilience Assessment):** A tool that operationalizes CRA by categorizing digital products into two distinct groups based on their potential cybersecurity risk and criticality.
    b. **DPRA (Digital Product Risk Assessment):** A tool which provides cyber risk management capabilities for organization assessing risks of individual elements of ICT products and estimating potential cascading effects and propagated risks.
    c. **DPMA (Digital Product Maturity Assessment):** A structured and modular cybersecurity assessment tool designed to help organizations (particularly SMEs, micro-enterprises, and start-ups) evaluate the cybersecurity maturity of their digital products.
    d. **PSTVA (Penetration Self-Testing and Vulnerability Assessment):** A customizable vulnerability assessment toolkit able to perform robust security assessments of digital artifacts to support manufacturers, particularly SMEs, in navigating their compliance journey against the CRA.
    e. **CAC (Conformity Assessment and Compliance):** A tool which provides conformity assessment outputs, forming the basis of CE marking documentation.

    Each tool is modular, interoperable, and deployable either independently or in sequence, allowing organizations to tailor compliance activities to their operational reality.

2. **Knowledge and Capacity Services**
    a. **Training Activity Catalogue (TAC):** Provides educational resources, practical guidelines, and capacity-building modules to enhance SME understanding of CRA requirements.
    b. **Community and Support Functions:** Facilitates knowledge sharing and best practices among SMEs, regulators, and industry stakeholders.
3. **Central Access Layer**
    a. **CURIUM User Interface (CURIUM UI):** Serves as the single-entry point for stakeholders, enabling seamless navigation across all tools, services, and outputs.

This modular architecture enables SMEs to engage with the Compliance Continuum either holistically or selectively, ensuring both scalability and adaptability across sectors, and enables future interoperability with possible external (certification) tools, notified bodies, and EU cybersecurity services.

3.3 Overview of technical alignment with CRA

The CURIUM Compliance Continuum has been explicitly designed to achieve technical alignment with the evolving **EU cybersecurity regulatory ecosystem**, ensuring that SMEs can address **horizontal CRA obligations.**

- **Alignment with CRA**
    - Supports CRA Annex I and II essential requirements, including secure product design, vulnerability handling, patch management, and security-by-default principles.
    - Facilitates preparation of **CE marking documentation**, aligning with conformity assessment procedures under CRA.

- Provides modular tools that address **self-assessment routes.**

By aligning with these regulatory and sectoral frameworks, the CURIUM Compliance Continuum ensures that SMEs are not only CRA-compliant but also equipped to meet broader EU cybersecurity governance obligations.

4. Toolchain & Services Overview

4.1 Curium Portal (Landing Page)

Curium incorporates a centralized frontend portal serving as the primary user entry point, where authenticated users access a curated dashboard presenting five specialized cybersecurity tools of CURIUM project: Digital Product Risk Management (DPRA), Digital Product Maturity Assessment (DPMA), Cyber Resilience Assessment (CyReA), Conformity Assessment and Compliance (CAC), and Penetration Self-Testing & Vulnerability Assessment (PSTVA).

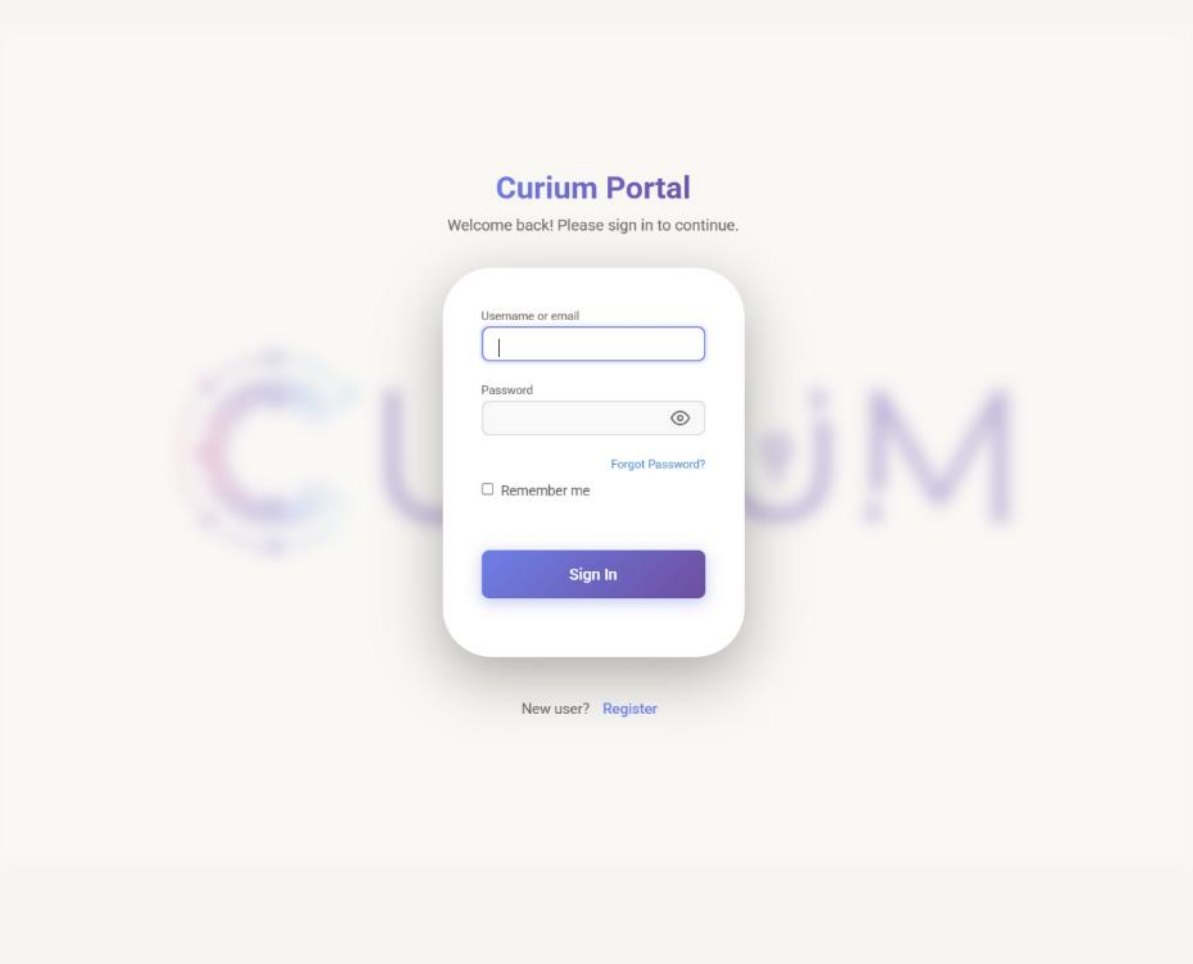


Figure 3 CURIUM Portal (landing page)

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) or federated identity protocols

that propagate authentication tokens from the portal to downstream services, ensuring frictionless, secure session continuity without redundant logins. For the PSTVA toolkit, a user manual is embedded directly within the portal, providing step-by-step guidance on local installation, utilities, and service startup procedures.

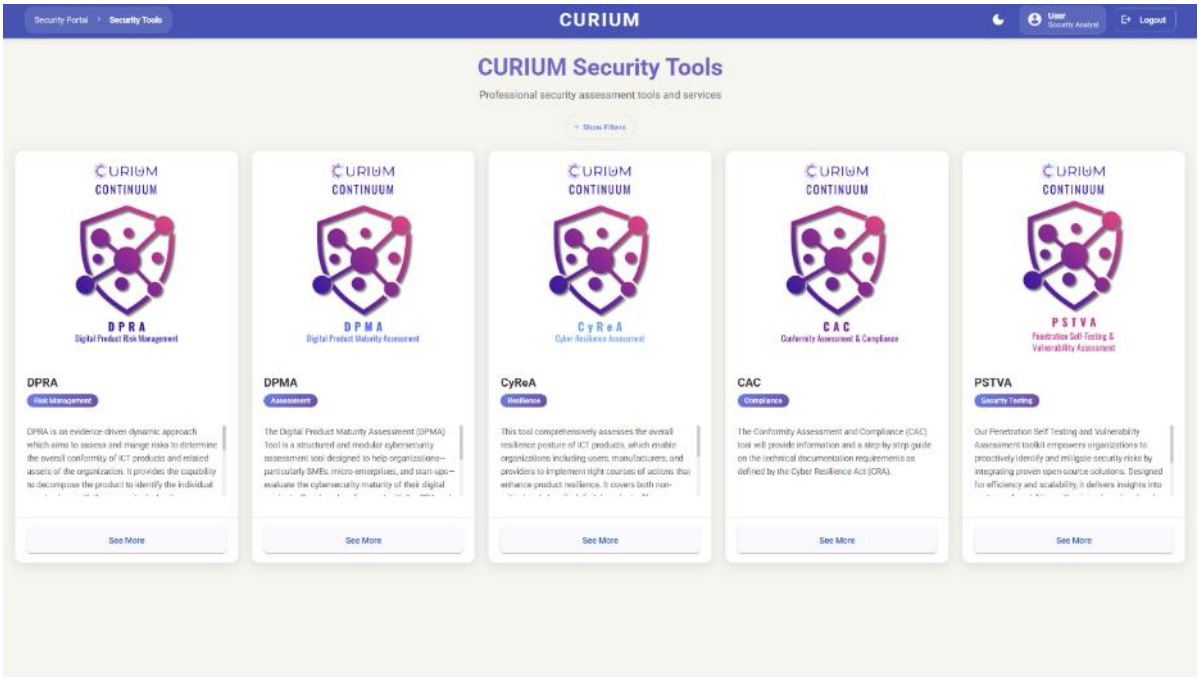


Figure 4 CURIUM Security Tools

4.2 List of mature tools adapted and integrated

4.2.1 CyReA – Cyber Resilience Assessment

CyReA is designed to support ICT product related stakeholders in achieving and demonstrating compliance with the comprehensive requirements of the EU Cyber Resilience Act (CRA) for their ICT products. This resilience assessment service utilizing CyReA aims to ensure that key stakeholders including manufacturer importer, distributor, authorized representative, and owner has systematically verified that their products with digital elements (ICT products) have been robustly assessed and comply with the essential requirements mandated by the CRA.

CyReA operationalizes CRA by categorizing products with digital elements into two distinct groups based on their potential cybersecurity risk and criticality.

- Assessment for default class - Non-Critical Digital Products: The baseline group includes non-critical digital products that do not exhibit high pose security risk. CyReA facilitates the required self-assessment to identify the security weakness and necessary mitigation strategy for the improvement.
- Assessment for Critical Digital Products (Class I and Class II): This group considers lower risk product under Class I, while higher risk product under Class II. CyReA facilitates formal assessment depending on the product type to identify the necessary vulnerabilities and their mitigation.

CyReA provides structured questionary-based wizard designed to facilitate and streamline the compliance assessment of their Products with Digital Elements (ICT products) against the requirements of the EU Cyber Resilience Act (CRA). These questions are organized according to a logical process flow that reflects the steps for the stakeholder to determine how the CRA applies to them.

Step 1: Scope & Role Determination: This initial foundation step establishes the organization's legal role including Manufacturer, Importer, Distributor, Authorized Representative, and End User under the CRA and verifies that they are involved with products that fall under the general scope of the regulation (products with digital elements). The role defines whether the organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing products with digital elements.

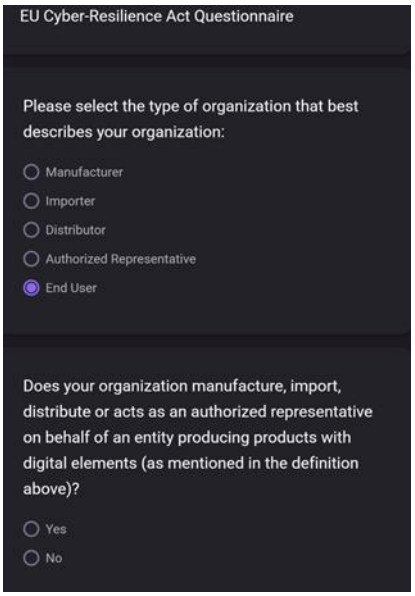


Figure 5 Questionnaire

Step 2: Product Screening: This step aims to screen the ICT product as CRA specifically excludes products with specific types that covered by other EU regulations such as Medical Devices, military products. Therefore, answering yes to any of these questions typically means the CRA does not apply to that specific product. The exclusion includes Medical Device regulated by the Regulation (EU) 2017/745, Transport by regulation (EU) 2019/2144, Aviation regulated by (EU) 2018/1139, National Security, and Software as a Service.

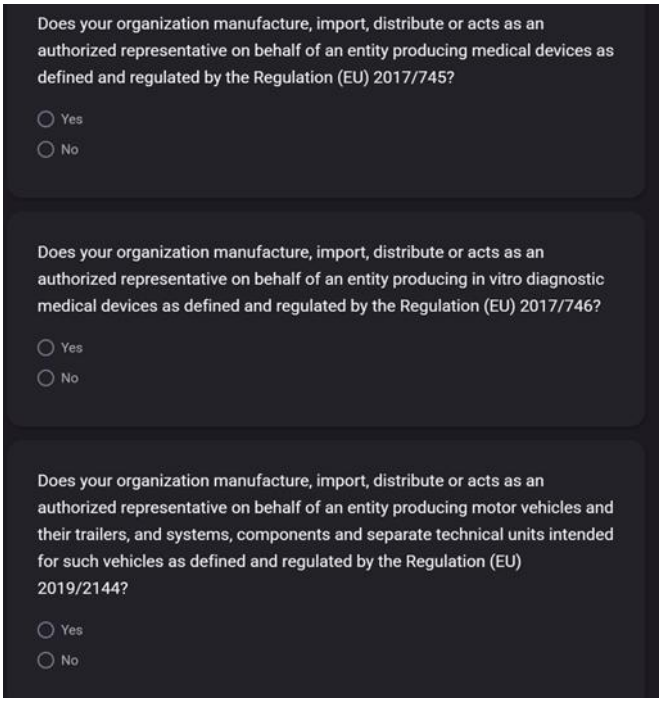


Figure 6 Product screening

Step 3: Product Classification: once the product is screen and within scope of CRA, then it is necessary to classify the product to determine the required level of conformity assessment. Class I product is classified with a list of 23 specific products including Identity Management, Browsers, Network Management, and Operating Systems. Similarly, Class II product is classified with a list 15 specific, high-risk products including Server OS, Hypervisors, Routers, Industrial Firewalls, and Smart Meters.

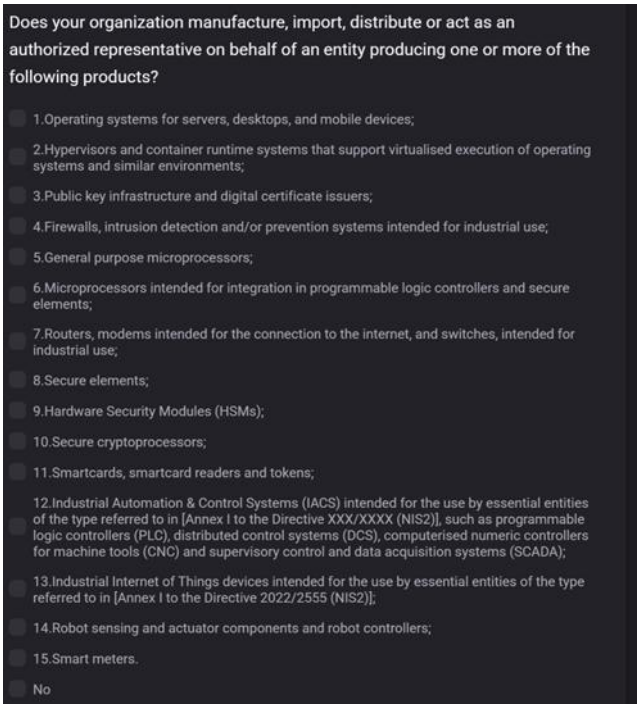


Figure 7 Questionnaire (continued)

Step 4: Conformity Assessment Readiness: This final step aims to assess the ability to successfully execute the required assessment through either internal self-assessment or preparation for third-party assessment based

on their resources, processes, and experience with risk assessment. Readiness is based on diverse parameters, i.e., assessment methodology using self-assessment or self-testing, risk assessment status and scope, and necessary resource, process and confidence.

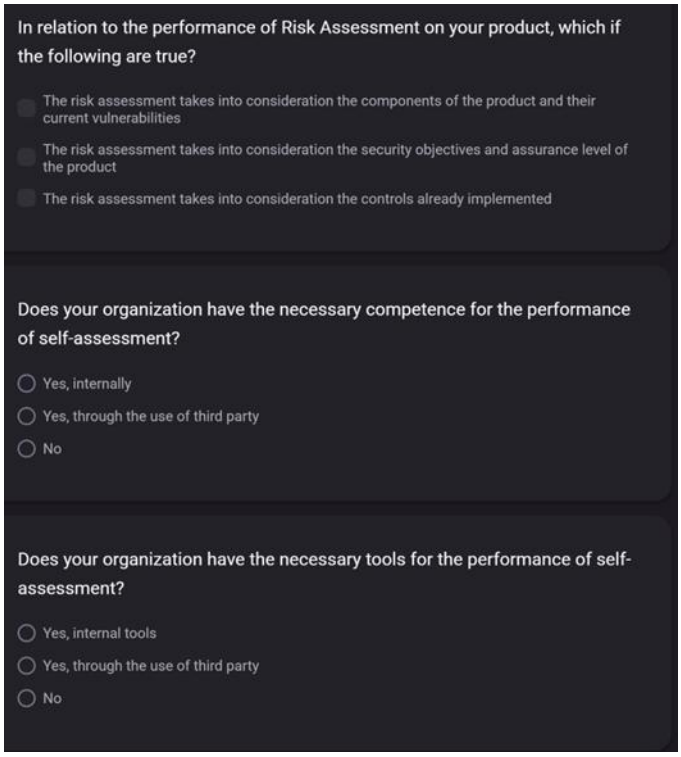


Figure 8 Questionnaire (continued)

Customizable CyReA capabilities

- Based on the response from step 1, CyReA satisfies determining if a user falls within the scope of the CRA. Specifically, the two distinct questions provide easy-to-understand process for scope determination and ensure that only applicable product requires to comply with CRA.
- The outcome of step 3 provides direct mapping the response to the defined product categories of the CRA, which determines conformity assessment procedure the organization must follow.
- CyReA wizard follows a systematic four steps compliance process and response from each step ensures that the generated evidence is a faithful record of the decision flow.

4.2.2 DPRA – Digital Product Risk Management

The Digital Product Risk Management (DPRA) service follows an evidence-driven, systematic risk management approach that aims to consider threats, vulnerabilities and risks arising from interdependent assets that constitute products of digital elements, and entire infrastructures of organizations. The tool provides cyber risk management capabilities for organizations in a holistic, cost-effective manner by assessing risks of individual elements of ICT products and estimating potential cascading effects and propagated risks. The tool utilizes open intelligence in real time to identify vulnerabilities and threats in products with digital elements based on international cybersecurity standards such as NIST 800-53 and ISO/IEC 15408 for a unified security evaluation and control. The DPRA of the CURIUM platform employs a hybrid top-down strategy that implements the following activities as part of the risk management process for products with digital elements, analyzed in the following sections:

- Asset Management
- Cyber Threat Intelligence (CTI) open repository

- Product Management
  - Create/manage Product with digital elements
  - Add/manage elements to the Product
- Review Risk Assessment results
- Definition of security details
  - Definition of Security Objectives
  - Definition of Security Requirements
- Security Control Management
- View Product's Protection Profile

4.1.2.1 Asset Management

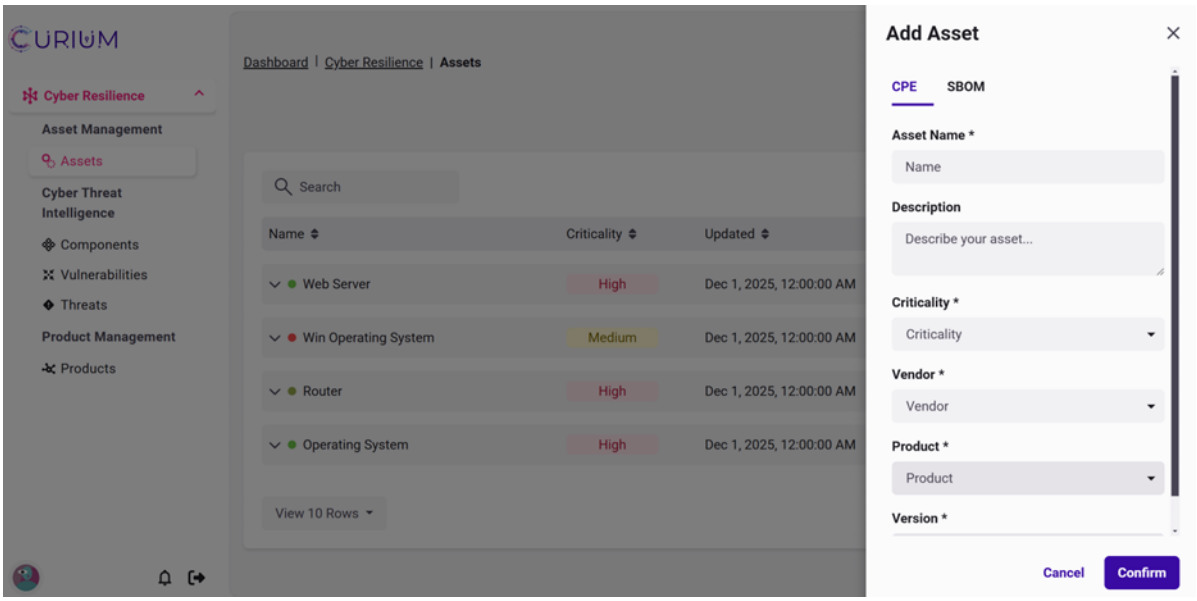


Figure 9 Assets Management

From DPRA "Assets" corresponding options, the user can edit/delete the created asset or view the asset profile details illustrating further technical and security information, supported by an asset dependency model.

4.1.2.2 Cyber Threat Intelligence (CTI)

A pool that collects and analyses information about existing and emerging cyber threats, including attack-types, and asset vulnerabilities based on prominent open repositories.

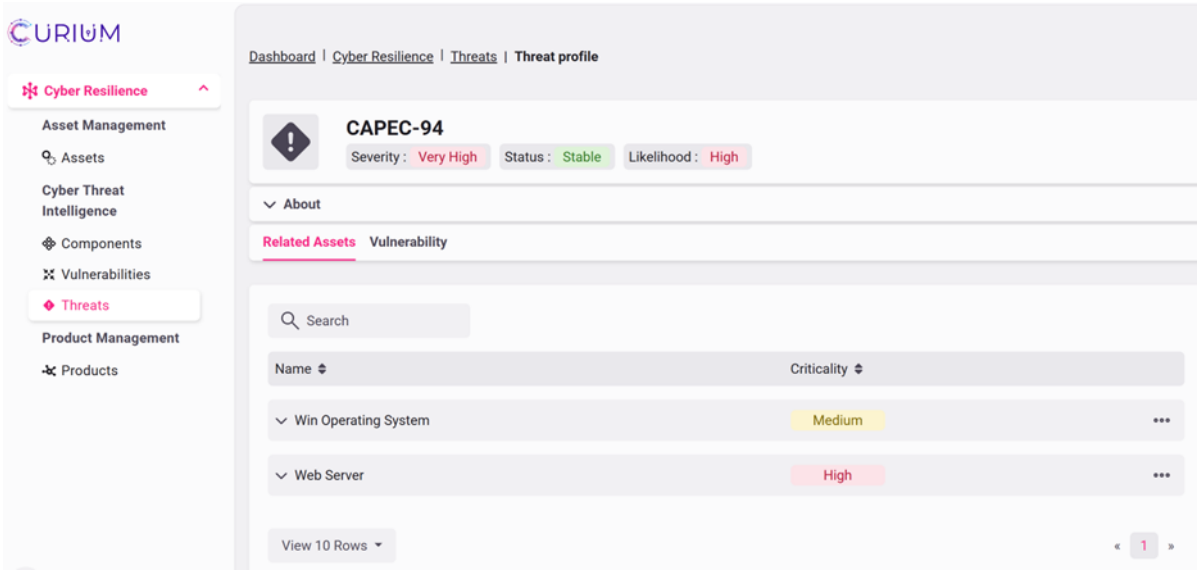


Figure 10 CTI environment of DPRA.

4.1.2.3 Product Management

The Product Management category of DPRA enables the user to create a product with digital elements and set the evaluation boundaries.

Create/manage Product with digital elements. To do so, the user clicks on the "Add Product" button and provides all the required information, including the selection of the assurance level that will be adopted for the security evaluation of the product following the ISO/IEC 15408 (Common Criteria) IT evaluation framework.[1] By selecting the desired assurance level further evaluation criteria are shown for the specific product (e.g. attack potential, cybersecurity certification scheme related information). The user can edit information on the declared product or delete the created product.

[1] ISO/IEC 15408 (Common Criteria)

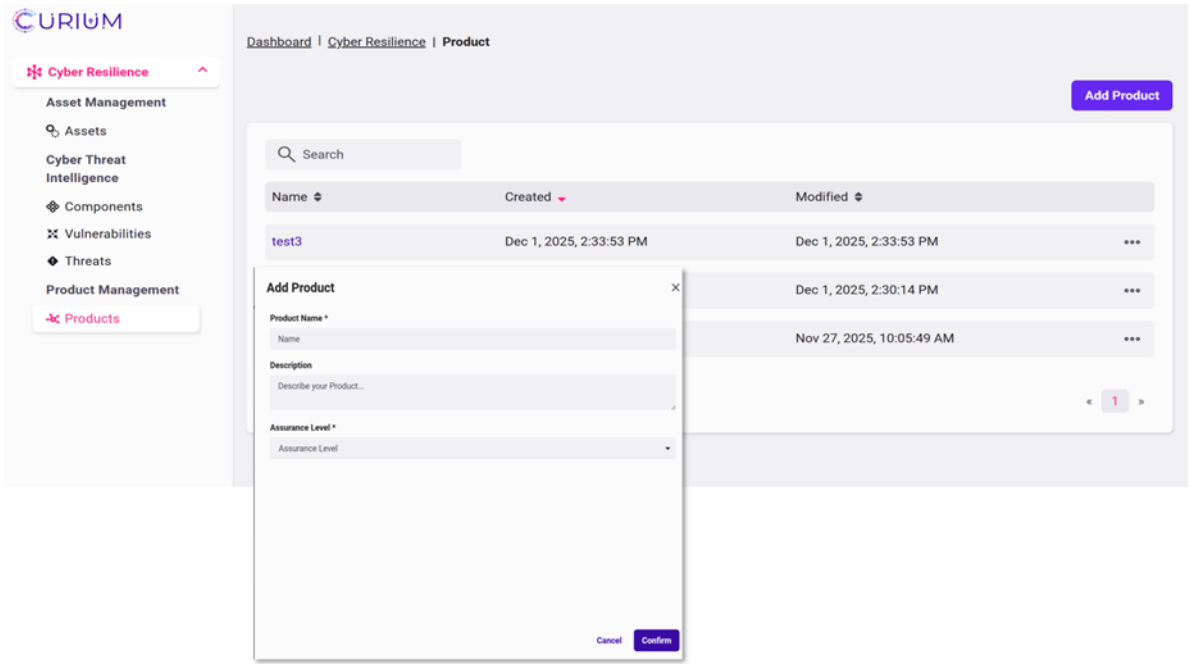


Figure 11 Create a Product with digital elements.

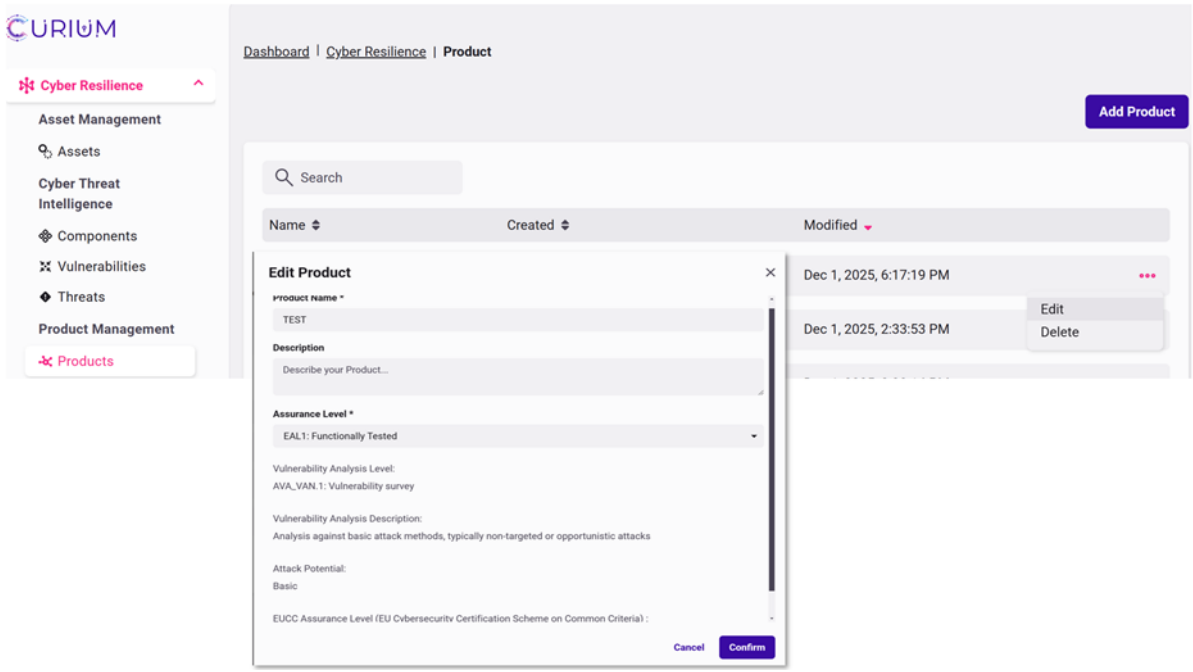


Figure 12 Manage Product with digital elements.

Add/manage elements to the Product. Upon creating the product and defining the evaluation criteria, the user shall add the individual elements (assets) that constitute the specific product by clicking on the “Add Asset” button from the “DPRA: Assets” tab in the Product Management environment and selecting the desired assets from a respective list derived from the “Asset Management” environment of DPRA. Information about the assets declared on a product can be viewed or edited or removed by clicking on the 3-dot menu from the respective asset and selecting the desired option.

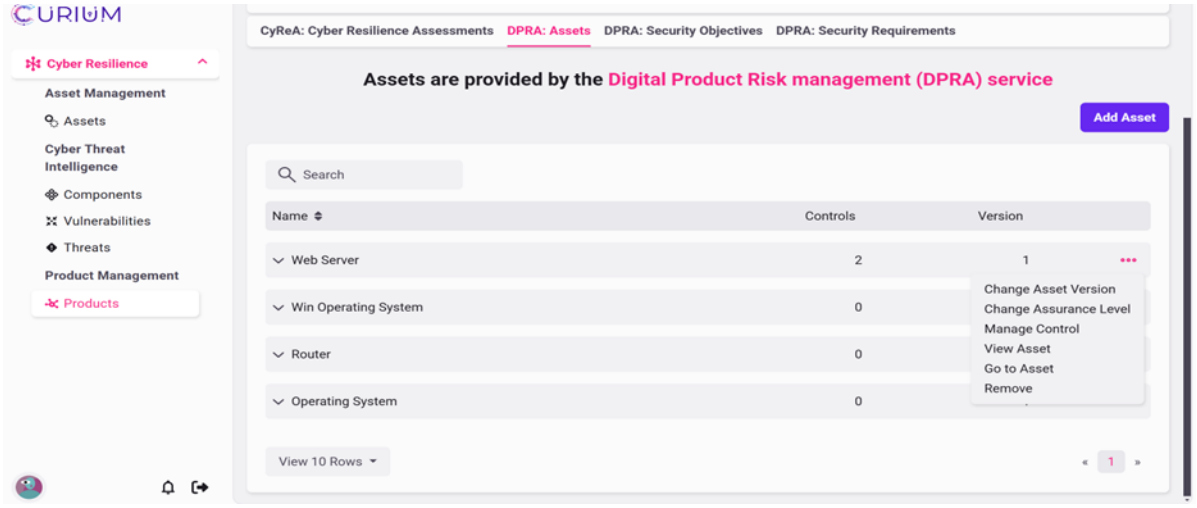


Figure 13 Add/manage Product elements (assets).

Moreover, the "Product Management" environment of DPRA provides visualization capabilities of the product's assets illustrating asset graphs that depict assets' technical interdependencies within the product.

4.1.2.4 Review Risk Assessment results

DPRA supports an evidence-driven, multi order dynamic risk assessment (D2.2[2]), that estimates vulnerabilities, threats and risks and their cascading effects on products with digital elements.

It implements a calculation model that incorporates a variety of IT and security taxonomies, catalogues, and other open repositories and supports the automated population of the adopted asset-threat-vulnerability model illustrating data from reputable threat intelligence sources. To review the risk assessment results of a product with digital elements, the user browses the preferred product from the corresponding list in the product management environment and from the "DPRA: Assets" tab, he/she clicks on the "View Asset" option appearing in the 3-dot menu on the right side of each product asset (Figure 13). Then, the user can navigate and review all the information of the identified threats, vulnerabilities and the calculated risks of the product's assets (Figure 14).

[2] https://curium-project.eu/wp-content/uploads/2025/07/public-deliverable-D2.2.pdf

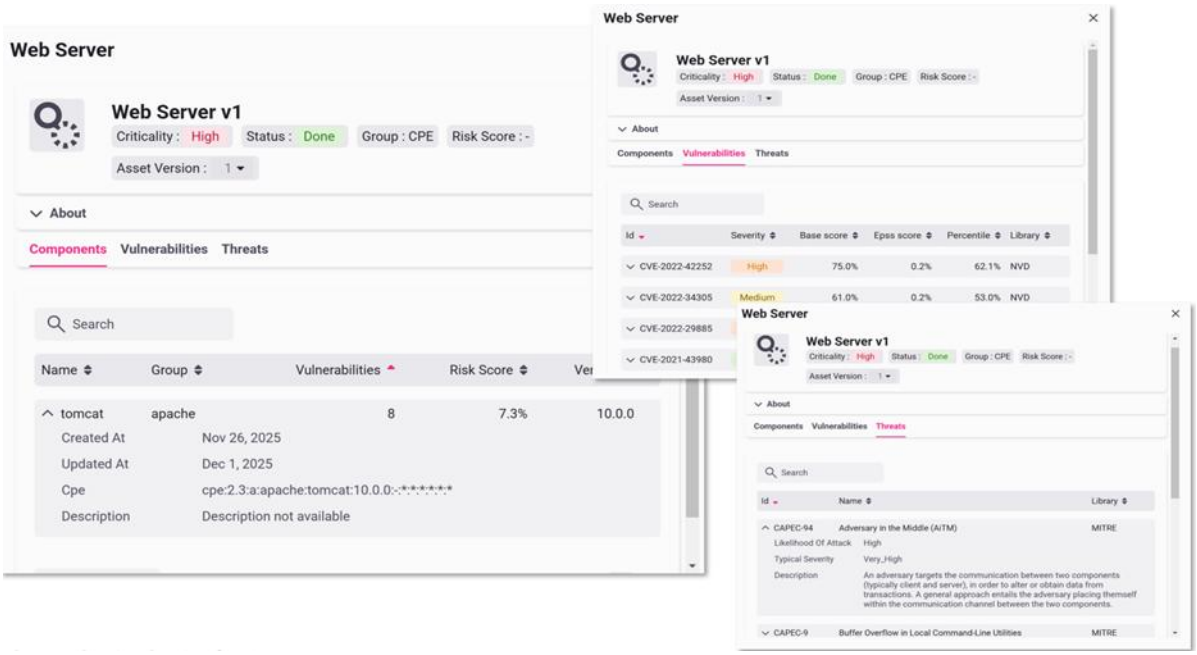


Figure 14 Review risk assessment results on assets of a product with digital elements.

selects on assets from a respective list derived from the "Asset Management" environment of DPRA. Information about the assets declared on a product can be viewed or edited or removed by clicking on the 3-dot menu from the respective product and selecting the desired option.

4.1.2.5 Definition of security details

After reviewing the risk assessment results, the DPRA user defines a set of security details, assumed as prerequisites for the security evaluation of the product with digital elements. The security details activity involves the definition of security objectives and security requirements on the product's assets. The activity relies on ISO/IEC 15408 international standard and utilizes a hybrid model that aggregates a set of security functional requirements and interrelates them with respective security objectives and controls.

Definition of Security Objectives. Security Objectives can be defined on the assets of the product with digital elements by clicking on the preferred product in the product management environment of DPRA, and then from the "DPRA: Security Objectives" tab by clicking on the "Add Security Objective" button. Afterwards, the user selects the preferred security objective(s) for each asset of the product. Furthermore, the user can view or edit details of the security objective or remove it from a product's asset. To do so, he/she clicks on the respective option from 3-dot menu appears at the right side of the preferred asset in the "DPRA: Security Objectives" tab.

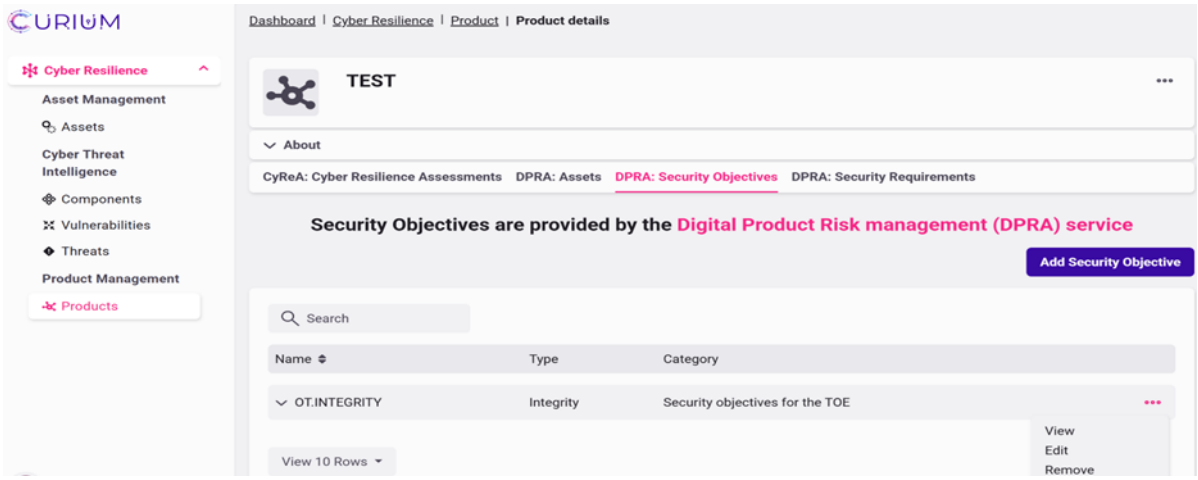


Figure 15 Security objectives list of a product with digital elements.

Definition of Security Requirements. Security Requirements can be defined on the assets of the product with digital elements from the "DPRA: Security Requirements" tab in the product management environment of DPRA. Security requirements are mapped with security objectives, as mentioned in the beginning of this section. Specifically, each security objective can be addressed by the satisfaction of one or more security requirements. Upon selecting the security objectives of the product's assets, a list of all interrelated requirements appears in the "DPRA: Security Requirements" tab.

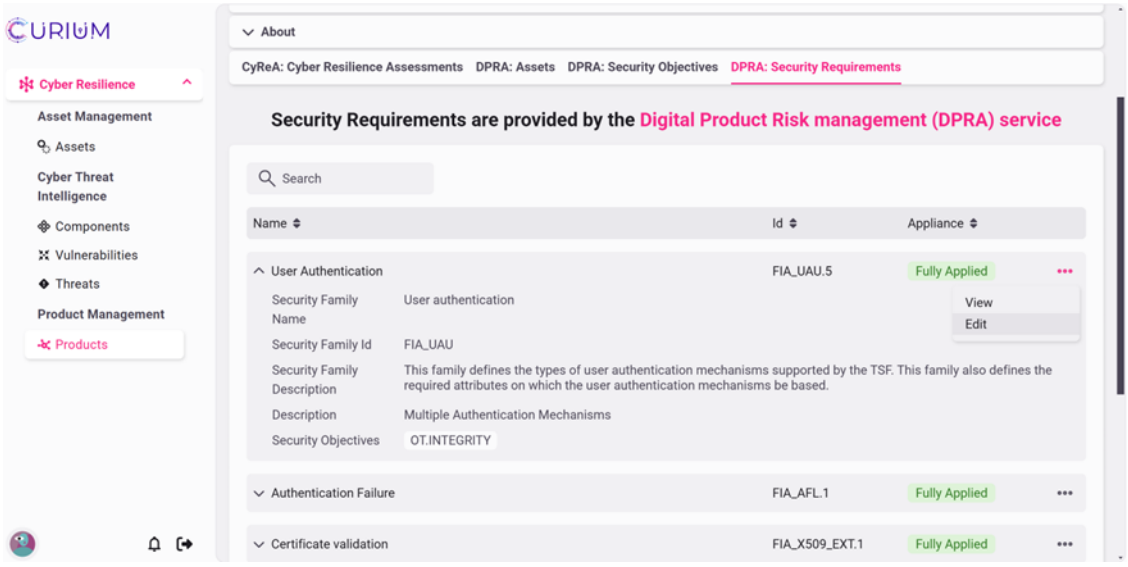


Figure 16 Security Requirements list of a product with digital elements.

The user can view the security requirements per product's asset and deselect those that he/she wants to exclude from the security evaluation process of an individual asset by navigating to the respective options of the 3-dot menu, depicted at the right part of each requirement.

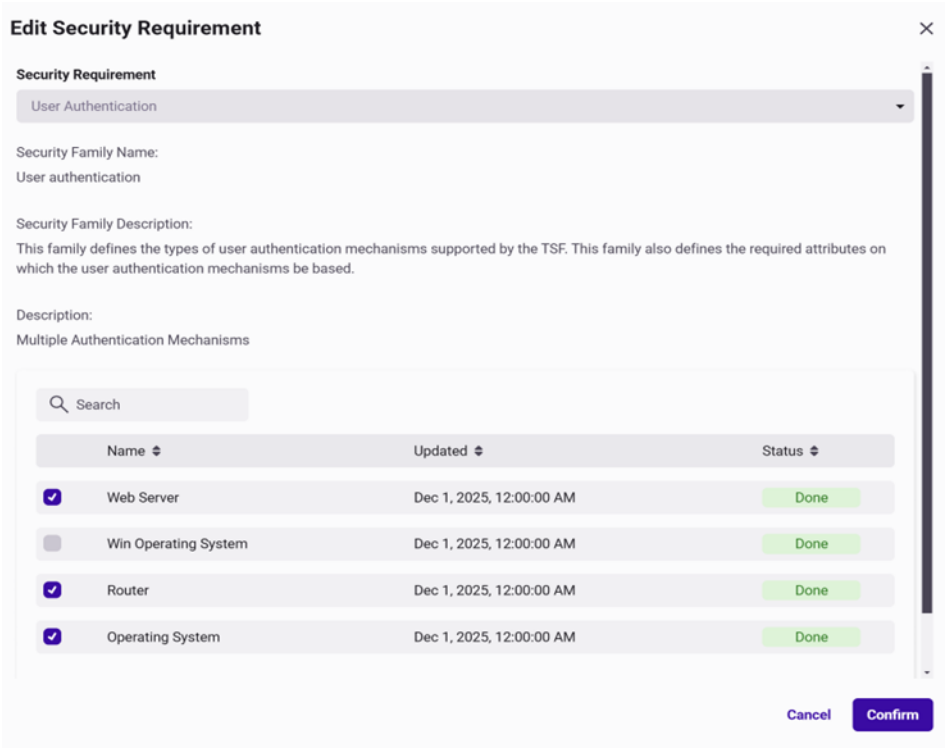


Figure 17 Include in/exclude from product's assets Security Requirements.

4.1.2.6 Security Control Management

Security requirements are interrelated with security controls following the hybrid model, mentioned in the beginning of Section 4.1.2.5. Specifically, an effective security control policy can satisfy the security requirements defined for a product. To add/manage security controls on assets, the user selects the preferred asset in the Product Management environment and by clicking on the 3-dot menu (Figure 13), he/she selects the "Manage Control" option. Then, the Control tab appears depicting all security requirements defined for the specific asset. To assign security controls on the product's asset, the user selects a security requirement and clicks from the 3-dot menu the option "Assign NIST Controls". Afterwards, from the "Manage NIST controls" tab, the user selects the security controls implemented to satisfy the specific requirement from a default list, as shown in Figure 18.

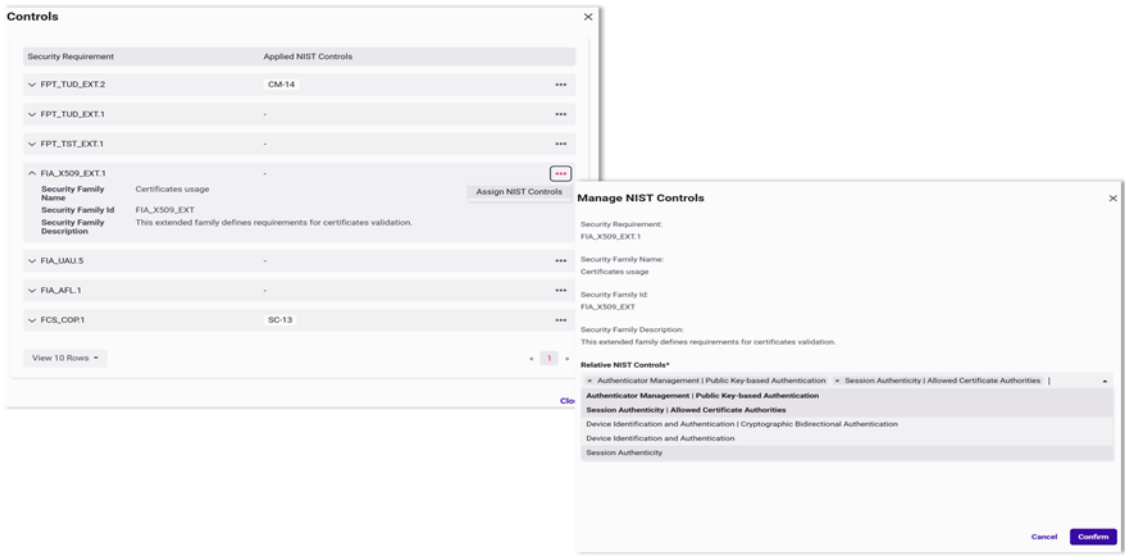


Figure 18 Assign security control(s) for a security requirement of a product's asset.

4.1.2.7 View Product's Protection Profile

After defining all the proper technical and security information of the product and its embedded elements (assets), the user can review the product's protection profile. To achieve this, the user selects the preferred product from the products' list in the product management environment of DPRA and then, he/she selects the "View Protection Profile" option from the 3-dot menu appearing at the right side in the product's tab.

Figure 19 View Protection Profile of a product with digital elements.

Finally, the Protection Profile details of the composite product are depicted, as shown in Figure 19. DPRA supports a standardized structure to illustrate the product's protection profile based on the ISO/IEC 15408:2022 (Common Criteria 2022 Release 1).

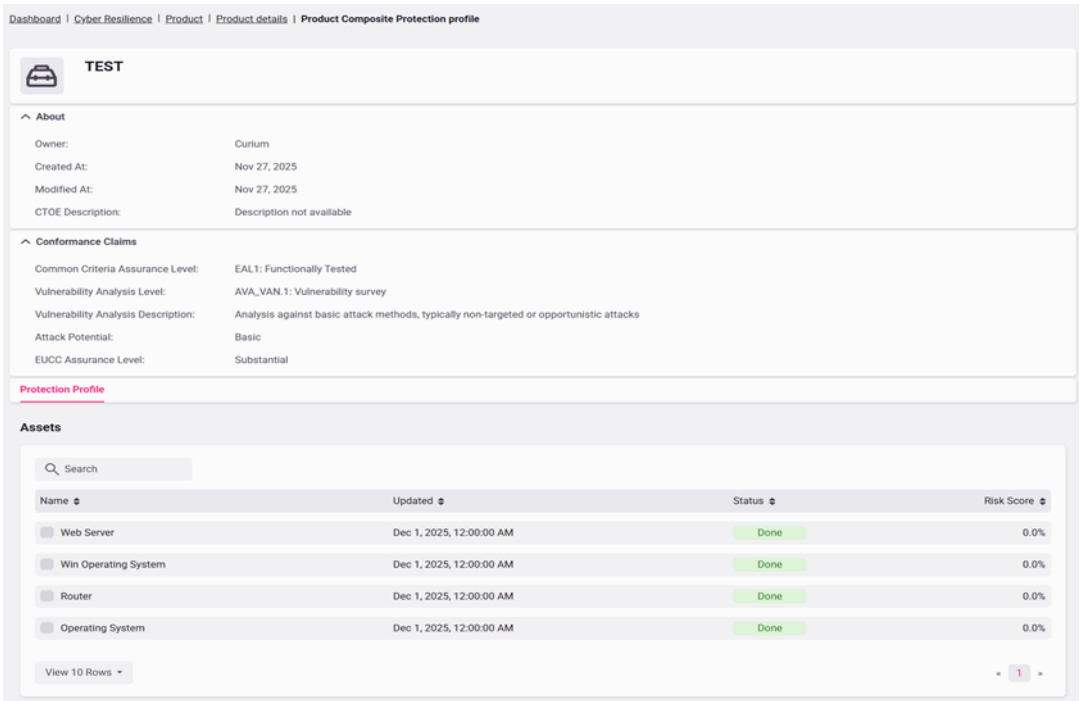


Figure 20 Protection Profile details of a product with digital elements.

4.1.2.8 Customizable DPRA capabilities

- SMEs can define the product that will be evaluated according to their needs (select preferred EAL, etc)
- Guides SMEs how to decompose the complex product and allows them to define the embedded assets either by following a standardized naming scheme or by automatically scanning a container and creating an SBOM

- Allows SMEs to define the security objectives by selecting from a default list the most appropriate to the product assets, according to the SME's needs
- Allows SMEs to select security requirements from a default list that seek to consider in the evaluation of their product, concerning the SME's assets' technical specificities (e.g. product types)
- Enables SMEs to identify efficient security control policy tailored to their activities and needs

4.2.3 DPMA – Digital Product Maturity Assessment

4.2.3.1 Introduction

The Digital Product Maturity Assessment (DPMA) Tool is designed to support organizations, particularly SMEs, micro-enterprises, start-ups, product managers and technical leads, in navigating the expanding and increasingly complex landscape of cybersecurity requirements for digital products. As regulatory expectations evolve, notably with the introduction (among others) of the Cyber Resilience Act (CRA) and the widespread adoption of international cybersecurity standards such as ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53 and CIS Controls v8, many organizations struggle to understand which measures apply to their needs and how these should be prioritized. The DPMA tool supports the cybersecurity risk management process implemented by any organization – having in scope the organization, a portion of it, specific services or specific products with digital elements.

4.2.3.2 Purpose and Scope of the DPMA Tool

The DPMA Tool's primary objective is to help organizations understand the maturity of their cybersecurity practices and identify which additional measures may be beneficial. The tool extracts cybersecurity requirements or recommendations from numerous established standards and frameworks and consolidates them into a common format that is easier to navigate and interpret. Through its hierarchical structure, the mapping to a common reference point (the ISO/IEC 27001 Annex A controls), threat correlation and maturity-level identification, users gain a comprehensive view of the security measures available to them and can evaluate how these relate to their operational context.

The tool is particularly suited to SMEs and micro-SMEs that may not possess extensive cybersecurity resources. The structured and comprehensible presentation of cybersecurity measures reduces barriers to understanding and supports users in planning their progression towards stronger cybersecurity capabilities. More experienced teams can benefit from the tool's harmonization of cybersecurity frameworks, enabling cross-framework comparisons and identification of gaps where controls may be missing or insufficient.

4.2.3.3 DPMA key concepts

The DPMA tool is built upon a series of key concepts. These concepts are:

Multi-framework approach

The treatment options / measures included within the tool have been extracted from well-known standards and frameworks.

a. **ISO/IEC 27001[3] (versions 2013 and 2022).** ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet. The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. ISO/IEC 27001 promotes a holistic approach to information

[3] https://www.iso.org/standard/27001

security: vetting people, policies and technology. An information security management system implemented according to this standard is a tool for risk management, cyber-resilience and operational excellence.

b. **ISO/IEC 27002[4] (versions 2013 and 2022).** ISO/IEC 27002 is an international standard that provides guidance for organizations looking to establish, implement, and improve an Information Security Management System (ISMS) focused on cybersecurity. While ISO/IEC 27001 outlines the requirements for an ISMS, ISO/IEC 27002 offers best practices and control objectives related to key cybersecurity aspects including access control, cryptography, human resource security, and incident response. ISO/IEC 27002 emerges as a crucial tool in this context, assisting organizations in navigating the intricate web of information security challenges.

c. **ISO/IEC 27003[5] (version 2017).** ISO/IEC 27003:2017 provides explanation and guidance on ISO/IEC 27001:2013.

d. **ISO/IEC 27004[6] (version 2016).** ISO/IEC 27004:2016 provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It establishes a) the monitoring and measurement of information security performance; b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls; c) the analysis and evaluation of the results of monitoring and measurement.

e. **ISO/IEC 27007[7] (version 2020).** This document provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. This document is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

f. **ISO/IEC 27008[8] (version 2019).** This document provides guidance on reviewing and assessing the implementation and operation of information security controls, including the technical assessment of information system controls, in compliance with an organization's established information security requirements including technical compliance against assessment criteria based on the information security requirements established by the organization. This document offers guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001.

g. **ISO 19011[9] (version 2018).** ISO 19011 is an international standard that provides guidelines for auditing management systems, including quality management systems (ISO 9001) and environmental management systems (ISO 14001). It outlines the principles of auditing, managing audit programs, and conducting management system audits. Using ISO 19011 helps organizations: Implement auditing best practices based on international consensus, demonstrate credibility and capability in auditing to customers and stakeholders, improve management systems and processes through structured audits, meet customer and regulatory audit requirements, Facilitate consistent auditor training and evaluation.

[4] https://www.iso.org/standard/75652.html
[5] https://www.iso.org/standard/63417.html
[6] https://www.iso.org/standard/64120.html
[7] https://www.iso.org/standard/77802.html
[8] https://www.iso.org/standard/67397.html
[9] https://www.iso.org/standard/70017.html

h. **ISO 31000[10] (version 2018).** ISO 31000 is an international standard that provides principles and guidelines for risk management. It outlines a comprehensive approach to identifying, analysing, evaluating, treating, monitoring and communicating risks across an organization. Benefits: Standard risk management principles, framework and process, Guidance for implementing risk management practices, Tools for contextualizing risk management to any organization, Criteria for monitoring, reviewing and continually improving risk management, Foundation for integrating risk management throughout an organization.

i. **CIS Critical Security Controls[11] (Version 8).** The CIS Critical Security Controls (CIS Controls) are a prioritized set of CIS Safeguards to defend against the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 was enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, work from home, and changing attacker tactics prompted the update and supports an enterprise's security as they move to both fully cloud and hybrid environments.

j. **NIST SP 800-53[12] (Revision 5).** This publication provides a catalogue of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines.

k. **NIST SP 800-160[13] (version 1, revision 1).** This publication describes a basis for establishing principles, concepts, activities, and tasks for engineering trustworthy secure systems. Such principles, concepts, activities, and tasks can be effectively applied within systems engineering efforts to foster a common mindset to deliver security for any system, regardless of the system's purpose, type, scope, size, complexity, or the stage of its system life cycle. The intent of this publication is to advance systems engineering in developing trustworthy systems for contested operational environments (generally referred to as systems security engineering) and to serve as a basis for developing educational and training programs, professional certifications, and other assessment criteria.

l. **SAFECODE - Defining Risks and Responsibilities for Securing Software in the Global Supply Chain[14].** This paper, the first in a series, will assess software supply chain integrity in the context of software engineering, providing a framework and common taxonomy for evaluating the associated risks and defining the industry's role in addressing them. This framework will serve as the foundation for subsequent work aimed at describing and analysing software integrity best practices.

m. **ISACA - Information Security Management Audit/Assurance Program[15].** The document published by ISACA provides a comprehensive framework and practical guidance for auditing and assuring

[10] https://www.iso.org/standard/65694.html

[11] https://www.cisecurity.org/controls/v8

[12] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[13] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

[14] https://safecode.org/publication/SAFECode_Supply_Chain0709.pdf

[15] ISBN 978-1-60420-156-7, *Information Security Management Audit/Assurance Program*

an organization's information security management function. The document is intended primarily for IT audit and assurance professionals and serves as a structured roadmap for evaluating how effectively information security is governed, managed, and operated within an enterprise.

n. **ENISA - Technical Guidelines for the implementation of minimum security measures for Digital Service Providers[16].** ENISA has issued this report to assist Member States and DSPs in providing a common approach regarding the security measures for DSPs. Although ENISA has already drafted a set of security objectives in the context of cloud security in 2014, this study goes further than that by broadening the scope of its work and by including security objectives for all three categories of digital service providers. This study lists 27 Security Objectives (SOs) for DSPs. In those 27 SOs, security measures that map to the NIS Directive requirements are also included.

Interoperable mapping

The treatment options / measures extracted from the different frameworks have been mapped to a common reference. Specifically, the controls of Annex A - ISO/IEC 27001:2022 & ISO/IEC 27002:2022 have been used as a common reference to all measures of the DPMA tool. This was decided because ISO/IEC 27001:2022 & ISO/IEC 27002:2022 controls are a globally recognized taxonomy. By mapping the ISO/IEC 27001:2022 & ISO/IEC 27002:2022 controls to each of the entry of the other frameworks, a connection is inferred between all of them.

Maturity level identification

For each treatment option / measure included within DPMA, a maturity level (security maturity level) has been assigned. This information has been derived through the cross mapping of the descriptions of the measures to those of well-known maturity models. (e.g. CIS Controls, CMMC, Cybersecurity capability maturity model (C2M2), Cyber Fundamentals and others). The maturity levels are represented by a number ranging from 1 to 6, with 1 representing the minimum level and 6 representing the highest level. These numbers do not represent actual numerical values in terms of security (i.e., level 6 does not mean that the organization implementing the measures of this level are exposed to 0% risk), but rather they provide a list of prioritized actions. When an organization wants to implement a series of measures in one area (e.g. backup), and they want to achieve the highest level, they should implement all the controls for this specific area for all levels from 1 to 6. (This means that each level identified adds to the previous levels to achieve the required level of security).

Correlation to threats

DPMA includes more than 200 threats (extracted from recognized standards) and cross mapped them to the ISO/IEC 27001:2022 & ISO/IEC 27002:2022 controls. For each threat one or more controls have been identified with the ability to reduce the exposure or the impact to the organization or asset to the threat. (a many to many relationship). By combining this information, users can search also with the related threats – and identify the controls and measures that could be used to treat them.

4.2.3.4 Navigating the DPMA

The DPMA Tool is accessible directly through a web browser and requires no installation or technical preparation / pre-requisites. Users are presented with a workspace that allows seamless interaction with the dataset. The primary navigation element is a free-text search bar located above the results table. This search bar provides

[16] https://www.enisa.europa.eu/sites/default/files/publications/WP2016%203-2%204%20Technical%20guidelines%20for%20implementation%20of%20minimum%20security%20measures.pdf

broad and flexible access to the underlying dataset, allowing users to explore measures using keywords, concepts or threat names. As shown in Figure 21, the search bar enables users to query the entire dataset quickly and receive results that align with the terms they have entered.

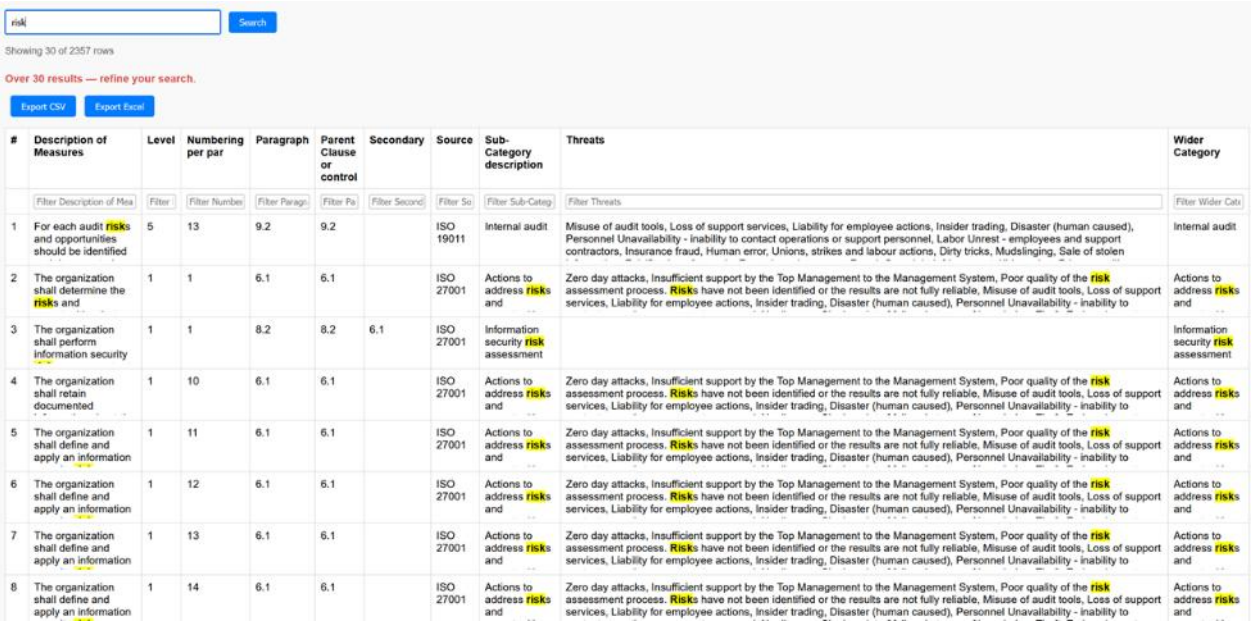
Figure 21 Main search bar

Beneath the search bar is the main table, which contains structured information on each cybersecurity measure. The table includes attributes such as category, description, maturity level, source reference, and threat associations. Users can scroll horizontally to view additional metadata, ensuring that all contextual information remains visible without overwhelming the interface. The results are capped at thirty entries, encouraging users to refine their search terms when initial queries are too broad.

4.2.3.5 Search and Filtering Capabilities

The DPMA Tool supports flexible exploration of cybersecurity measures. The free-text search function enables keyword-based discovery, allowing users to locate relevant measures by typing specific terms such as “malware,” “risk,” “logging” or “cryptography.” This functionality is particularly useful for users who know what they are searching for but require support in understanding available measures and their level of maturity.

Alongside the global search function, the tool includes column-specific filters that allow users to refine results more accurately. Filters can be applied to categories, maturity levels, descriptions, or threats. As seen in Figure 22, filtered searches allow users to narrow the dataset to a highly specific subset, such as all maturity-level-three controls related to incident detection or all controls mitigating a particular threat. This dual approach of global search and attribute-based filtering enables both broad and highly targeted use.


risk Search

Showing 30 of 2357 rows

Over 30 results — refine your search.

Export CSV Export Excel

#	Description of Measures	Level	Numbering per par	Paragraph	Parent Clause or control	Secondary	Source	Sub-Category description	Threats	Wider Category
	Filter Description of Mea	Filter	Filter Number	Filter Paragr	Filter Pa	Filter Second	Filter So	Filter Sub-Categ	Filter Threats	Filter Wider Cate
1	For each audit risks and opportunities should be identified	5	13	9.2	9.2		ISO 19011	Internal audit	Misuse of audit tools, Loss of support services, Liability for employee actions, Insider trading, Disaster (human caused), Personnel Unavailability - inability to contact operations or support personnel, Labor Unrest - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labour actions, Dirty tricks, Mudslinging, Sale of stolen	Internal audit
2	The organization shall determine the risks and	1	1	6.1	6.1		ISO 27001	Actions to address risks and	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit tools, Loss of support services, Liability for employee actions, Insider trading, Disaster (human caused), Personnel Unavailability - inability to	Actions to address risks and
3	The organization shall perform information security	1	1	8.2	8.2	6.1	ISO 27001	Information security risk assessment		Information security risk assessment
4	The organization shall retain documented	1	10	6.1	6.1		ISO 27001	Actions to address risks and	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit tools, Loss of support services, Liability for employee actions, Insider trading, Disaster (human caused), Personnel Unavailability - inability to	Actions to address risks and
5	The organization shall define and apply an information	1	11	6.1	6.1		ISO 27001	Actions to address risks and	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit tools, Loss of support services, Liability for employee actions, Insider trading, Disaster (human caused), Personnel Unavailability - inability to	Actions to address risks and
6	The organization shall define and apply an information	1	12	6.1	6.1		ISO 27001	Actions to address risks and	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit tools, Loss of support services, Liability for employee actions, Insider trading, Disaster (human caused), Personnel Unavailability - inability to	Actions to address risks and
7	The organization shall define and apply an information	1	13	6.1	6.1		ISO 27001	Actions to address risks and	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit tools, Loss of support services, Liability for employee actions, Insider trading, Disaster (human caused), Personnel Unavailability - inability to	Actions to address risks and
8	The organization shall define and apply an information	1	14	6.1	6.1		ISO 27001	Actions to address risks and	Zero day attacks, Insufficient support by the Top Management to the Management System, Poor quality of the risk assessment process. Risks have not been identified or the results are not fully reliable, Misuse of audit tools, Loss of support services, Liability for employee actions, Insider trading, Disaster (human caused), Personnel Unavailability - inability to	Actions to address risks and

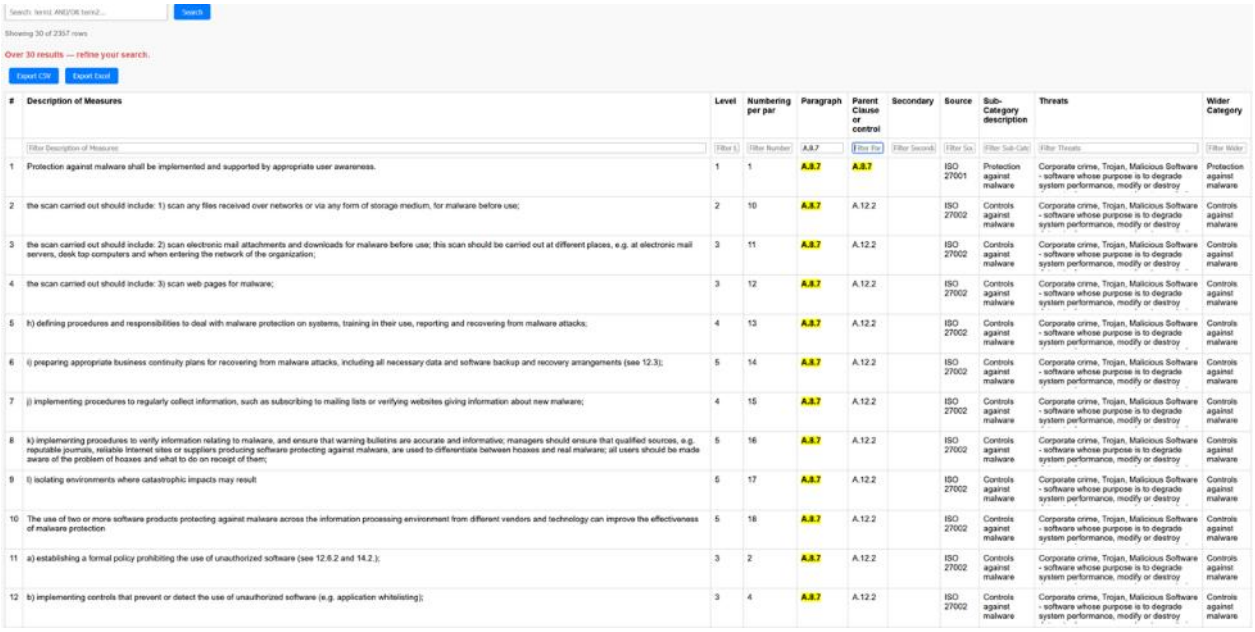
Figure 22 Example of free-text search using keywords

4.2.3.6 Interpreting Maturity Levels and Threat Associations

Each cybersecurity measure in the DPMA database includes a maturity level that indicates the assigned level of security of the measure using a scale from 1 to 6. Lower maturity levels represent foundational practices that every organization should consider, while higher maturity levels correspond to advanced measures found in

more mature security programs. This maturity model allows organisations to reflect on their current capabilities and strategically plan their roadmap towards stronger cybersecurity practices.

The tool also links each cybersecurity measure to the threats it mitigates, creating a traceable relationship between threats and controls. This traceability is essential for supporting threat-informed defense strategies. As shown in Figure 23, the threat correlations help users understand why particular measures exist and how they contribute to addressing specific risks. This enables a more integrated approach to risk management, whereby organizations can prioritize measures based on the threats most relevant to them.



#	Description of Measures	Level	Numbering per par	Paragraph	Parent Clause or control	Secondary	Source	Sub-Category description	Threats	Wider Category
1	Protection against malware shall be implemented and supported by appropriate user awareness.	1	1	A.8.7	A.8.7		ISO 27001	Protection against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Protection against malware
2	the scan carried out should include: 1) scan any files received over networks or via any form of storage medium, for malware before use;	2	10	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
3	the scan carried out should include: 2) scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;	3	11	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
4	the scan carried out should include: 3) scan web pages for malware;	3	12	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
5	h) defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;	4	13	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
6	i) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements (see 12.3);	5	14	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
7	j) implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware;	4	15	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
8	k) implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them;	5	16	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
9	l) isolating environments where catastrophic impacts may result	5	17	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
10	The use of two or more software products protecting against malware across the information processing environment from different vendors and technology can improve the effectiveness of malware protection	5	18	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
11	a) establishing a formal policy prohibiting the use of unauthorized software (see 12.6.2 and 14.2.);	3	2	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware
12	b) implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting);	3	4	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy	Controls against malware

Figure 23 Example of free-text search using filters

4.2.3.7 Exporting Results

When working with subsets of measures containing thirty entries or fewer, users may export the results into CSV or Excel formats for further analysis. Exported files retain the structure and metadata of the measures, allowing organizations to integrate the information into internal reviews, risk assessments, or compliance planning exercises. A typical export screen is illustrated in Figure 24, demonstrating how results can be easily extracted for offline use.

Description of Measures	Level	Numbering per par	Paragraph	Parent Clause or control	Secondary	Source	Sub-Category description	Threats	Wider Category
Protection against malware shall be implemented and supported by appropriate user awareness.	1	1	A.8.7	A.8.7		ISO 27001	Protection against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code, Malware, Cyberstalking, Spyware, Viruses, Worms, Damage caused by a third party, Electronic Emanations - information-bearing spurious emissions associated with all electronic equipment (prevented by TEMPEST equipment or shielding), Cyberwarfare, Eavesdropping, Cracks, Cross-Site Scripting XSS, Computer warfare (including physical disruption of communication satellites etc)	Protection against malware
the scan carried out should include: 1) scan any files received over networks or via any form of storage medium, for malware before use;	2	10	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code, Malware, Cyberstalking, Spyware, Viruses, Worms, Damage caused by a third party, Electronic Emanations - information-bearing spurious emissions associated with all electronic equipment (prevented by TEMPEST equipment or shielding), Cyberwarfare, Eavesdropping, Cracks, Cross-Site Scripting XSS, Computer warfare (including physical disruption of communication satellites etc)	Controls against malware
the scan carried out should include: 2) scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;	3	11	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code, Malware, Cyberstalking, Spyware, Viruses, Worms, Damage caused by a third party, Electronic Emanations - information-bearing spurious emissions associated with all electronic equipment (prevented by TEMPEST equipment or shielding), Cyberwarfare, Eavesdropping, Cracks, Cross-Site Scripting XSS, Computer warfare (including physical disruption of communication satellites etc)	Controls against malware
the scan carried out should include: 3) scan web pages for malware;	3	12	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code, Malware, Cyberstalking, Spyware, Viruses, Worms, Damage caused by a third party, Electronic Emanations - information-bearing spurious emissions associated with all electronic equipment (prevented by TEMPEST equipment or shielding), Cyberwarfare, Eavesdropping, Cracks, Cross-Site Scripting XSS, Computer warfare (including physical disruption of communication satellites etc)	Controls against malware
h) defining procedures and responsibilities to deal with malware protection on systems,	4	13	A.8.7	A.12.2		ISO 27002	Controls against malware	Corporate crime, Trojan, Malicious Software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, Malicious code, Malware, Cyberstalking, Spyware, Viruses, Worms, Damage caused by a third party, Electronic Emanations -	Controls against malware

Figure 24 Image Description: Example of export in excel format

4.2.4 CAC – Conformity Assessment & Compliance

4.2.4.1 CAC Introduction

Conformity Assessment and Compliance (CAC) tool supports users (SMEs) in both ex-ante and post-market monitoring activities, enabling them to meet rigorous market expectations. The tool features an automated self-assessment process with full visualization, allowing SMEs to clearly understand the requirements and identify potential gaps.

The tool includes comprehensive technical documentation management capabilities. It assists users in the creation of technical documentation in line with the requirements of the Cyber Resilience Act (CRA). The CAC Tool also enables the import of Software Bill of Materials (SBOM), allowing users to “better know” the key components of their software products.

The post-market analysis functionality provides SMEs with insights into the product's status after market entry. The tool can generate several essential reports, such as the Declaration of Conformity, Maturity Status, SBOM analysis, and technical documentation summaries.

The tool provides information and a step-by-step guide on the Technical Documentation requirements as introduced in Annex VII – Contents of the technical documentation of the CRA.

The tool also provides information of what each content of the technical documentation means and provide a space where information can be provided (either in open text or as an attachment). The tool has the ability to facilitate the implementation of a self-gap analysis of the available technical documentation in comparison to the requirements of Annex VII of the CRA. The tool adopts user-readable models to conceptualize and automate the self-conformity process.

The CAC service has a multi-faceted goal:

- To determine the level of stringency and depth of the evaluation that should be applied, considering the assurance level set for each digital element of the product.
- To provide a visual representation of the validation checks and tests that should be performed to ensure compliance with cybersecurity standards and certification schemes.
- To visually guide SMEs in providing evaluation proofs, evidence that justify the extent to which security requirements have been fulfilled.
- To evaluate the digital products based on the provided technical documentation and all the relevant evidence and proofs that the assurance level that has been set has been reached.
- To benchmark the maturity of a digital product in terms of addressing requirements.
- To generate a statement of conformity (DoC) the completion of the evaluation process for digital products.
- The tool incorporates advanced compliance management capabilities that empower SMEs with actionable intelligence and provide insightful, customizable reports.
- The tool can produce technical documentation as defined in the CRA in the form of enriched reports.

CAC service key features:

- Explain to the users that only basic tests should be performed to validate the cyber resilience of products with digital elements, for which a 'basic' assurance level has been considered.
- Guide the SME through the process of checking compliance with the CRA and visualize the whole process.
- Guide the SME through the process of uploading technical documentation, as well as “evidence” to justify which security requirements are fulfilled.
- Evaluate digital products based on the uploaded evidence (documentation) with assurance level.
- Generate a Declaration of Conformity (DoC) as proof attesting to the completion of the evaluation process.
- Generate an enriched report based on the uploaded and required technical documentation, in accordance with the CRA.
- Implement Post-market Analysis/Monitoring capability with notification to the SME about new vulnerabilities or new regulatory/legal changes in CRA.

4.2.4.2 CAC registration and login

To access the application, the user should open a web browser and navigate to the following URL: https://web.cac-cyber.com/ . The user should see the screen as depicted below in Figure 25.

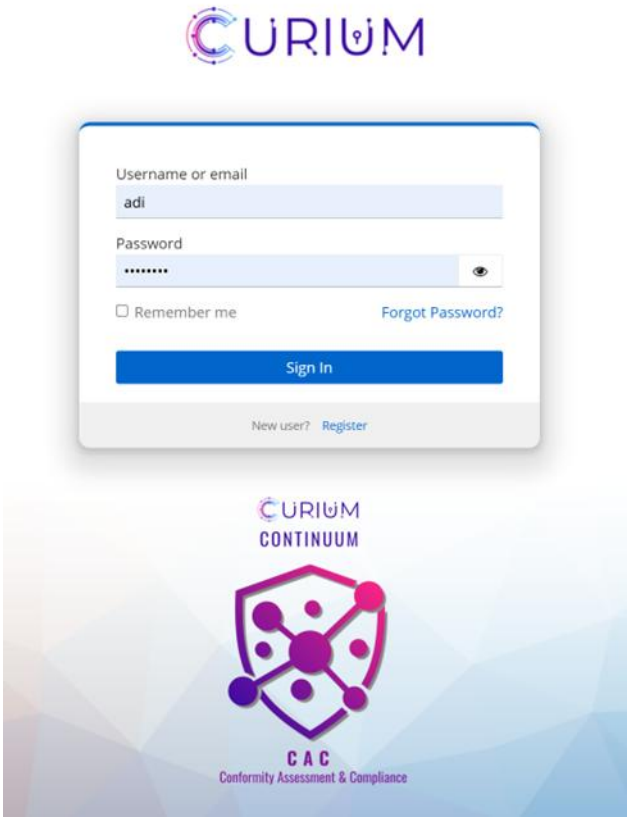


Figure 25 CAC tool

Once the user opens the URL, the login page will appear.

- If the user already has an account, they should enter email address and password, then click the "Login" button to access the system.
- If the user does not have an account, they should click on the "Register" button to begin the account creation process as shown in Figure 26.

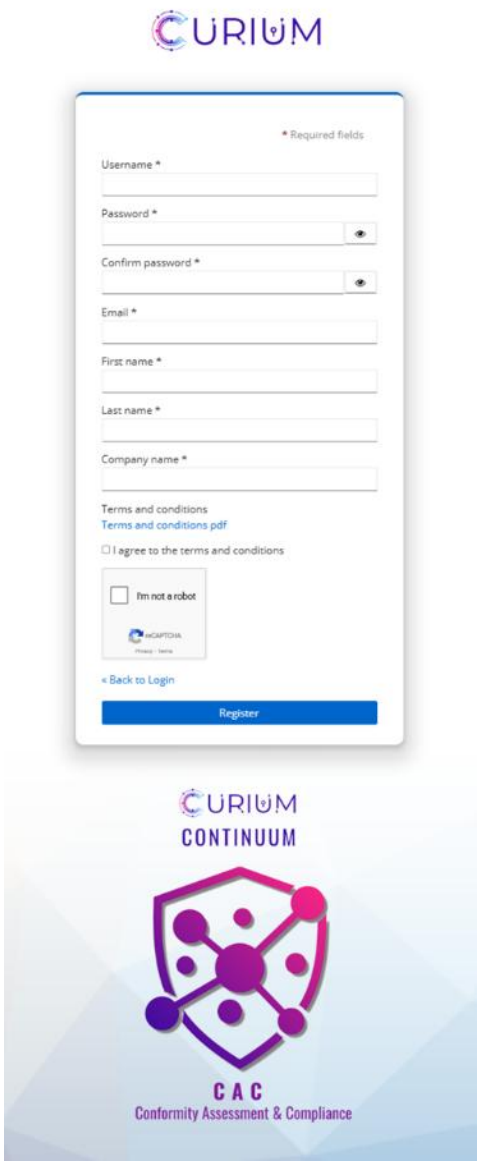


Figure 26 User registration

On the registration page, the user is required to fill out a form with the necessary information to create a new account, verify account through its email and start using application.

After successful login, the user can edit account information, upload e.g. company's logo, signature, download Terms and conditions and User Manual.

4.2.4.3 CAC Adding new product and evaluation

Upon entering the application, the user is presented with a list of available products. Initially, the list is empty. By clicking the “Add new product” button, the user begins the process of creating a new product.

A form then appears for entering the basic product information, and after entering all mandatory data and clicking the “Save” button, the new product appears in the product list, and a wizard for product assessment is automatically opened containing a product questionnaire.

Immediately after the questionnaire responses are saved, a wizard for uploading technical documentation for the newly created product is displayed.

Product overview screen shows information about the product. In this screen user can check and modify product information, see Figure below.

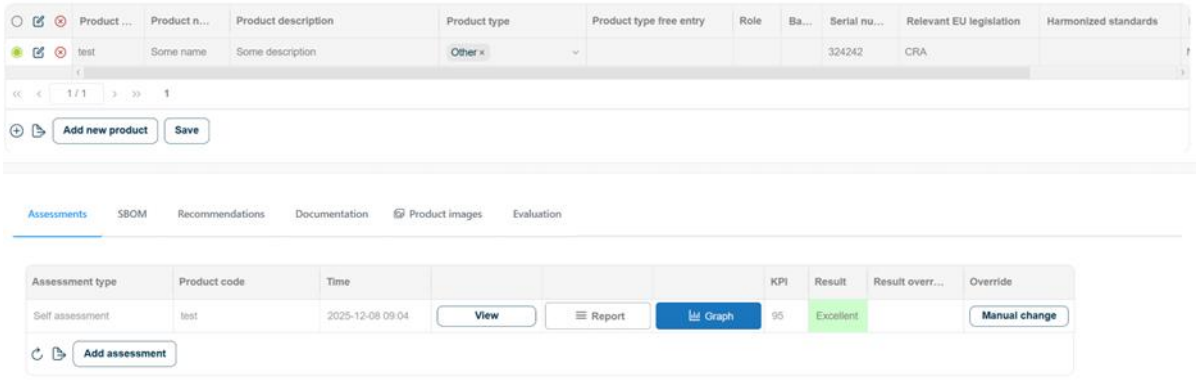


Figure 27 Product information

By clicking on edit button in a row, it opens a dialog for editing product information.

In the Assessment tab the user can manage product assessments. Products assessments are questionnaires where each answer is scored, and the sum of these per-question scores upon submitting produces a total points result that is graded into three categories (e.g. "Bad" for 0-50%, "Good" for 50-75%, or "Excellent" 75-100%). The final result can also be displayed as a chart. Also, the result can be manually overridden, with an optional override comment.

First assessment is filled when new product is added. If necessary, a product can be re-assessed multiple times by creating and filling out additional copies of the questionnaire. This is performed by clicking Add assessment button.

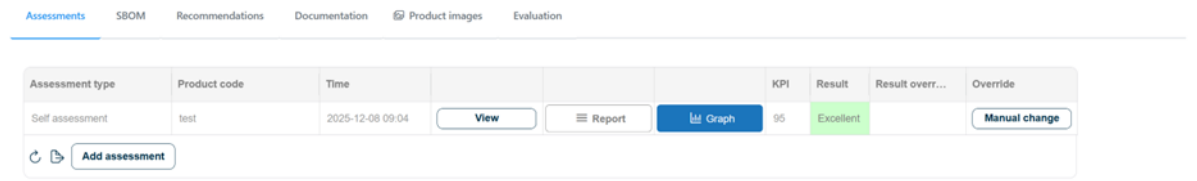


Figure 28 Assessment Tab

Each assessment has following information:

- **Assessment type** – Type of assessment - always *Self assessment*.
- **Product code** – Read only identifier of the assessed product).
- **Time** – Timestamp when the assessment was created or last updated.
- **Edit** – Opens the assessment form for changes.
- **Report** – Opens a detailed report view (scoring, checks, evidence).
- **Graph** – Opens a KPI/metrics chart for this assessment.
- **KPI** – Numeric score or key performance indicator (e.g., 36).
- **Result** – Qualitative outcome derived from KPI (e.g., *Bad, Good, Excellent*).
- **Result override** – Shows the current override status/value if any.
- **Override** – Button to change the computed result manually.

- **Override comment** – Free-text reason recorded with an override.

By selecting View button, product assessment is displayed in table format to review questions and responses.

By clicking on Report button, summary representation of assessment is shown, as in Figure 29.

Category	Points	Percentage	Percentage_status
DATA	4	100	Excellent
PRODUCTS	9	100	Excellent
VULNERABILITIES	8	88	Excellent
	21	95	Excellent

« ‹ 1 / 1 › » 1

Number of records: 4

Figure 29 Report

By clicking on Graph button, summary representation of assessment is shown as a graph, see figure below:

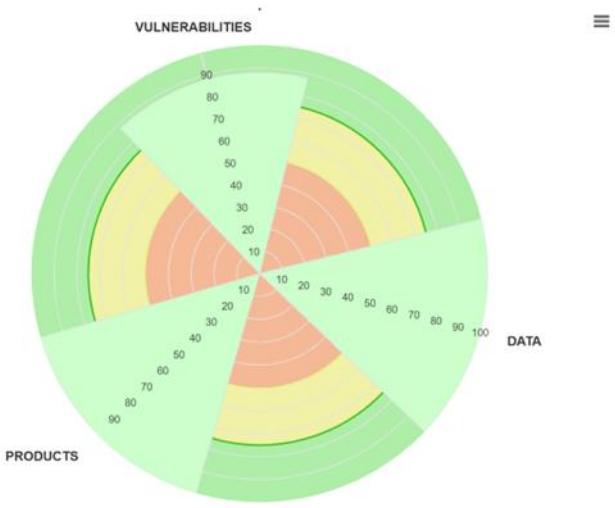


Figure 30 Graph

On the SBOM tab, an interface is displayed containing a table with a list of uploaded SBOM files for the selected GRC product (in SPDX 2.3 format). SBOM is short for Service bill of materials. This is a list of all third party libraries that are used in creation of product with digital elements.

The user is responsible for obtaining the SBOM file, as it cannot be generated within the CAC application.

By clicking on a specific row in the table that lists SBOM document versions, a tree structure appears below the table, showing all components that make up the product, along with highlighted vulnerabilities and their descriptions.

On Recommendations tab, user can see recommendations for problems with uploaded SBOM file, assessment questionary and missing documentation. Each record has a Category value that specifies what was the input for recommendation.

Documentation is mandatory for every product.

Under the Documentation tab, a table is displayed where each row corresponds to a specific type of document that must be uploaded as part of the documentation process.

Initially, the table contains information about the document type and the group to which that type belongs. Other values are filled in once the documentation for a specific document type is uploaded.

By clicking the edit icon in a row, a wizard opens, displaying a form for uploading a document corresponding to that row. The user can choose between the following options:

- Upload
- Later
- Not Applicable

After uploading a "Technical details – SBOM" document, the system automatically triggers a file evaluation, and the evaluation results are recorded in the SBOM tab.

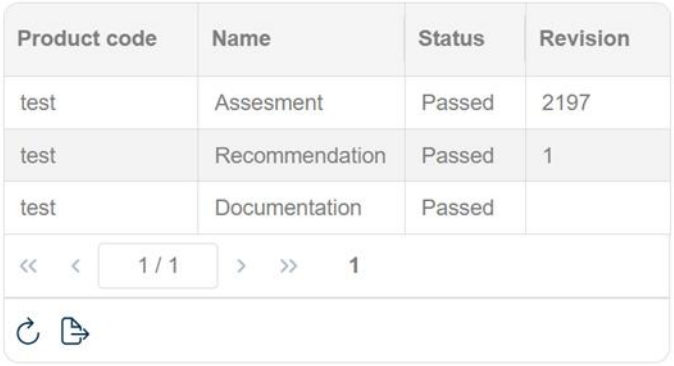
By clicking on the Modules Dropdown in the main menu and selecting the GRC (Governance, Risk, Compliance) Product

item, a table with an overview of the entered GRC products is displayed.

Rows in the table can be selected, and upon selection, a new view with tabs is opened. Clicking the Evaluation button opens an interface containing a component for product evaluation which can be used to create an EU Declaration of Conformity.

The user can also upload images associated to evaluated product, under Product images tab.

Button Start evaluation starts a new evaluation. All steps must be ”Passed” for the evaluation to be Passed, see Figure 31 below. In that case EU Declaration of Conformity can be generated, as shown in Figure 31.



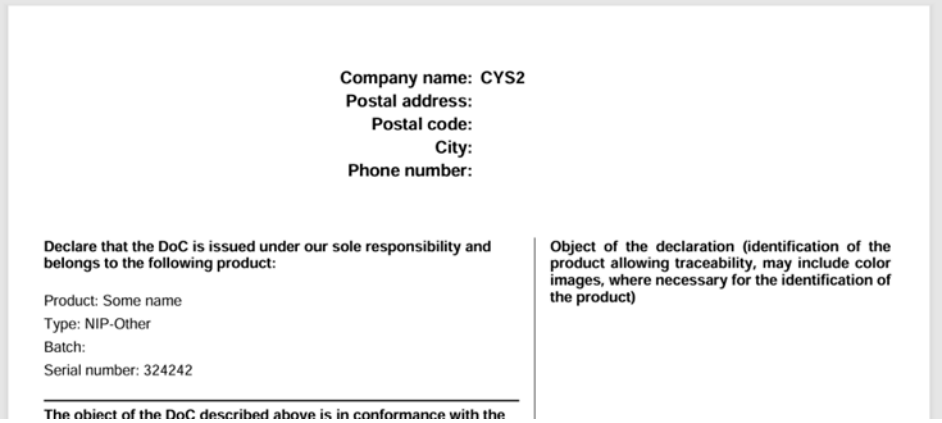


Figure 31 Generated DoC

4.2.4.4. Customizable CAC capabilities

Future roadmap (after releasing beta version) of service implementation:

- Advanced visualization of the full CRA compliance journey.
- Enhanced reporting features and technical documentation summaries.
- Post-market monitoring capabilities with automated alerts on new vulnerabilities or regulatory updates under the CRA.
- CAC tool will be extended to support CRA and requirements for future products, processes and services in cybersecurity domain.

4.2.5 PSTVA – Penetration Self-Testing & Vulnerability Assessment

Scope

The PSTVA toolkit deploys an extensible platform to enable organizations to proactively identify and mitigate security risks through automated network and web security scans This solution integrates established open-source instruments including Nmap for network discovery, Nikto for web server auditing, Ffuf for directory and parameter fuzzing, and Kerbrute for Active Directory enumeration, collectively delivering granular insights into system vulnerabilities, misconfigurations, and potential attack surfaces. The deployment emphasizes operational efficiency, scalability, and minimal resource overhead, ensuring cost-effective enhancement of organizational security posture while facilitating compliance with regulatory frameworks through standardized vulnerability reporting.

This deployment targets cybersecurity professionals and teams focused on strengthening security posture and ensuring regulatory compliance (e.g., via standardized vulnerability reporting). It supports scalable testing workflows for web applications, databases, networked devices (switches, routers, firewalls, servers), and exploitability checks (e.g., buffer overflows, underflow/overflow errors, SQL injections, XSS). Results are consolidated in a unified format, including vulnerability descriptions, impacts, prioritized remediations (patches, reconfigurations), and threat metrics, stored for advanced querying. The scope excludes custom tool development, it leverages Docker for portable, isolated deployment across systems.

Architecture

The PSTVA architecture manifests as a fully containerized, microservices-oriented platform orchestrated entirely through Docker containers, ensuring deterministic isolation, reproducible deployments, and zero-dependency execution across diverse host systems. At its core, FastAPI serves as the RESTful API gateway, providing robust endpoint orchestration, input validation via schemas, and synchronous request handling, while Celery distributed task queue, broker through Redis, manages asynchronous scan execution. This decoupling enables horizontal scaling of worker nodes to process high-volume assessment campaigns without blocking the API layer.

- **Client Layer**: Handles project creation and assessment initiation via a dashboard or external client software.
- **API Layer**: FastAPI manages REST endpoint orchestration, request validation, and integration with client connections.
- **Security Layer**: Implements Basic RBAC authentication/authorization using JWT tokens and API keys.
- **Task Layer**: Celery workers (with Redis as broker) dispatch and monitor asynchronous scan tasks, providing real-time visibility and control.
- **Data Layer**: Neo4j graph database stores results for querying relationships between assets, services, and vulnerabilities; supports read/write operations and report generation.

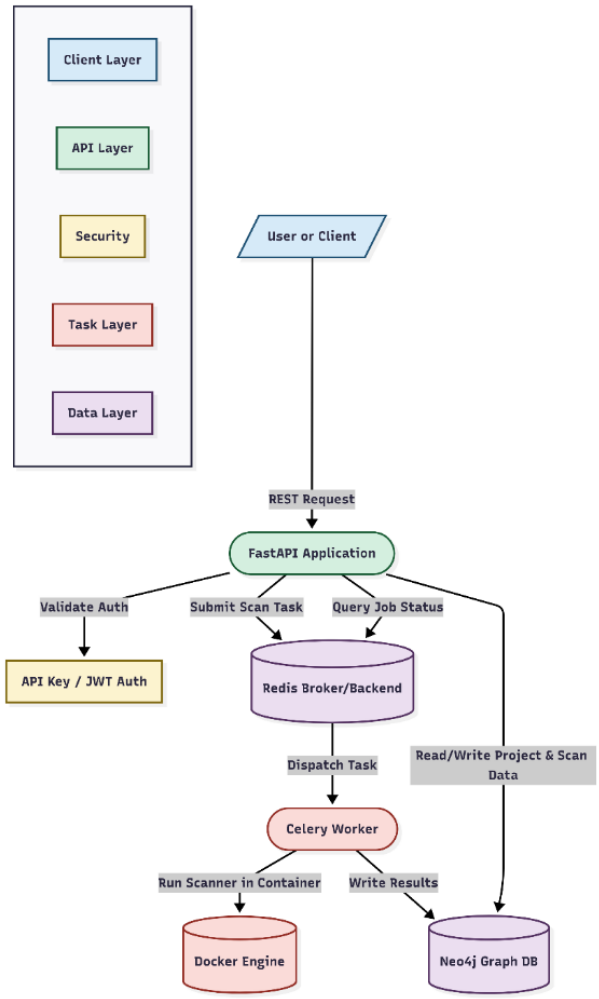


Figure 32 Architecture

Key Concepts

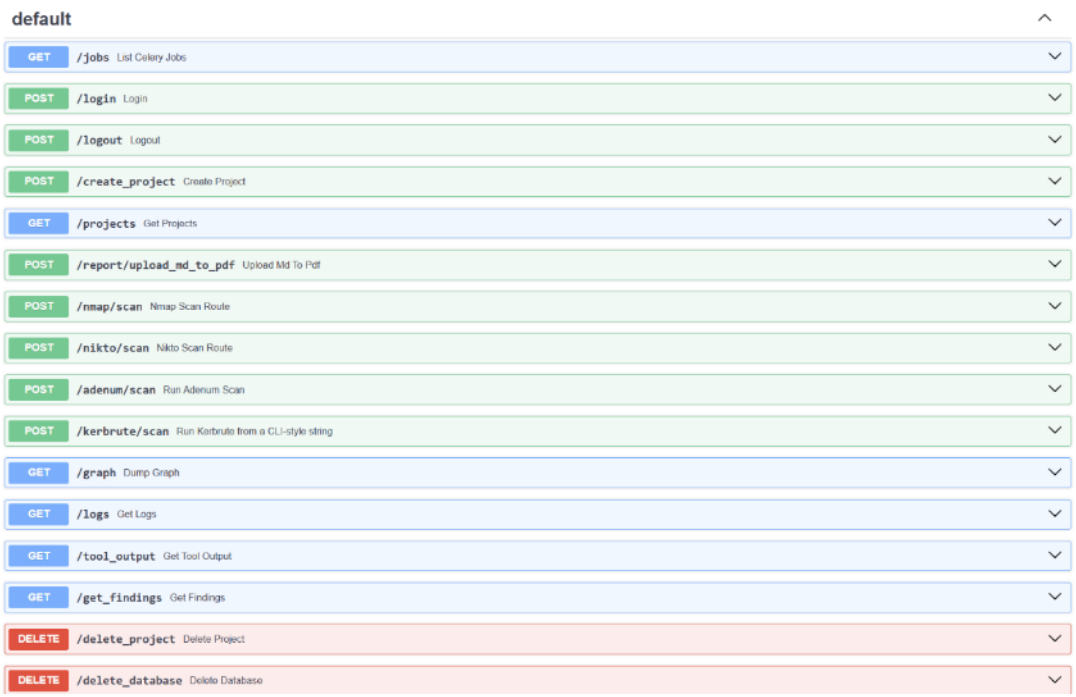
Central to PSTVA functionality are vulnerability scanners stratified into two primary categories: web application and database scanners, which conduct directed analysis against HTTP endpoints and backend data stores to detect canonical weaknesses such as SQL injection payloads, cross-site scripting vectors, and least-privilege violations; and network vulnerability assessment tools exemplified by Nmap, which perform comprehensive host discovery, service enumeration, and vulnerability fingerprinting across networked assets including infrastructure devices and endpoints, identifying implementation flaws like buffer overflow exposures and protocol misconfigurations.

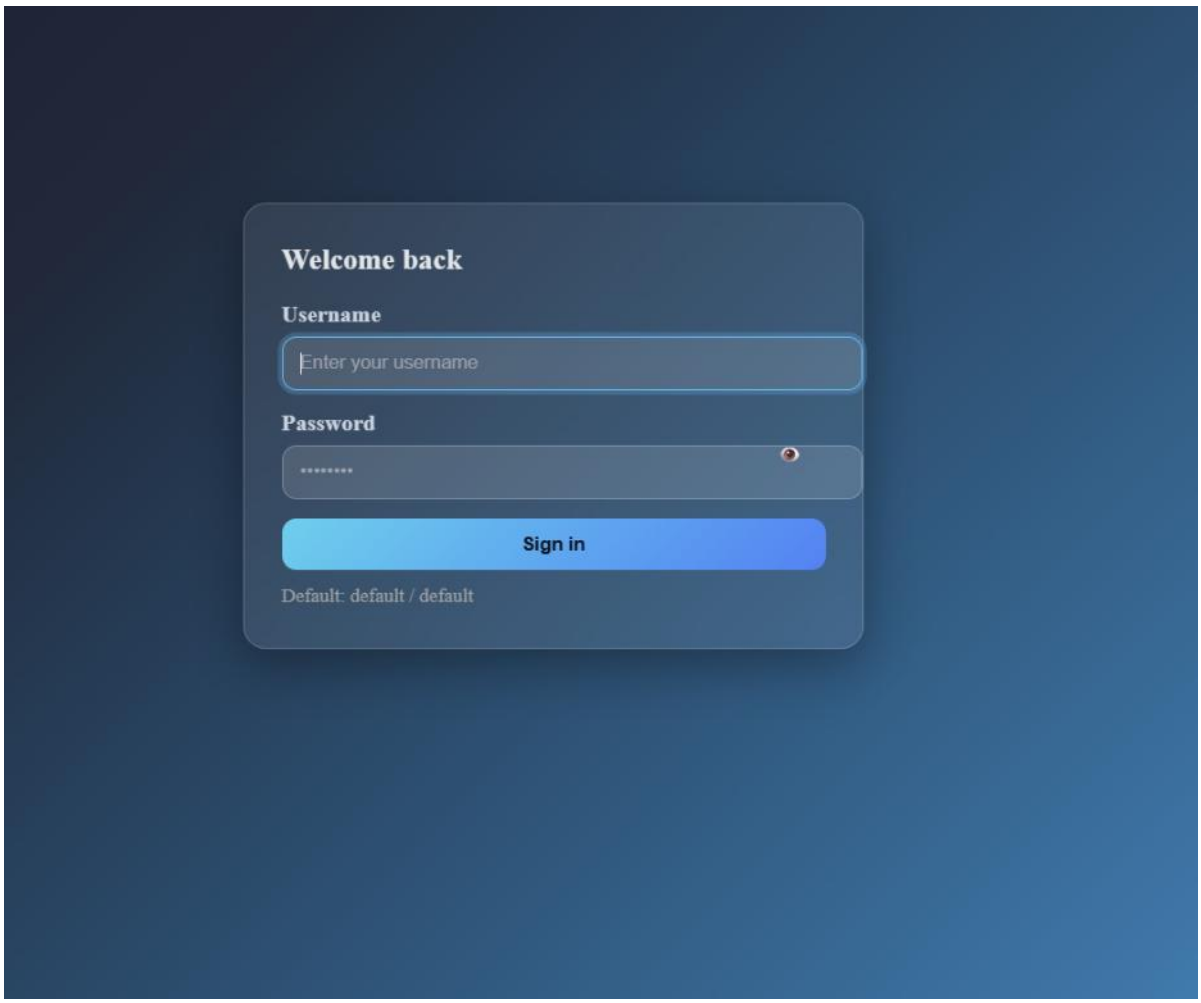
Asynchronous orchestration via Celery and Redis implements a producer-consumer pattern optimized for distributed scan workloads, where task serialization minimizes inter-process communication latency and enables fault-tolerant retry mechanisms. Neo4j's graph-native storage paradigm excels in modeling cybersecurity ontologies, representing vulnerabilities as nodes with directional edges to affected assets and services, thereby supporting advanced analytics such as blast radius computation and multi-hop exploit chain identification through graph traversal. Docker-mediated isolation enforces principle-of-least-privilege execution environments for each scan instance, coupled with the platform's low-overhead design, achieved through ephemeral container lifecycles and efficient result parsing, renders it suitable for continuous integration into production security monitoring pipelines. Standardized output consolidation bonds to formats like CVE descriptors and CWE classifications, ensuring interoperability with enterprise vulnerability management systems.

User Flow

The PSTVA simple user workflow follows a structured, dashboard-driven sequence designed for cybersecurity professionals, commencing authentication and culminating in actionable reporting.

- **Login**: Access the dashboard at and authenticate using JWT tokens or API keys via the FastAPI security layer, granting access to project management interfaces and Swagger-documented endpoints.


default
GET /jobs List Celery Jobs
POST /login Login
POST /logout Logout
POST /create_project Create Project
GET /projects Get Projects
POST /report/upload_md_to_pdf Upload Md To Pdf
POST /nmap/scan Nmap Scan Route
POST /nikto/scan Nikto Scan Route
POST /adenum/scan Run Adenum Scan
POST /kerbrute/scan Run Kerbrute from a CLI-style string
GET /graph Dump Graph
GET /logs Get Logs
GET /tool_output Get Tool Output
GET /get_findings Get Findings
DELETE /delete_project Delete Project
DELETE /delete_database Delete Database


Welcome back
Username
Enter your username
Password
Sign in
Default: default / default

- **Create Project**: Initiate a new project through the client interface to group related scans, leveraging CRUD operations for organization and scoping assessment campaigns.

Figure 33 Create Project page

- **Select Tool**: Choose the appropriate scanner from available options—Nmap for network discovery, Nikto for web vulnerability assessment, Ffuf for directory fuzzing, or Kerbrute for enumeration—based on target requirements.
- **Configure Scan Type**: Specify scan parameters including targets, ports, scope, and execution options, with real-time validation ensuring input integrity prior to submission to the Celery task queue.

Figure 34 Scan type

- **Monitor via Celery Tab**: Track asynchronous execution in real-time through the Celery monitoring interface, viewing job states from Redis, worker progress, logs, and detailed process metrics for ongoing scans.

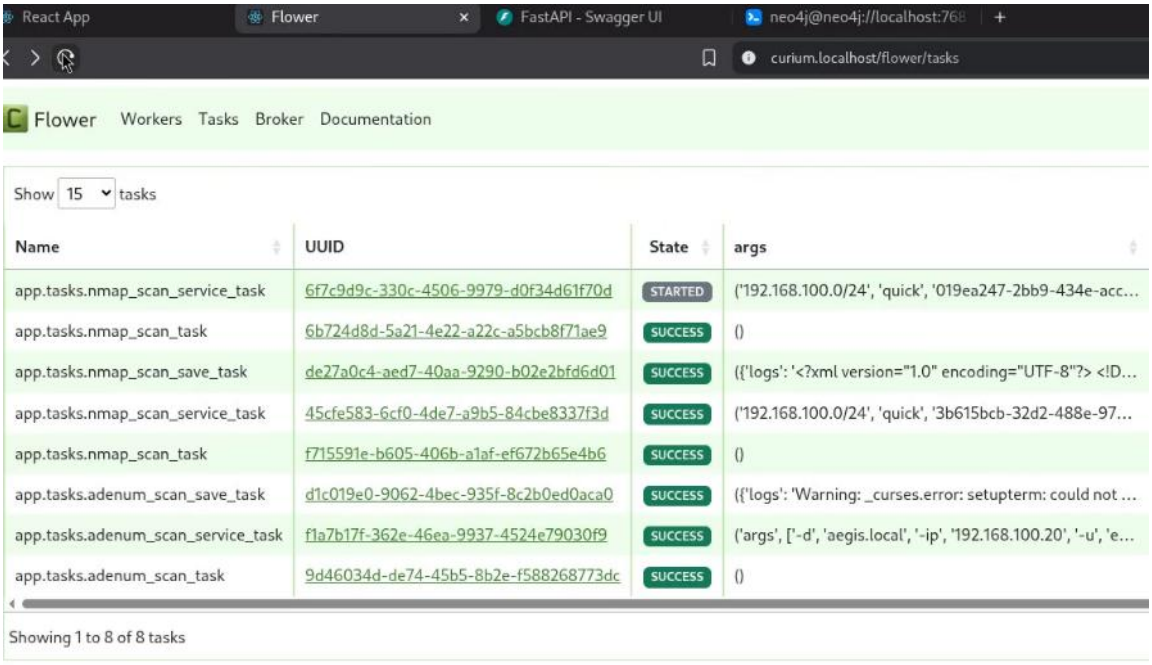


Figure 35 Metrics for on-going scans

- **View Process Details**: Drill down into specific task instances to inspect execution status, intermediate outputs, and any anomalies, enabling proactive intervention if required.

- **Retrieve Scan Results**: Upon successful completion, access parsed results directly in the dashboard, including vulnerability details, CVE correlations, severity scores, and Neo4j graph visualizations of asset-service relationships.

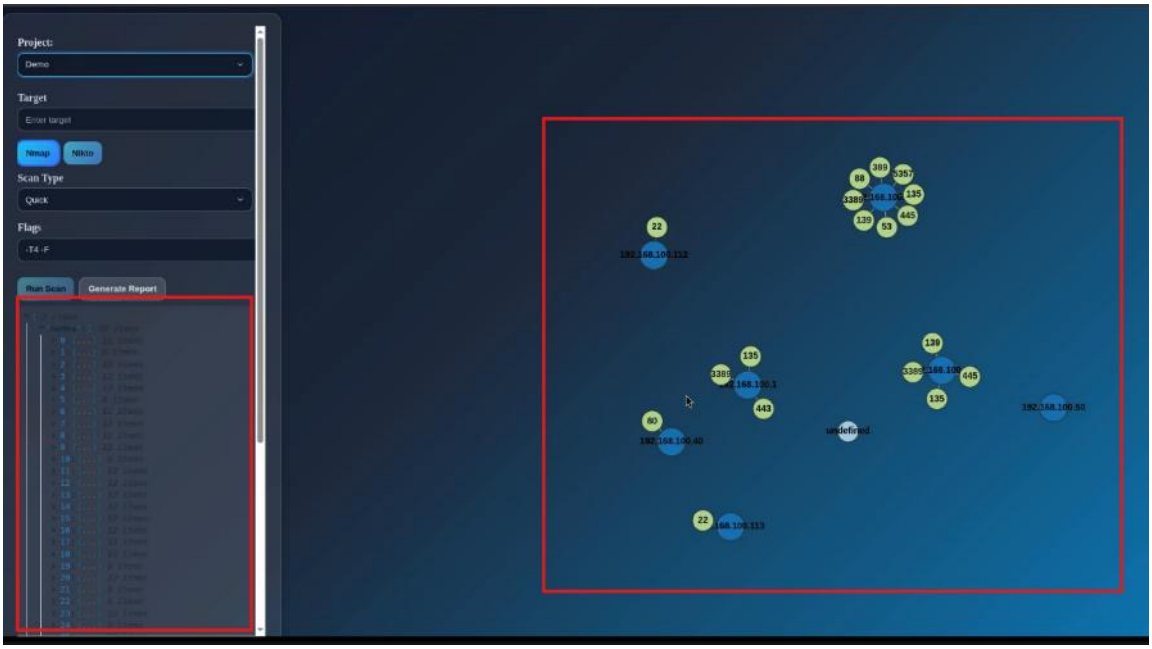


Figure 36 Scan results

- **Conduct Vulnerability Assessment**: For tools like Nikto, review web-specific findings such as SQLi, XSS, or misconfigurations, complete with impact analysis and prioritized remediations.

- **Generate Report**: Trigger automated report creation via User interface or API endpoints, consolidating findings into structured JSON, or PDF formats for compliance and user review.

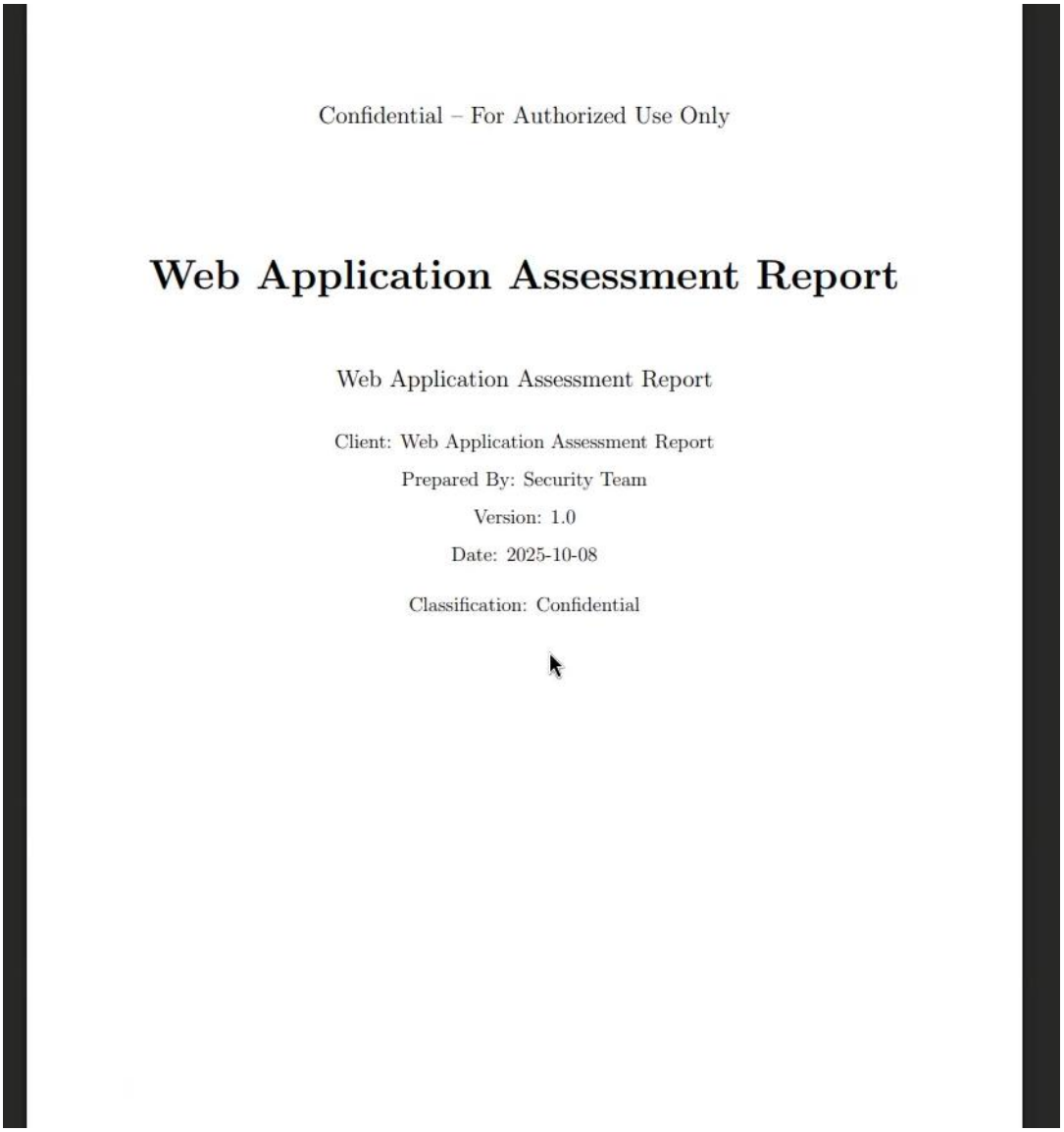


Figure 37 Full report

- **Validate Security Posture**: Analyze final PDF outputs and CVE mappings to assess overall risk posture, plan remediations, and iterate on subsequent scans within the project context.

- Reference: https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D

4.0.3 3. CVE-2024-38474 (Critical)

Field	Value
ID	192.168.100.40:80-21
Severity	Critical
Affected	192.168.100.40:80 (Apache/2.4.58 (Ubuntu) Apache/2.4.58 (Ubuntu) -)
Status	Open
CVSS	9.8
Remediation Summary	Patch or mitigate the affected service.
References	https://vulners.com/cve/CVE-2024-38474

Vulnerability observed on `192.168.100.40:80`.

- Service: Apache/2.4.58 (Ubuntu)
- Product: Apache/2.4.58 (Ubuntu)
- Version: -
- Reference: https://vulners.com/cve/CVE-2024-38474

5. Deployment Strategy

The deployment of the CURIUM Compliance Continuum is a critical step in ensuring that the tools and services developed in WP3 are operational, accessible, and usable by SMEs, micro-enterprises, and other stakeholders. Task 3.2 focuses on establishing the technical and operational conditions for the progressive release of the Continuum, beginning at M7, and on refining deployment through iterative updates based on feedback from validation. First big release of the tools and services was planned for M8, where is to expect minimum TRL 6 of the tools.

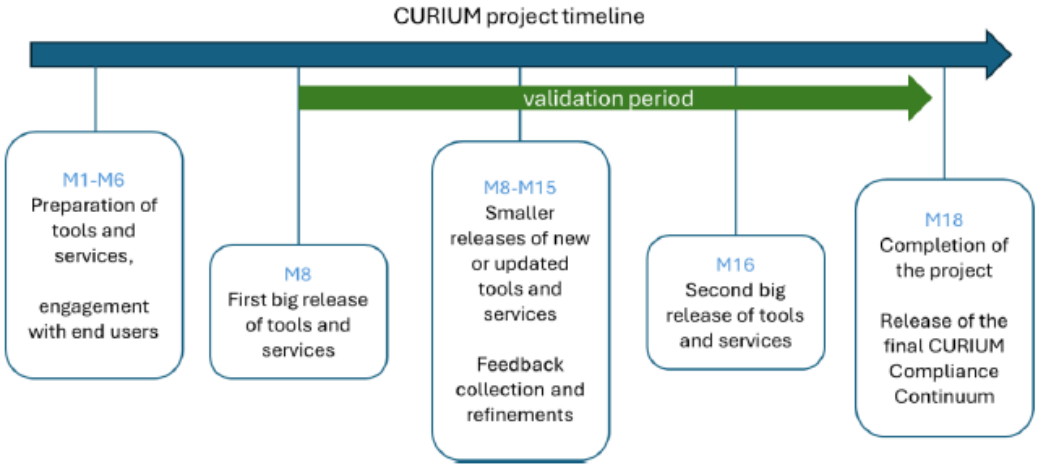


Figure 38 CURIUM validation strategy with the timeline

5.1 Deployment environments and infrastructure (timelines and methodology)

The deployment follows an incremental release methodology, common in Horizon Europe projects, where an early prototype (alpha release) is delivered to internal partners, followed by staged public releases (beta and stable). The timeline is aligned with project milestones:

- M8: Initial deployment of core services in a controlled environment (alpha release).
- M15: First, smaller public pilot release to selected SMEs and project partners (beta release).
- M18: Iterative updates with refined features, scalability improvements, and regulatory adjustments and final stable release with full functionality and training/support resources. (Figure 38)

The infrastructure is designed with modularity and scalability in mind, enabling each tool to be deployed independently while remaining accessible via the unified CURIUM platform (SSO).

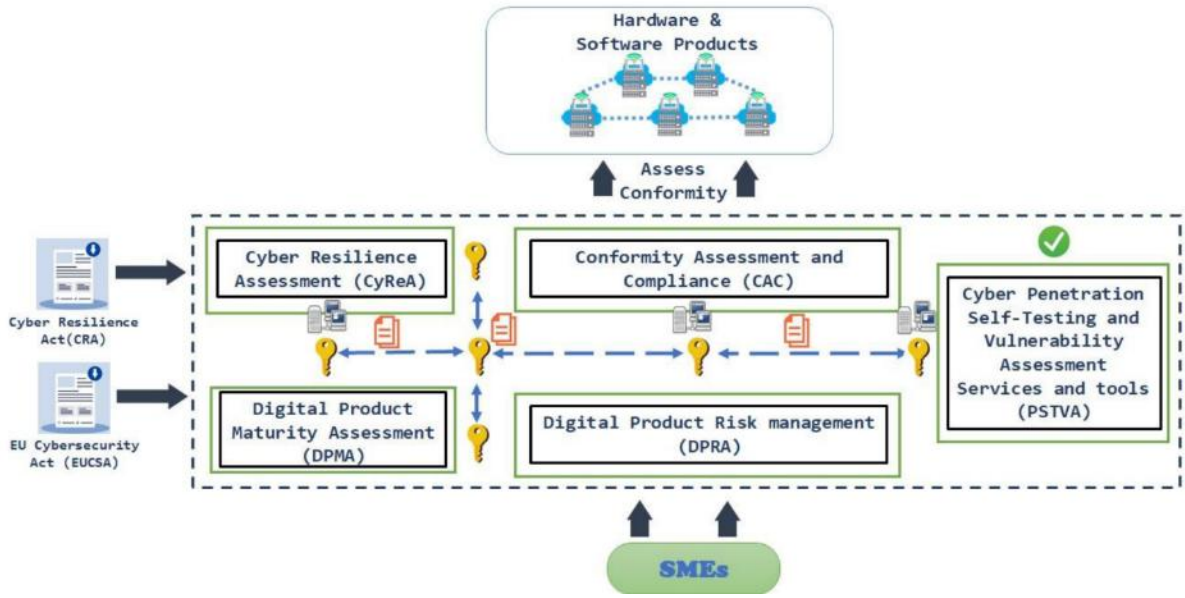


Figure 39 CURIUM Blueprint

Interoperability mechanisms have already been implemented with the following functionality: SSO/Keycloak, standard export formats (CSV/Excel, PDF/JSON), SBOM SPDX import, etc.

To meet its objectives, the proposed Compliance Continuums provides a bundle of Services and tools customized to the constraints and requirements of SMEs, specifically particular of the small and micro enterprises, which will be seamlessly integrated into a unified platform. In particular, the proposed Continuum (Figure 39) will incorporate and implement five distinct groups of Services and tools:

Cyber Resilience Assessment service: The Cyber Resilience Assessment (CyReA) service, will introduce its users to the main facts of the CRA (b) shall guide them – through a series of questions – in identifying if they fall under the scope of the CRA and – if yes – in which category their products fall under. Since, based on the CRA, the type of conformity assessment imposed is dependent on the type of product, the results extracted from the usage of the CyReA service, shall also provide them with a clear identification of whether their product(s) need to undergo a third-party conformity assessment process or not.

Digital Product Risk management: *The Digital Product Risk management (DPRA) service*, will allow users to undertake an assessment of the cybersecurity risks associated with each of their products with digital elements that fall within the scope of the CRA (as identified by the CyReA). The outcome of this assessment is required to be used by the manufacturer during the planning, design, development, production, delivery and

maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing security incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.

Digital Product Maturity Assessment: *The Digital Product Maturity Assessment (DPMA) service*, will allow the manufacturers to look up risk mitigation measures per risk in relevant libraries. These measures shall be ranked on a maturity scale based on existing maturity models. The manufacturer shall be able to take into account the intended use, the level of identified risks and the existing capabilities in selecting the suitable maturity level and the corresponding mitigating actions.

Conformity Assessment and Compliance service: *The Conformity Assessment and Compliance (CAC) service*, will provide information and a step-by-step guide on the Technical Documentation requirements as introduced in ANNEX VII - CONTENTS OF THE TECHNICAL DOCUMENTATION of the CRA. The tool shall provide information of what each content of the technical documentation means and provide a space where information can be provided (either in open text or as an attachment). The tool shall also have the ability to facilitate the implementation of a self- gap analysis of the available technical documentation in comparison to the requirements of Annex VII of the CRA. The manufacturer should have the ability to fulfil some of the requirements of the technical documentation by utilizing services of the Compliance Continuum (e.g. risk assessment, risk treatment measures, SBOM, vulnerability reports, penetration testing reports etc).

Penetration Self-Testing and Vulnerability Assessment Services and tools: *The Penetration Self-Testing and Vulnerability Assessment Services and tools (PSTVA)* is a comprehensive, customizable toolkit designed for efficiency and simplicity in order to support manufacturers, particularly SMEs, in navigating their compliance journey against the CRA. It integrates a variety of capabilities, including vulnerability assessment, code review, and penetration testing, to perform robust security assessments of digital artifacts and Active Directory environments. At the end, it concludes with the generation of detailed and customizable reports that highlight security issues, risk levels, and mitigation guidance.

Table 3 Release Snapshot

Nr.	***Tool***	***Version***	***Status***	***TRL***
1	*CyReA*	*1.0*	*Deployed, accessible, operational*	*TRL6-7*
2	*DPRA*	*1.0*	*Deployed, accessible, operational*	*TRL6-7*
3	*DPMA*	*1.0*	*Deployed, accessible*	*TRL6-7*
4	*CAC*	*0.9*	*Deployed, accessible*	*TRL6*
5	*PSTVA*	*1.0*	*Accessible, operational*	*TRL6-7*

At the time of this deliverable, the CURIUM tools are assessed at Technology Readiness Level (TRL) 6–7[17], CAC TRL6[18]. The solutions are fully integrated, deployed, and demonstrated in relevant operational environments,

[17] TRL6-7 means that the tools are fully deployed web-based, accessible, operational in controlled environment and used in early validation activities

[18] TRL6 means that the tool is deployed, accessible, operational including assessment, documentation and reporting

corresponding to TRL 6. In parallel, several components are being actively used in early operational validation activities with external stakeholders and pilot use cases, marking the transition toward TRL 7. As these operational validation activities are still ongoing, the maturity is expressed as TRL 6–7 to reflect both the achieved level and the progression toward full operational demonstration.

5.2 Continuous deployment process & DevOps pipelines

The deployment strategy adopts a DevOps approach, with continuous integration and deployment (CI/CD) pipelines established to ensure rapid iteration. This includes:

- Automated builds, testing, and deployment using GitLab CI/CD.
- Containerized services (Docker/Kubernetes) to simplify portability and scalability.
- Regular release cycles with change logs and backward compatibility for SMEs.
- This approach ensures that bug fixes, security patches, and new features are delivered without service disruption.

5.3 Compliance coverage per CRA Annexes

This section describes how the deployment of the CURIUM Compliance Continuum supports compliance with the Cyber Resilience Act (CRA) by mapping deployed tools and services to the relevant CRA annexes. The mapping reflects how CURIUM operationalizes regulatory requirements through technical means, while acknowledging that legal responsibility for compliance remains with the manufacturer of products with digital elements.

The mapping between deployment outputs and CRA requirements is maintained as a compliance matrix, updated in line with regulatory changes (See full mapping in Annex I)

5.4 Challenges, known limitation & Mitigation during deployment

There are several challenges which are anticipated in the deployment of the Compliance Continuum:

- Heterogeneous SME environments: SMEs differ in maturity, resources, and digital infrastructure.
  Mitigation: Provide flexible deployment options (cloud, on-premise if needed, if needed sandbox for testing).
- Functionality overlapping issues between tools developed by different partners.
  Mitigation: Tools are autonomous and APIs will not interact, they will have unified authentication (Keycloak SSO).
- Regulatory updates during project lifetime (CRA delegated acts, harmonized standards).
  Mitigation: Continuous monitoring of regulatory sources and flexible update cycles in CI/CD pipeline.
- Performance and scalability concerns when tools are scaled to larger SME networks.
  Mitigation: Cloud-native architecture with scaling and stress-testing.
- User adoption barriers due to complexity of compliance processes.
  Mitigation: Simplified UI, training materials, and capacity-building activities under Task 3.4.

6. Continuous Feedback Collection & Tools Refinement

Task 3.3 is responsible for collecting all feedback from the WP4 validation activities, analyzing it, and defining the needs for re-design and further adjustments of the tools/services and the overall CURIUM Compliance Continuum. It serves as the link between WP4, where assessments of CURIUM solutions are collected from external stakeholders, and WP3, where this input is translated into concrete fine-tuning actions. This process ensures that the development of the Continuum is user-driven and continuously improved based on real-world testing.

6.1 The Feedback Management Framework

To systematically manage the flow of information, a comprehensive Feedback Management Framework had to be established. This framework governs the entire lifecycle of a feedback item, from its collection to its resolution.

The main tool for implementing this framework is the **Feedback-to-Action Tracker**. This shared repository was designed to provide a transparent and traceable log for all stakeholder input. It captures key information for each feedback item, including its source, the CURIUM component it relates to, its assigned priority, the type of action required, its status, etc. The **Feedback-to-Action Tracker** is a central log designed to systematically capture, analyse, prioritise, and monitor the resolution of all feedback received from stakeholders during the project's validation rounds. Its goal is to ensure that feedback is transparently processed and translated into concrete fine-tuning actions for the CURIUM Compliance Continuum, its tools, and its training materials.

The Feedback-to-Action Tracker is structured with the following fields to ensure comprehensive management of all inputs, as shown in Table 3:

Table 4 Structure and Field Definitions of the CURIUM Feedback-to-Action Tracker

Field	Description
Feedback ID	A unique code (e.g., FDBK-001) for tracking and referencing the feedback item.
Date Reported	The date the feedback was formally logged, typically corresponding to a validation activity.
Source	The specific event or activity that generated the feedback (e.g., Internal Workshop, SEC Forum 2025).
Stakeholder Group	The type of user or stakeholder providing the input (e.g., SME, consultant, internal partner).
CURIUM Component	The specific tool, service, or resource the feedback applies to (e.g., CAC, DPMA, CURIUM Portal).
Feedback Summary	A concise, one-sentence summary of the issue or suggestion.
Feedback Category	Classification of the feedback type, such as Usability, Functionality, Performance, or Documentation.
Priority	The assessed urgency for addressing the feedback (e.g., High, Medium, Low), determining its place in the refinement queue.

Action Type	The nature of the work required to resolve the feedback (e.g., Technical Refinement, Documentation Update).
Assigned To	The consortium partner(s) responsible for implementing the required action.
Action Description	A specific, clear description of the task to be performed by the assigned partner.
Status	The current state of the action item (e.g., In Progress, Done, Paused).
Target Release	The planned project release (e.g., v1.1, Hot Fix) in which the resolution is scheduled to be deployed.
Resolution Notes	A brief note detailing how the feedback was ultimately addressed or resolved.

All incoming feedback is analysed and prioritised based on a combination of factors, including:

- **Criticality** to core compliance goals
- **Frequency** of the feedback across different stakeholder groups
- **Technical feasibility** and **effort**

This structured approach ensures that development resources, through each refinement phase, are focused on the most valuable refinements.

6.2 Execution of the First Feedback Cycle

For each validation activity that took place during the first validation period, a structured report containing all the gathered feedback was generated.

- The process for logging this feedback is currently being executed as follows:
- Step 1 – Consolidation: All raw feedback (including survey results, interview notes, comments during hands-on sessions and presentations, etc.) is being collected by WP4 and synthesized into a structured report to ensure no input is lost.
- Step 2 – Triage: The T3.3 lead, in cooperation with the relevant tool owners (WP3 partners), reviews each incoming feedback item and validates it.
- Step 3 – Logging: Each distinct item is logged in the Feedback-to-Action Tracker, where it is assigned a unique ID, categorized, and given an initial priority based on the criteria defined in Section 6.1.
- Step 4 – Assignment: Items are formally assigned to the responsible consortium partner for resolution, with a target release date set based on the complexity of the required action and/or its severity.

This rigorous process will allow the consortium to convert qualitative feedback from the first validation round into actionable technical tasks.

6.2.1 Tool-specific feedback patterns and early lessons learned

The execution of the first feedback cycle has already produced **tool-specific insights**, particularly for the Conformity Assessment and Compliance (CAC) tool and the Penetration Self-Testing and Vulnerability Assessment (PSTVA) toolkit. While the overall Feedback Management Framework applies uniformly across the Compliance Continuum, the nature of the feedback and the resulting refinement actions differ significantly depending on the target user profile and tool complexity.

Feedback related to the CAC tool

Feedback collected during CAC demonstration and validation activities primarily reflects the perspective of **SMEs and non-expert users** engaging with CRA compliance processes for the first time. Recurring themes include the need for clearer guidance on regulatory expectations, especially in relation to **CRA Annex VII technical documentation**, and improved clarity regarding assessment scoring and conformity outcomes.

Users highlighted that, while the CAC workflow is logically structured, additional contextual explanations are required to better understand:

- Why specific documentation artefacts are requested,
- How questionnaire scores are calculated and interpreted,
- How assessment results translate into conformity readiness and the generation of the EU Declaration of Conformity (DoC).

Based on this feedback, several refinement actions have been logged in the Feedback-to-Action Tracker, including:

- The introduction of **contextual help texts and tooltips** linked directly to CRA provisions,
- The provision of **example templates and guidance notes** for Annex VII documentation fields,
- Improved visual explanations of assessment scoring, result categories, and override mechanisms.

These actions aim to further reduce the compliance burden for SMEs by increasing transparency and usability, while preserving the regulatory accuracy of the CAC outputs

Feedback related to the PSTVA toolkit

In contrast, feedback for the PSTVA toolkit primarily reflects the needs of **technical users and cybersecurity practitioners**, while also highlighting challenges faced by SMEs with limited penetration-testing expertise. Validation activities revealed that users value the technical depth and flexibility of PSTVA but require additional support to efficiently configure scans and interpret results in a compliance-oriented context.

Key feedback themes include:

- The perceived complexity of scan configuration parameters for non-expert users,
- The need for clearer prioritisation and explanation of identified vulnerabilities,
- The desire for reports that more explicitly link technical findings to CRA obligations, particularly Annex I (Part II) vulnerability handling requirements.

In response, refinement actions have been defined to:

- Introduce **simplified, pre-configured scan profiles** tailored for SME use cases,
- Enhance result visualisation and vulnerability prioritisation guidance,
- Improve reporting outputs by explicitly mapping vulnerabilities and remediation actions to CRA-aligned evidence artefacts.

These refinements ensure that PSTVA maintains its technical robustness while becoming more accessible and actionable for SMEs operating without dedicated security teams. [19]

[19] In the time of writing this deliverable, phase of collecting the feedback from the Stakeholders after Cyprus event is in the place.

6.2.2 Updated status and integration into future refinement cycles

The initial analysis of CAC and PSTVA feedback confirms that **user needs vary significantly across tools**, reinforcing the importance of a flexible, tool-aware feedback management approach. The Feedback-to-Action Tracker has proven effective in capturing these nuances and translating them into prioritised, actionable refinement tasks.

As feedback collection activities continue within WP4, further iterations will focus on:

- Strengthening consistency of user guidance across tools,
- Enhancing CRA traceability of outputs and reports,
- Aligning training and support materials with the most frequently reported user challenges.

The iterative integration of tool-specific feedback ensures that the CURIUM Compliance Continuum evolves in line with real-world SME usage, supporting both regulatory compliance and practical adoption throughout the project lifecycle.

6.3 Current Status and Future Plans

As of the submission of this deliverable, the Feedback Management Framework has been fully deployed and proved effective in structuring the initial intake of data, ensuring a transparent and auditable link between stakeholder needs and technical development. The consortium is currently in the active phase of populating the Feedback-to-Action Tracker with the results from the initial activities of the first validation cycle.

The Feedback-to-Action Tracker will continue to be the central instrument for managing this iterative refinement process, ensuring the CURIUM Compliance Continuum remains aligned with user requirements throughout the project's lifecycle.

At the time of this deliverable, initial feedback collection activities are ongoing. Preliminary observations indicate recurring needs related to user guidance clarity, tool functionality expectations, and documentation usability. These inputs are being consolidated and will inform prioritisation in the next development cycle.

7. Capacity Building, Training & Support

The present chapter reports on designed and implemented activities within the scope of task T3.4 titled CURIUM support, knowledge, and capacity building. It documents

a. training resources to support the use of services and tools of the Compliance Continuum (section 7.1);
b. training activities related to CRA compliance and mainly targeted to SMEs (section 7.2);
c. activities aiming to raise awareness (section 7.3);
d. activities aiming to build capacity and knowledge through experimentation, testing and advisory services (section 7.4);
e. networking and collaboration activities for extensive outreach and validation of the project's outcome and generated knowledge.

Presented activities implement the Knowledge and Capacity Building Plan, as has been documented in Chapter 6 of D.2.2, submitted in June 2025. They take due account of the insights gained from the stakeholders' survey, which was performed the first months of the project and addressed CRA related needs, challenges and expectations.

7.1 Training resources on CURIUM Continuum

The Compliance Continuum is the core strategic idea of CURIUM. Rather than focusing on a single scanner or checklist, the project builds a holistic assessment framework that can evaluate digital products both individually and in the context of their wider system interconnections. It is explicitly tailored for SMEs and micro-enterprises and is intended to simplify compliance processes while remaining cost-effective and modular. In other words, it recognises that small manufacturers need more than legal explanations: they need repeatable workflows and practical tooling that map directly onto the CRA's lifecycle obligations.

Within this framework, CURIUM brings together five key services which are accessed through the CURIUM portal **https://portal.curium-project.eu.** The project's website (https://curium-project.eu/) is being updated to properly promote and link to the portal. Each service of the compliance continuum in the portal is accompanied by a description and an intuitive and easy to follow user manual, briefly introduced in the following.

Cyber Resilience Assessment (CyReA) Tool
User Manual

The CyReA tool aims to systematically verify that ICT products with digital elements (ICT products) have been robustly assessed and comply with the essential requirements mandated by the CRA. It provides structured questionary-based wizard designed to facilitate and streamline the compliance assessment of Products with Digital Elements (ICT products) against the requirements of the EU Cyber Resilience Act (CRA). The initial step of CyReA is to determine the scope of CRA for the organisation based on their legal role including Manufacturer, Importer, Distributor, Authorized Representative, and End User under the CRA.

Digital Product Risk Management (DPRA) Tool
User Manual

DPRA is an evidence-driven, stepwise dynamic approach which aims to determine the compliance of ICT products based on the associated assets and their risks and controls to mitigate the risks. The tool adopts open intelligence in real time to identify the vulnerabilities and threats that are linked with the assets, and standards like NIST 800-53 and ISO/IEC 15408 for unified security declaration and control. The user manual provides a step-by-step guide to organizations to the offered capabilities for managing their security risks in a holistic and cost-effective manner by assessing both individual and cascading risk taking into account the vulnerabilities and threats that are linked with the ICT product.

Digital Product Maturity Assessment (DPMA) Tool
User Manual

The Digital Product Maturity Assessment (DPMA) Tool is designed to support SMEs, micro-enterprises and start-ups in identifying relevant cybersecurity measures for digital products in a simple and practical way. The tool provides access to a consolidated and structured dataset of cybersecurity measures, aligned with the Cyber Resilience Act (CRA) and widely adopted standards such as ISO 27001, ISO 27002, NIST 800-53, CIS V8 Controls and others. The User Manual is intended for SMEs, micro-enterprises and start-ups, product managers and technical leads, non-expert users involved in product development, maintenance, or compliance planning. No advanced cybersecurity or regulatory expertise is required to use the tool.

Conformity Assessment and Compliance (CAC) Tool
User Manual

The Conformity Assessment and Compliance (CAC) Tool is being developed to support SMEs in ex-ante compliance activities and help them meet emerging market expectations. It provides an automated self-assessment process with visual guidance, allowing users to clearly understand the requirements and identify potential gaps. The tool also includes capabilities for managing technical documentation in line with the Cyber Resilience Act (CRA) and enables the import of Software Bill of Materials (SBOM) to define key components of software products. The User Manual provides a guide to the provided tool capabilities including informing users about the level of needed assessment depending on the assurance level 'basic' or 'substantial', evaluation and assignment of assurance level, and generation of a Declaration of Conformity.

Penetration Self-Testing and Vulnerability Assessment (PSTVA) Services and Toolkit
User Manual

PSTVA is an extensible platform for orchestrating and storing results from network and web security scans. It integrates multiple scanning technologies (Nmap, Nikto, ADenum, Kerbrute) and manages results and metadata using a Neo4j graph database. The system leverages FastAPI for RESTful orchestration, Docker for tool isolation, Redis for distributed task brokering, and Celery for asynchronous scan management. The User Manual provides step-by-step instructions for installation, operation, and advanced usage tailored to cybersecurity professionals.

Video tutorials, based on the user-manuals, are under preparation and will feature in the project's website and other promotion channels.

7.2 CRA compliance training

To support CRA adoption across Europe, capacity building activities are designed, organised, and performed. They include training on CRA-related EU policies and regulations, and are designed to involve end-users, security providers and standardisation and certification experts in a continuous feedback loop.

The capacity building activities are on-going and in the present document we present the ones that were implemented within 2025.

Prepare Your SME for EU Cyber Rules – Training Session

On September 25, 2025, CURIUM, in collaboration with SME4DD, hosted an online training session aimed at helping small and medium-sized enterprises (SMEs) understand and prepare for the upcoming EU cybersecurity regulations. The event was designed to provide practical, actionable insights and training to SMEs, guiding them through the key compliance requirements of the new rules.

The training featured expert speakers who provided clear explanations of the regulations and practical tools tailored to the unique needs of SMEs. Argyro Chatzopoulou from Apiroplus Services, Esther Garrido Gamazo from 28DIGITAL, and Asja Kamenica from 28DIGITAL shared their expertise, offering step-by-step advice on how SMEs can start preparing or improve their current cybersecurity practices.

The session covered the most pressing aspects of the new EU rules, offering SMEs the resources to assess their current state, identify gaps, and implement effective solutions. Attendees gained relevant knowledge on practical tools, tips, and insights that would help them navigate the new regulatory landscape.

As a training activity, this session reinforced CURIUM's commitment to supporting SMEs in building their cybersecurity capacity and ensuring they are well-equipped for compliance with the upcoming regulations. It provided a valuable opportunity for SMEs to gain the knowledge needed to strengthen their digital resilience in line with EU requirements.

Internal Trainings and Tools Presentations

Several internal training sessions were held to showcase the tools developed within the CURIUM project, providing valuable opportunities for feedback and collaboration among project partners. Overall, 30 participants received training on the CURIUM tools being developed.

- On 4 November 2025, a 90-minute online session was conducted, during which Cyber Security Ltd. and NeaLogic presented their tools, CAC, CyReA and DPRA, to partners' members of staff. The CURIUM

partnership involves SMEs, security solutions providers, suppliers and producers of digital assets. Around 10-15 participants attended, and tool owners collected feedback to further enhance their tools, ensuring they meet the needs of users effectively.

- On 11 November 2025, another 90-minute online session took place, where AEGIS and Apiroplus Services presented their tools, PSTVA and DPMA, to partners' members of staff. Again, 10-15 participants attended, providing valuable feedback for the continuous improvement of the tools.

These training sessions not only facilitated the sharing of tools but also created an ongoing loop of feedback and improvement, enhancing the usability, effectiveness and ultimately adoption of the tools being developed by the project.

CURIUM's Active Support for the CRA Cluster and CYBERSTAND Working Groups

CURIUM is actively engaged in the CRA Cluster activity organized by Cyberstand and has appointed representatives in all three key community groups. These groups focus on technical interoperability, training and outreach, and standardization.

In the Technical Community Group, CURIUM contributes to coordinating the interoperability of tools developed across various EU projects. This group is working to map out CRA coverage, identify gaps, and create common formats for data exchange, allowing SMEs to easily transition between tools based on their needs. In the standardization group, CURIUM is involved in coordinating feedback to standards and contributions to standardisation activities including information on use cases.

In the outreach and training community group, which is the most relevant to the scope of the present chapter, the general aim is to co-ordinate among projects the outreach, education and training activities to SMEs. The group will put effort to streamlining and where applicable integrating or linking offered material and eliminating duplication. The group will also co-ordinate the timing and content of the various capacity building activities of the projects and create a calendar of events and engagement initiatives.

Through its participation in these groups, CURIUM is contributing to building practical, interoperable solutions and resources that support SMEs in meeting CRA requirements and enhancing their cybersecurity resilience.

7.3 Awareness Raising Activities

In the present section, awareness raising activities implemented in the second semester of 2025 are presented.

Cyber Security & Resilience Workshop at Techritory 2025

The Cyber Security & Resilience Workshop organised by p-NET Emerging Networks & Verticals at Techritory 2025 served as a significant **awareness-raising activity** for the CURIUM project. Held in Riga on 23 October 2025, the event provided a high-visibility platform for informing the audience about the growing cybersecurity challenges affecting next-generation communication infrastructures.

Experts from research, industry and regulatory bodies participated, and CURIUM was presented alongside three other EU-funded projects - NATWORK, SAND5G and CUSTODES. Their joint presence acted as an effective clustering activity, allowing CURIUM to raise awareness not only of its own objectives but also of the wider ecosystem of European initiatives working to enhance network security and resilience.

Throughout the workshop, participants explored the increasing importance of cybersecurity certification as networks become more complex and critical to societal functions. A central message communicated to the audience was that technical security alone is insufficient; trust must be reinforced through compliance with EU cybersecurity regulations and emerging certification schemes. This offered CURIUM a valuable opportunity to raise awareness of its mission to provide practical tools and frameworks that support organisations - particularly SMEs - in understanding and navigating these certification requirements.

The discussions also highlighted the urgency of addressing new and rapidly evolving cyber threats, including those driven by AI, underscoring the need for forward-looking resilience strategies. By gathering diverse stakeholders, the workshop helped spread understanding of how European research and innovation projects can work together to strengthen the security foundations of future communication systems.

For CURIUM, the event functioned not only as dissemination but as a targeted effort to increase awareness of the project's relevance, solutions, and contribution to Europe's cybersecurity landscape. By participating in this workshop and clustering with related EU initiatives, CURIUM helped promote the importance of accessible certification support and contributed to broader awareness of the collective effort required to build a resilient and trustworthy digital society.

During the workshop, CURIUM partners CYS and AEGIS had the opportunity to present their tools and showcase them in a demo exploration session where participants had the opportunity to engage directly with project teams for further insights.

Figure 40Techritory Forum

Figure 41 CURIUM presentation on Techritory

COcyber Concertation Workshop at DIGITALEUROPE

The first COcyber Concertation Workshop, held on 19 November 2025 at DIGITALEUROPE and organised by AMETIC, brought together ten EU cybersecurity projects, including CURIUM, to explore practical ways of collaborating across Europe's cybersecurity and digital trust ecosystem.

The workshop raised awareness of shared priorities and aligned participants around five cooperation pillars: networking and communication, policy alignment, knowledge and technology transfer, research and innovation, and skills and training. Through breakout sessions, participants identified joint opportunities, compared tools and datasets, and defined initial collaborative tasks. The event highlighted the importance of coordinated action and set the stage for tangible outputs over the next twelve months, including joint policy briefs, co-hosted events, coordinated skills activities, and shared technology assets.

Figure 42 Cocyber event

Cybersecurity Fair in Nicosia, Cyprus

The Cybersecurity Career Fair was held on 25 and 26 November 2025 at the ICT Academy of the Office of the Commissioner of Communications in Nicosia and was organized by the Office of the Commissioner of Communications in collaboration with the Digital Security Authority (DSA).

This two-day event brought together students, graduates, and cybersecurity professionals to explore career opportunities, academic pathways, and practical roles in the field of digital security, as part of the European Cybersecurity Month initiative. The event aimed to raise awareness of the growing importance of cybersecurity in today's digital world and to engage stakeholders in building knowledge and interest in the sector.

The CURIUM project participated with a dedicated booth, providing visitors with information on its objectives and activities, including capacity building, training, and innovation in cyber resilience. The event offered an opportunity to inform attendees about CURIUM's role in supporting organisations and individuals in developing the skills and understanding needed to strengthen cybersecurity preparedness.

Through this awareness-raising activity, participants gained insight into emerging career and learning opportunities in cybersecurity, while also learning about practical tools and initiatives, such as those developed by CURIUM, that contribute to building a more resilient digital ecosystem in Europe.

Figure 43 Cyber-security fair in Cyprus

CURIUM at the ISACA Athens Chapter Conference 2025

On 4 December 2025, the ISACA Athens Chapter Conference 2025 brought together cybersecurity professionals, CISOs, policy makers, researchers, and others in the digital security field. The National Cybersecurity Authority of Greece (NCSA) hosted a booth at the Decoding Digital Trust exhibition to promote and raise awareness of the CURIUM project. This outreach activity aimed to raise awareness of CURIUM's tools for Cyber Resilience Act (CRA) compliance and engage attendees with information about the project.

At the booth, participants learned about CURIUM's objectives, received informative flyers, and subscribed to the project newsletter. The event served as an excellent opportunity for CURIUM to connect with industry professionals and contribute to the ongoing effort to strengthen digital security and trust across Europe.

Figure 44 ISACA conference

Preparing Stakeholders for CRA Compliance – Awareness-Raising and Hands-On Engagement

The Office of the Commissioner of Communications, in collaboration with the Digital Security Authority of Cyprus (DSA), hosted a dedicated awareness-raising event to inform stakeholders about the latest developments related to Cyber Resilience Act (CRA) compliance. Also serving as an information day, the event took place on 11 December 2025 at the ICT Academy, Nicosia – Office of the Commissioner of Communications and was attended by stakeholders from across Cyprus.

The event featured live demonstrations and hands-on sessions of the CRA compliance support tools. Demonstrations were delivered by Cyber Security Ltd., AEGIS, NeaLogic and Apiroplus Services enabling participants to explore how the tools assist in interpreting regulations, identifying compliance gaps, and implementing necessary measures.

By combining awareness-raising with practical engagement, the workshop provided stakeholders with both knowledge and direct experience using the CURIUM tools. This approach reinforced the project's mission to support organisations, particularly SMEs, in navigating the evolving CRA regulatory landscape and enhancing cybersecurity readiness.

Figure 45 Prepare stakeholders - awareness

7.4 Testing, Experimentation and Advisory Services

CURIUM leverages the capabilities of p-NET's **Testing and Experimentation Facility (TEF)**, which has the capability to support a range of activities such as:

- hosting equipment vendors for conformance testing;
- developing and testing new functionality, services, applications;
- performing KPI Measurements and cybersecurity assessments;
- conformance and interoperability testing aligned with 3GPP and EU 5G security recommendations;
- supporting hands-on training for operators, businesses, regulators and researchers.

p-NET's TEF offers a unified and fully operational smart network and services environment suitable for a wide range of experimentation activities. It allows controlled testing and supports end-to-end validation of network functions, services, and performance characteristics. In the following, illustrative example categories of experiments that can be supported are presented.

Traffic, Behaviour and Anomaly Observation

Experiments examining network behaviour under typical, atypical or artificially generated conditions:

- monitoring traffic patterns and workload variations
- examining system response under congestion or bursts
- detecting unexpected usage patterns or deviations
- studying the interaction of multiple concurrent service types.

Robustness, Resilience and Incident Handling Exercises

Testing how the infrastructure reacts to disruptions or unexpected events:

- resilience under high load or partial component failure
- response to misconfigurations or unintended behaviour
- validation of monitoring, alerting and operational procedures
- time-to-recover measurements after controlled disturbances.

In addition, a **Project HelpDesk** is set-up at the Patras Science Park. It is operated by p-NET and serves as a physical point of presence of the CURIUM project. The HelpDesk informs about and facilitates access to the services delivered by the project and support the physical and on-line interfacing of interested individuals to CURIUM participants, facilities, and activities. It facilitates the set-up of advisory sessions with experts on every module of the CURIUM Continuum.

7.5 Collaboration and Sustainability

Networking and collaboration activities are implemented to build and reinforce connections and synergies among partners, as well as with other established or emerging networks and initiatives in the field of cybersecurity and resilience compliance at both European and global levels. Through these efforts, CURIUM aims to promote innovation, support knowledge and technology transfer, enhance trust, and improve communication—ultimately strengthening the EU's security posture. These efforts include creating cooperative links with relevant initiatives, projects, and organizations to facilitate knowledge exchange, promote the uptake of CURIUM results, and validate their relevance and acceptance. In doing so, the project will help ensure that CURIUM solutions remain sustainable and continue to deliver value beyond the project's lifetime.

To boost collaboration activities and clustering, NSCA and involved partners, have prepared and started implementing a dedicated, direct communication campaign for the last months of 2025. The campaign includes the reach out and setting up meetings and bilateral communications with:

a. relevant to CURIUM projects for synergies in the design and delivery of joint dissemination events, workshops, webinars, open discussions etc.
b. Direct communication with National Authorities from Member States, for sharing the CURIUM 1st release of solutions and lessons learned within the first half of the project.
c. Active participation by CURIUM Partners in ECCC's and ENISA's planned activities, which involve projects. These activities are part of Task 5.3 and will be documented in detail in deliverable D5.2 in M18.

Conclusion

Deliverable D3.1 has documented the first consolidated release of the CURIUM Compliance Continuum, representing a major milestone in the implementation of Work Package 3. The work presented demonstrates how regulatory requirements stemming from the Cyber Resilience Act (CRA) have been translated into a coherent, modular, and SME-oriented ecosystem of tools, services, and capacity-building resources.

Through the adaptation and deployment of five core services—CyReA, DPRA, DPMA, CAC, and PSTVA—the CURIUM project delivers a practical compliance pathway that supports the entire lifecycle of products with digital elements. These tools collectively address key CRA obligations, including risk management, secure design, vulnerability handling, conformity assessment, technical documentation, and post-market monitoring, while maintaining proportionality and usability for SMEs and micro-enterprises.

In parallel, the establishment of a unified deployment strategy, continuous integration pipelines, and a structured feedback management framework ensures that the Compliance Continuum is not static but evolves iteratively based on validation results and stakeholder input. The integration of training materials, user manuals, awareness activities, and advisory services further strengthens the project's capacity-building dimension, ensuring that technical solutions are accompanied by the necessary knowledge and skills for effective adoption.

The results achieved under WP3 confirm that CURIUM goes beyond theoretical compliance guidance by offering operational, evidence-based instruments that lower the barrier for SMEs to meet CRA requirements. While the first release already demonstrates significant maturity (TRL6-7), ongoing refinement, extended validation, and deeper integration with regulatory updates will remain priorities for the next project phases.

References

1. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
2. https://digital-strategy.ec.europa.eu/en/policies/cra-summary
3. ISO/IEC 15408 (Common Criteria)
4. https://curium-project.eu/
5. https://curium-project.eu/wp-content/uploads/2025/07/public-deliverable-D2.2.pdf
6. https://curium-project.eu/wp-content/uploads/2025/07/public-deliverable-D2.1.pdf

Annex I Regulatory (CRA) traceability

This Annex provides a consolidated and high-level traceability table linking the relevant Cyber Resilience Act (CRA) annexes and requirement themes to the tools delivered in D3.1, the corresponding capabilities described in the deliverable, and the concrete evidence artefacts produced. The table supports transparency and auditability, while clarifying that legal responsibility for compliance remains with the manufacturer.

Table 5 Full Mapping CRA requirements with CURIUM tools

CRA Annex / Theme	**Tool(s)**	**What capability in D3.1 proves it**	**Evidence artefact produced**
Annex I – Secure-by-design & secure-by-default	CyReA, DPRA, DPMA	CRA scoping, product context definition, risk-based security assessment, and maturity evaluation supporting secure design decisions	CRA scope report, risk assessment results, maturity profiles
Annex I – Risk management across the lifecycle	DPRA	Identification of assets, threats, vulnerabilities, and cascading risks across product components	Risk analysis reports, threat and impact matrices
Annex I (Part II) – Vulnerability identification	PSTVA, CAC	Automated vulnerability scanning and security testing of products and components	Vulnerability scan reports
Annex I (Part II) – Vulnerability assessment & prioritisation	DPRA	Risk-based prioritisation of identified vulnerabilities	Vulnerability prioritisation outputs
Annex I (Part II) – Post-market monitoring	PSTVA, DPRA, CAC	Support for recurring assessments and reassessment of vulnerabilities over time	Monitoring and reassessment reports
Annex I (Part II) – Vulnerability documentation	CAC	Centralised documentation of vulnerability handling activities and outcomes	Documented vulnerability records
Annex II – Information and instructions to the user	CURIUM Portal, CAC, Training & Support resources	Provision of guidance, templates, and training material supporting secure installation, use, update, and maintenance information	User guidance documents, training materials
Annex III & IV – Critical and highly critical products	CyReA	Product classification logic supporting determination of criticality and applicable requirements	Product classification results and rationale

Annex VII – Technical documentation	CAC, DPRA, PSTVA	Centralised workspace for collecting and organising technical documentation and assessment evidence	Structured technical documentation set
Annex V & VI – EU Declaration of Conformity	CAC	Generation of EU Declaration of Conformity templates based on documented evidence	EU Declaration of Conformity template
Annex VIII – Conformity assessment procedures	CyReA, CAC	Support for identifying applicable conformity assessment routes and preparing assessment evidence	Conformity assessment readiness package
D2.2 Section 5.3 – System and tool requirements	CyReA, DPRA, DPMA, PSTVA, CAC	Implementation of the functional and technical requirements defined in D2.2 through the integrated CURIUM Compliance Continuum, including CRA scoping, risk assessment, vulnerability assessment, documentation support, conformity preparation, deployment, feedback management, and capacity-building services	Assessment reports, risk analysis outputs, test reports, documentation artefacts, conformity templates, training materials

The requirements defined in Section 5.3 of Deliverable D2.2 are implemented through the tools released in D3.1 and are reflected in the CRA-aligned capabilities and evidence artefacts summarized in this table.

The Annex demonstrates how CURIUM operationalizes CRA requirements through technical tools and services, while maintaining the principle that legal accountability for conformity remains with the manufacturer.

Annex II Traceability between D2.2 Requirements and D3.1 Implementation

Table 6 Mapping requirements described in D2.2 with the CURIUM

Table 7 Req. ID	Requirement Description (verbatim meaning from D2.2 Table 7)	CURIUM Tool(s)	Implementation in D3.1	Relevant D3.1 Section(s)
CR-REQ-01	The system shall support identification of whether an organisation and its product with digital elements fall under the scope of the CRA	CyReA	CRA scope determination via guided questionnaire and exclusion checks	§4.2.1
CR-REQ-02	The system shall support identification of the economic operator role according to the CRA	CyReA	Role identification (manufacturer, importer, distributor, authorised representative)	§4.2.1
CR-REQ-03	The system shall support classification of products with digital elements according to CRA criticality	CyReA	Product screening and classification (default, Class I, Class II)	§4.2.1
CR-REQ-04	The system shall support risk-based cybersecurity assessment for products with digital elements	DPRA	Asset-based, threat-driven risk assessment with cascading risk analysis	§4.2.2
CR-REQ-05	The system shall support identification and modelling of assets composing a product with digital elements	DPRA	Asset inventory, dependency modelling and product decomposition	§4.2.2
CR-REQ-06	The system shall support identification of threats and vulnerabilities affecting product assets	DPRA, PSTVA	CTI integration (DPRA) and automated vulnerability scanning (PSTVA)	§4.2.2, §4.2.5
CR-REQ-07	The system shall support vulnerability prioritisation based on risk	DPRA	Correlation of vulnerabilities with likelihood and impact	§4.2.2
CR-REQ-08	The system shall support cybersecurity maturity assessment of products with digital elements	DPMA	Maturity assessment aligned with CRA-relevant practices and standards	§4.2.3
CR-REQ-09	The system shall support security-by-design and security-by-default principles	CyReA, DPRA, DPMA	Early scoping, risk assessment and maturity evaluation	§3.3, §4
CR-REQ-10	The system shall support vulnerability assessment and penetration testing activities	PSTVA	Self-testing and vulnerability assessment toolkit	§4.2.5
CR-REQ-11	The system shall support preparation for conformity assessment procedures	CyReA, CAC	Readiness assessment and conformity workflows	§4.2.1, §4.2.4
CR-REQ-12	The system shall support generation and management of technical documentation required by the CRA	CAC, DPRA, PSTVA	Aggregation of technical evidence across tools	§4.2.4
CR-REQ-13	The system shall support preparation of the EU Declaration of Conformity	CAC	Automated EU DoC template generation	§4.2.4

CR-REQ-14	The system shall support post-market activities, including reassessment and monitoring	DPRA, PSTVA, CAC	Continuous reassessment and monitoring capabilities	§3.3, §5.3
CR-REQ-15	The system shall be usable and accessible by SMEs and micro-enterprises	All tools	Guided workflows, simplified UI, training support	§4, §7
CR-REQ-16	The system shall provide a centralised access point to all tools and services	CURIUM Portal	Central portal with unified access and SSO	§4.1
CR-REQ-17	The system shall support continuous improvement through feedback mechanisms	All tools	Feedback Management Framework and iterative refinement	§6
CR-REQ-18	The system shall support training, awareness and capacity-building activities	Training resources, all tools	CRA training, awareness events, advisory services	§7