



Cra sUpPoRt contInuUM

Validation and CURIUM Compliance Continuum assessment report

Document Summary Information

Grant No	Agreement	101190372	Acronym	CURIUM
Full Title	Cra sUppoRt contInuUM			
Start Date	01.01.2025	Duration	18 months	
Project URL	www.curium-project.eu			
Deliverable	D4.1: Validation and CURIUM Compliance Continuum assessment report			
Work Package	Work Package 4: Demonstration and Validation activities			
Contractual due date	30/06/2026	Actual submission date	30/09/2026	
Type	R	Dissemination Level	PU	
Lead Beneficiary	28DIGITAL			
Responsible Author	28DIGITAL			
Contributions from	All partners			

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
0.1	20.2.26	5	Initial Table of Contents, Introduction and assignment of activities and sections to partners	28DIGITAL
0.2	15.9.26	95%	Contribution from partners included	CYS, AEGIS, APIRO, NLG
0.3	18.9.26	99%	Executive Summary and conclusions included. Ready for internal review	28DIGITAL
0.4	25.9.26	100%	Review comments addressed. Ready for submission	28DIGITAL, CYS, AEGIS, APIRO, NLG
0.5	28.9.26	100%	Internal Review completed	p-NET
0.6	28.9.26	100%	Internal Review completed	DSA
1.0	30.9.26	100%	Deliverable submission	CYS

Disclaimer

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

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

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

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

Copyright message

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 This Deliverable contains original unpublished work except where clearly indicated otherwise.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

Table of Contents

1.	Executive Summary.....	9
2.	Introduction	10
2.1.	Mapping Deliverable Contents to Related CURIUM GA outputs.....	10
2.2.	Deliverable Overview and Report Structure.....	11
3.	Overview of the Validation Plan	12
4.	Iterative Validation	15
4.1.	Methodology	15
4.2.	Internal Validation	16
4.2.1.	Requirements	16
4.2.2.	Key Performance Indicators (KPIs)	51
4.3.	External Validation	59
4.3.1.	Riga validation workshop	59
4.3.2.	Cyprus validation workshop	64
4.3.3.	Athens validation workshop.....	70
4.3.4.	Zagreb validation workshop.....	75
4.3.5.	Cyprus Skills validation workshop	82
4.3.6.	BEYOND validation workshop	85
4.3.7.	Dedicated product testing.....	89
4.3.8.	External Validation Summary	94
5.	Final Assessment.....	98
5.1.	Requirements	98
5.2.	KPIs	99
6.	Conclusions and next steps.....	102
7.	Annexes.....	103
7.1.	Annex 1 – Use case template for Dedicated Product testing activities.....	103
7.2.	Annex 2 – Compliance Coverage Matrix.....	105

Table of Figures

Figure 1: CAC tool — Download CRA technical documentation template guidelines	17
Figure 2: CAC tool — Evidence upload and validation within a product assessment	17
Figure 3: CAC tool — Manage DP metadata	18
Figure 4: CAC tool — Automated EU Declaration of Conformity generated upon successful assessment completion.....	19
Figure 5: PSTVA tool — Scan execution on a selected target within a project-assessment.....	20
Figure 6: PSTVA tool — Vulnerability scan report generated after target assessment	21
Figure 7: PSTVA tool — Report generation	22
Figure 8: DPMA tool — log in	22
Figure 9: DPMA tool — searching for security control	23
Figure 10: DPMA tool — Description of measures and maturity level of the selected security control	23
Figure 11: DPMA tool — Searching for threats	23
Figure 12: DPMA tool — Identification of security controls for a maturity level	24
Figure 13: DPMA tool — Searching for security controls	25
Figure 14: DPMA tool — Identification of security controls for a targeted maturity level	25
Figure 15: DPMA tool — Extracting the information of potential controls that can be implemented after searching for a keyword	26
Figure 16: DPRA tool — Decomposition of an ICT product into individual assets	26
Figure 17: DPRA tool — Security objectives and requirements for an ICT product	27
Figure 18: DPRA tool — ICT product-based asset inventory	27
Figure 19: DPRA tool — Threats, vulnerabilities, and associated risks from NVD and CAPEC by MITRE	28
Figure 20: DPRA tool — Vulnerabilities of an ICT product obtained from the associated assets	28
Figure 21: DPRA tool — ICT product with vulnerabilities and threats obtained from the associated assets	29
Figure 22: DPRA tool — Risk level shown for each asset	29
Figure 23: CyReA tool — Questionnaire based on the organization type and specific product type	30
Figure 24: CyReA tool — Questionnaire and related responses	31
Figure 25: CyReA tool — Providing information about the scope of a product.....	32
Figure 26: CyReA tool — Categorization of a product into four distinct classes.....	32
Figure 27: CyReA tool — Presentation of the questionnaire and purpose	33
Figure 28: HTTPS/TLS 1.3 protocol for accessing tools CURIUM Portal tools / CyReA	34
Figure 29: CURIUM portal and its tools	34
Figure 30: Isolated container environment verification	35
Figure 31: Restarting of containers verification	35
Figure 32: Data storage verification	36
Figure 33: Data storage encrypted and immutable	36
Figure 34: Asset inventory	36

Figure 35: SBOM uploaded	37
Figure 36: SBOM tests provided	37
Figure 37: Parsing feedback based on API integrations.....	37
Figure 38: Documentation formats	38
Figure 39: Secure document storage.....	39
Figure 40: System information upon building on terminal.....	40
Figure 41: PSTVA User Interface after log-in	40
Figure 42: Docker container logs of the system	41
Figure 43: DPMA tool – Viewed via browser	42
Figure 44: DPMA tool – Formulas embedded in the web app.....	43
Figure 45: DPMA tool – Web-based app providing integrity.....	43
Figure 46: System accessible via any browser.....	44
Figure 47: CAC tool - Error handling message	44
Figure 48: CURIUM portal privacy policy.....	45
Figure 49: First version of the login user interface	45
Figure 50: Old version of CURIUM portal user interface	46
Figure 51: Latest version of CURIUM portal user Interface.....	46
Figure 52: Resources consumption of each tool’s container.....	47
Figure 53: Privilege configurations for each tool’s container.....	47
Figure 54: Example from PSTVA user manual	48
Figure 55: Technical Documentation and architecture of the PSTVA inside the repository	48
Figure 56: DPRA tool - Access only for authorized users.....	49
Figure 57: DPRA tool – Example of the intuitive interface	49
Figure 58: DPRA tool – Example of secure storage and browser-based access	50
Figure 59: DPRA tool - Ability to incorporate up-to-date open intelligence information	50
Figure 60: CyRea tool - Access only for authorized users.....	51
Figure 61: CyRea tool – Interactive wizard-based questionnaire	51
Figure 62: Techritory event promotional material	59
Figure 63: Techritory event activities	60
Figure 64: Cyprus event promotional material.....	64
Figure 65: Cyprus event activities.....	66
Figure 66: Athens event activities	71
Figure 67: Zagreb event promotional material.....	75
Figure 68: Zagreb event activities.....	76
Figure 69: Cyprus Skills event activities.....	83
Figure 70: BEYOND event activities	86

List of Tables

Table 1: Adherence to CURIUM GA Deliverable & Tasks Descriptions	10
Table 2: Matrix of scan capabilities against scan targets	41
Table 3: Essential requirements compliance coverage matrix fully covered by CURIUM tools	53
Table 4: Essential requirements partially covered and guided compliance	54
Table 5: Open-source components made available	55
Table 6: CURIUM tools mapping to specific requirements	57
Table 7: CRA Documentation and associated tool	57
Table 8: Techritory event requirements validation	60
Table 9: Techritory event KPIs validation	62
Table 10: Cyprus event requirements validation.....	67
Table 11: Cyprus event KPIs validation	67
Table 12: Athens event requirements validation	71
Table 13: Athens event KPIs validation	72
Table 14: Zagreb event requirements validation.....	77
Table 15: Zagreb event KPIs validation.....	78
Table 16: Cyprus Skills event requirements validation.....	83
Table 17: Cyprus Skills event KPIs validation	84
Table 18: BEYOND event requirements validation	86
Table 19: BEYOND event KPIs validation	87
Table 20: Validation participants	91
Table 21: Comparison table and outcomes of the guided sessions	91
Table 22: KPIs related to Tool Development and Technical Implementation	99
Table 23: KPIs for CRA Compliance and Requirements Coverage	100
Table 24: KPIs for User Adoption and Feedback.....	100
Table 25: KPIs for Project Management and Operations	101

List of Abbreviations

Abbreviation	Description
Avg.	Average
CAC	Conformity Assessment and Compliance (Service)
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CyReA	CRA Scoping and Product Classification Service
DP	Digital Product
DPMA	Digital Product Maturity Assessment
DPRA	Digital Product Risk Management
DSA	Digital Security Authority
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCC	EU Cybersecurity Certification scheme
FR	Functional Requirement
GA	Grant Agreement
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JTC	Joint Technical Committee
KPI	Key Performance Indicator
NCSA	National Cybersecurity Authority
NFR	Non-Functional Requirement
M	Month
MS	Member State
PDE	Product with Digital Elements
PSTVA	Penetration Self-Testing and Vulnerability Assessment (Services and Tools)
PU	Public (dissemination level)
PEIK	Pseudonymized Entity Identification Key

SaaS	Software as a Service
SBOM	Software Bill of Materials
SDO	Standards Developing Organisation
SME	Small and Medium-Size Enterprise
SSO	Single Sign-On
TR	Technical Requirement
UI	User Interface
UX	User Experience
WP	Work Package

1. Executive Summary

This deliverable reports on the demonstration and validation activities carried out in the CURIUM project, documenting the process followed, the evidence collected, and the assessment of the CURIUM Compliance Continuum against the requirements and KPIs defined in D2.2 and the Grant Agreement.

The CURIUM Compliance Continuum comprises five cybersecurity tools (CyReA, DPRA, DPMA, PSTVA, and CAC), accessible through a unified portal, designed to guide SMEs and other organisations through the full CRA compliance journey: from product scoping and classification, through risk assessment and maturity evaluation, to vulnerability testing and technical documentation. The validation process covered two complementary dimensions: system validation, assessing whether the tools meet their defined requirements; and performance monitoring, tracking progress through the project KPIs.

Validation process. The validation was carried out through two parallel tracks. Internal validation, led by the tool-developing partners, confirmed compliance with 55 of the 57 requirements through demonstration, inspection, and testing. The remaining two requirements: NFR-002 (usability by non-cybersecurity experts) and NFR-005 (clean, simple UI) were validated externally through structured questionnaires administered across six external validation events: Riga (M10), Cyprus (M12), Athens (M15), Zagreb (M16), Cyprus Skills (M18), and BEYOND (M18). In addition, dedicated one-to-one testing sessions were organised with SMEs testing the tools with their own real digital products, providing the most in-depth validation evidence collected throughout the project.

Requirements. All 57 requirements are confirmed as met. External validation confirmed a clear improvement trajectory across the project lifetime: the weighted mean UX score rose from 3.65/5 at Riga to 4.6/5 at BEYOND, and label comprehension rose from 25% to 100%, directly reflecting the impact of the iterative feedback and refinement cycles between validation rounds.

KPIs. Of the 20 KPIs tracked in this deliverable, 16 are confirmed as met, 4 are partially met. Key results include: 47 unique testers across 6 events, plus 1 additional SME recruited through direct partner outreach for the dedicated product testing activities. 5 SMEs from Zagreb event also joined these activities but are not counted again, as they are already included in the 47 unique testers (KPI5, target >20); 95% of respondents reported cost reduction potential (KPI8, target >85%); 83% reported increased CRA awareness (KPI22, target >80%); and 100% feedback rate was achieved across all events (KPI21, target >90%). Tool acceptance (KPI26, target >75%) was partially met adoption intent reached 63% while recommendation intent reached 80%, reflecting the gap between finding a tool valuable and committing to adopt it, a gap expected to narrow as the CRA's regulatory deadlines approach.

Overall assessment. The CURIUM Compliance Continuum is a functional, usable, and CRA-aligned system that delivers genuine value to SMEs navigating regulatory compliance. Its strength lies in the complementarity of its five tools, which together address the complete set of obligations a manufacturer must meet under the CRA. The portal will remain publicly accessible until the end of 2027, aligned with the full entry into force of the CRA in December of that year, ensuring that the Continuum can accompany organisations throughout the entire compliance transition period.

2. Introduction

2.1. Mapping Deliverable Contents to Related CURIUM GA outputs

This section presents the CURIUM Grand Agreement (GA) commitments, as extracted from the formal documentation and task description, in respect to their outputs and work to be performed.

TABLE 1: ADHERENCE TO CURIUM GA DELIVERABLE & TASKS DESCRIPTIONS

CURIUM GA Component Title	CURIUM GA Component Outline	Related Objectives
TASKS		
Task 4.1	<i>Setup and continuous configuration of the CURIUM validation activities.</i> <i>This task will receive input from WP2 and continuously refine the validation plan by mapping the feedback from end users against the developed components and services of WP3. It will also receive user driven KPIs of T2.2 and based on the technical WPs will steer CURIUM validation activities, providing the testing protocol to be followed. It will also produce an aggregated KPIs list to be further enhanced and assessed within T4.2 and T4.3.</i>	<i>O4.2. Continuously revise validation activities throughout the whole series of tools and services releases.</i>
Task 4.2	<i>CURIUM Compliance Continuum Demonstration and Validation.</i> <i>This task will perform the testing and validation activities during multiple rounds or services and tools releases. The first round of CURIUM solutions is planned after M6 and the co-creation phase (continuous releases and feedback from the community) will begin. The feedback will then be used to refine requirements, Compliance Continuum design, and improve provided solutions and services, ensuring alignment with stakeholders' needs and expectations. Two more similar rounds will follow after M11 and M16. These rounds are situated among the co-creation, validation and final release phases. The task will follow the validation plan and testing methodology that has already been defined by T2.4 and will include execute a series of scenarios investigating configuration and integration quality, functionality and usability aspects etc.</i>	<i>O4.1. Perform the validation activities for CURIUM Compliance Continuum, individual tools and components and services.</i> <i>O4.4. Support external stakeholders during the validation process using the training and knowledge capacity building activities of WP3.</i>
Task 4.3	<i>CURIUM platform assessment for different end users.</i> <i>Based on the initial setup of the validation activities this task will focus on making the necessary adjustments to the validation plan and activities in order to better connect with the diverse stakeholders that will be engaged. Such adjustments are expected to produce higher engagement</i>	<i>O4.3. Diversify the process to ensure that it meets the needs of different stakeholders and beneficiaries that test and evaluate CURIUM's solutions.</i>

	<i>rates, more accurate feedback and better insights for targeted training and knowledge building.</i>	
DELIVERABLE		
<i>D4.1. Validation and CURIUM Compliance Continuum assessment report.</i> <i>This deliverable will report the actions done during the validation phase and the final assessment of the CURIUM solutions and services. It will reflect all outcomes of WP4.</i>		

2.2. Deliverable Overview and Report Structure

This deliverable reports on the demonstration and validation activities carried out throughout the CURIUM project, documenting the process followed, the evidence collected, and the assessment of the tools and services against the requirements and KPIs defined in D2.2 and the Grant Agreement.

It is structured as follows:

- Section 1 provides an executive summary of the document.
- Section 2 serves as a link between the Grant Agreement and this document, mapping its contents to the relevant tasks and objectives, and providing an overview of its structure.
- Section 3 presents an overview of the validation plan defined in D2.2, highlighting the key aspects of the project context that shaped its design and implementation.
- Section 4 describes the iterative validation activities carried out throughout the project. It opens with the methodology followed, including the classification of requirements and KPIs into internal and external validation, and the supporting tools and engagement mechanisms used. It then presents the results of the internal validation (Section 4.2), followed by the results of the external validation (Section 4.3).
- Section 5 provides the final assessment of the CURIUM Compliance Continuum, consolidating the validation results against the full list of requirements and KPIs.
- Section 6 concludes the document.
- Section 7 contains the document annexes.

3. Overview of the Validation Plan

The CURIUM validation is a systematic and agile process designed to ensure that the Compliance Continuum tools are practical, accessible, and fully aligned with the Cyber Resilience Act (CRA). The CURIUM validation plan, described in Deliverable D2.2, was structured around four pillars: stakeholder identification and engagement, agile validation cycles, co-creation and feedback loops, and the use of dedicated validation tools and channels. It defined two complementary evaluation dimensions: system validation, which confirms that the tools and services meet their defined technical, functional, and non-functional requirements; and performance monitoring, which tracks progress of the validation process itself through the Key Performance Indicators (KPIs) defined in the Grant Agreement. This plan was primarily designed around external validation, engaging SMEs, national authorities, and other stakeholders to test and evaluate the tools through workshops, hands-on sessions, and structured questionnaires.

As the project moved into implementation, the consortium evolved this plan in two important ways. First, a distinction was introduced between internal and external validation: not all requirements and KPIs needed to be assessed by external stakeholders. Many technical and functional requirements could be verified more reliably through internal validation by the tool developers themselves. Introducing this distinction allowed the consortium to focus the external validation effort on what truly required end-user input. Second, to operationalise both dimensions consistently, the consortium built and maintained collaboratively two core tracking documents: a System Validation excel file covering all requirements defined in D2.2, and a Performance Monitoring one covering the validation process KPIs, in which each item was assigned a responsible owner, classified as internally or externally evaluable, and linked to a defined means of verification. These documents served as the reference point for all validation activities throughout the project, ensuring consistency and traceability across events, tools, and partners.

The following aspects of the project context shaped the design and evolution of the plan and are worth highlighting, as they directly inform how the validation activities documented in this deliverable were planned and executed:

Validating while building. Unlike projects where validation follows development, CURIUM's 18-month timeline required both to happen in parallel. While the first release of tools was planned for M8, tools became available progressively between M8 and M12, with individual tools reaching sufficient maturity for external testing at different points during this period. This had a direct impact on the early validation events: rather than being able to present and test the full Compliance Continuum from the outset, the consortium had to adapt each event to the tools available at that moment, gradually expanding the scope of external validation as more tools became ready. The validation strategy was designed from the outset as an iterative process with multiple rounds of feedback and refinement, each feeding directly into the next development cycle through T3.3, and the progressive tool delivery reinforced this approach in practice.

Internal validation as a parallel track. Alongside the external engagement activities, the tool developers carried out internal validation of the requirements classified as internally evaluable, providing evidence in the form agreed upon by the consortium. The results of this internal validation are documented in Section 4.2 of this deliverable. The technical refinements implemented as a result of both internal and external validation feedback are documented in D3.2.

The consortium as a validation network. The strength of the external validation approach relied heavily on the complementary networks and roles that each consortium partner brought to the engagement process. The two National Cybersecurity Authorities (DSA and NCSA) provided direct connections to institutional and regulatory stakeholders, lending credibility to the project's outreach and facilitating engagement with national-level actors involved in CRA implementation. The technical partners (AEGIS, NLG, SPHYNX, CYS, APIRO) brought access to the cybersecurity practitioner community, enabling engagement with users who could evaluate the tools from a technical perspective. Partners with established SME networks (p-NET, 28DIGITAL) contributed access to the primary target audience of the Compliance Continuum: the SMEs and micro-enterprises that the tools were ultimately designed to serve. This diversity meant that the validation process could reach a broad range of stakeholders across multiple EU Member States, sectors, and levels of technical expertise, rather than reflecting a single community's perspective. The validation plan was designed to leverage this collective reach, with all

partners contributing to stakeholder identification, event organisation, and feedback collection according to their specific role and network.

A practical and adaptive evaluation approach. For each external validation event, the relevant requirements and KPIs were selected from the two core tracking excel files, drawing only those classified as externally evaluable and suitable for that specific moment in the project, taking into account the level of tool maturity, the use cases that could be prepared, the available time, the stakeholder profile, and the format of the activity. The agreed evaluation criteria for each selected requirement and KPI then informed the design of the event-specific questionnaire, ensuring that each question was directly linked to what the consortium had committed to measuring. Structured feedback was collected through these questionnaires, while unstructured observations gathered during hands-on sessions were logged separately in a central Feedback-to-Action Tracker, where each entry was categorised and prioritised to drive concrete technical improvements in the next development cycle. Progress against performance KPIs was reviewed after each event, allowing the consortium to identify gaps and adjust the engagement strategy where needed. Additionally, recurring weekly technical meetings on WP3 and WP4 activities supported ongoing monitoring and timely adjustments throughout the project.

Data collection instruments. To capture a holistic view of the CURIUM tools validation, the project employed a variety of quantitative and qualitative data collection instruments. By combining these instruments, CURIUM ensures that validation data reflects a diverse range of stakeholders, from micro-enterprises to national cybersecurity authorities:

- Hands-on Use Case Scenarios: Participants with test tools using prepared use-case scenarios (such as performing a risk assessment for a CCTV system or generating an automated EU Declaration of Conformity) to provide an experiential basis for their evaluation.
- Structured digital questionnaires: Following tool interaction, users' complete tool-specific questionnaires (via MS Forms). These became granular enough to assess usability and UI quality for each individual tool in the Continuum.
- Interviews and Unstructured Feedback: Consortium members capture interview notes and spontaneous comments during live demo sessions. This qualitative data is synthesized into structured reports and recorded in the Feedback-to-Action Tracker.
- Interactive Engagement Polls: Tools like Slido are used during workshop presentations to collect real-time data on audience awareness of the CRA and immediate reactions to tool features.
- Internal Validation Audits: For technical requirements, developers conduct architectural audits and testing to provide evidence of compliance without requiring external user input.

The diversification of the validation process to meet the specific needs of various stakeholders, ensuring higher engagement rates and more accurate feedback, was primarily managed under Task 4.3 (CURIUM platform assessment for different end users).

Adjustments made during implementation. The validation plan was iteratively adjusted throughout the project to better connect with diverse stakeholders and respond to emerging needs:

- Increased granularity in tool assessment. Starting with the Athens workshop (March 2026), the project shifted from generic post-event surveys to five separate tool-specific questionnaires, allowing for finer assessment of usability across individual tools.
- Validation of the integrated user journey. Based on early feedback that tools felt unlinked, the consortium adjusted the plan to validate the CURIUM Portal as a unified access point during the Zagreb workshop (April 2026), reordering the tool sequence (CyReA → DPRA → DPMA → PSTVA → CAC) to reflect a coherent customer journey for manufacturers.
- Tailored engagement for diverse profiles. The consortium leveraged the complementary networks of its partners to reach different stakeholder groups: national authorities for institutional engagement, SME-focused partners for micro and small enterprises, and technical partners for the cybersecurity practitioner community.
- Mitigating access constraints. To accommodate stakeholders who could not access SaaS versions of the tools, the plan was adjusted to include guided demos, pre-configured test environments, and asynchronous validation where users could provide feedback after the session.

- Refined recruitment and adoption strategy. To boost SME participation, outreach tactics were refined throughout the project, and a dedicated product testing strategy was introduced to allow SMEs to engage in one-to-one sessions using their own organisation's products. This is described in detail in Section 4.3.7.

The detailed implementation of this approach, including the outcomes of both internal and external validation, is described in the following sections.

4. Iterative Validation

4.1. Methodology

The preparatory work carried out by the consortium across several meetings consisted of agreeing how each requirement and KPI would be interpreted and evaluated. This resulted in two core tracking documents maintained by 28DIGITAL with input from and consensus of all partners: a system validation document covering all functional, non-functional, and technical requirements defined in D2.2, and a performance monitoring document covering the project KPIs relevant to the validation process. Both documents assigned a responsible owner to each requirement and KPI, ensuring accountability throughout the project, and included the classification of each requirement and KPI according to its validation approach:

- **Internal validation** applies to requirements and KPIs that can be verified by the tool developer through inspection, testing, demonstration, or architectural audit, without requiring input from external stakeholders. This includes, for example, technical requirements such as the use of HTTPS/TLS, containerization, or SSO implementation, as well as functional requirements that can be demonstrated through a controlled walkthrough of the tool's features.
- **External validation** applies to requirements and KPIs whose assessment depends on the response of real end-users interacting with the tools. This includes non-functional requirements such as usability by non-technical users or the simplicity of the dashboard interface, as well as KPIs related to stakeholder engagement, CRA awareness, tool adoption, and cost reduction. For these, external validation was conducted through structured questionnaires administered during validation events, complemented by unstructured feedback collected directly during hands-on sessions.

Internal validation was carried out by the tool developers within the consortium. For each requirement or KPI classified as internal, the responsible partner was asked to define the means of evidence, being this test results, screenshots, architectural documentation, or a structured walkthrough of the relevant functionality. The results of the internal validation are presented in Section 4.2, organised by requirement and KPI, with the supporting evidence provided by each responsible partner.

For the external validation, the consortium organised several validation events. For each validation event, a dedicated tracking document was derived from the two core documents, containing only the requirements and KPIs identified as externally evaluable in that specific context. This selection considered the profile of the participants, the format of the activity, and the level of tool maturity at that point in the project. The event-specific document was populated by the responsible owners after each activity, under the coordination of 28DIGITAL.

External validation followed a consistent two-step structure: first, a demonstration or hands-on session in which participants were shown or directly interacted with the relevant tool features; and second, a structured questionnaire through which participants provided their assessment. This sequence was essential, as participants needed to have seen or used the functionality before being asked to evaluate it. The questionnaires were designed specifically for each event, drawing on the agreed evaluation criteria for each requirement and KPI, and always included a field for participants to provide their contact details if interested in future testing activities. The results of the external validation are presented in Section 4.3, organised by validation event, in addition to the dedicated product testing sessions in which SMEs used the CURIUM tools with their own digital products. These sessions generated more in-depth, product-specific feedback than the workshop format allowed, and are described in Section 4.3.7. This is followed by the aggregated assessment of requirements and KPIs across all activities.

In parallel, a separate Feedback Tracker was maintained at consortium level to capture unstructured observations collected during hands-on sessions, recording each input with its source, category, priority, and assigned action. This provided the technical team with a structured log of qualitative insights that complemented the quantitative data from the questionnaires and fed directly into the tool refinement activities of T3.3.

Reaching the right participants for each validation activity was an ongoing effort that combined multiple channels and approaches. The project used the CURIUM website, LinkedIn, and video content to maintain visibility and awareness throughout the project lifetime. For structured validation workshops, each event was promoted through a dedicated registration form, communicated via LinkedIn and the project website, and followed up with a post-event news item and an email to participants including the slides presented. For events

where CURIUM participated within a broader programme organised by third parties or through stand-based interaction at an exhibition, promotion and follow-up were handled through the organising entity's own channels, complemented by the project's standard communication channels where applicable. Partners played an active role in direct outreach through their own networks, which proved particularly effective in reaching relevant stakeholders in each location. After each event, participants were invited to stay connected and informed about upcoming activities, building a growing community of engaged stakeholders across the project lifetime. A subset of these contacts (those who expressed interest in testing the tools with their own digital products) were subsequently followed up individually and some progressed towards the dedicated product testing sessions described in Section 4.3.7, representing the deepest level of engagement achieved throughout the validation campaign.

4.2. Internal Validation

This section presents the results of the internal validation carried out by the tool developers within the consortium. It covers two types of evidence: the validation of requirements classified as internally evaluable, and the assessment of KPIs that can be verified without external stakeholder input. The results are organised first by requirement, then by KPI.

For each requirement, the following fields are provided:

- Evaluation Aspect refers to the dimension of the system being assessed. Five aspects were defined in D2.2: Functionality (whether the tool performs its intended compliance function), Reliability and Functional Stability (whether the tool operates consistently and securely), Usability and ease of access (whether the tool is accessible and intuitive for non-expert users), Knowledge capacity (whether the tool is supported by adequate documentation and guidance), and Financial factors (whether the tool operates within cost-effective resource limits).
- Evaluation Method refers to the technique used to verify the requirement. The methods used in internal validation are Demonstration (a structured walkthrough of the tool's functionality), Inspection (review of architectural documentation, configuration, or source artefacts), and Test (execution of a defined test procedure with measurable output).
- Assumptions and Means to Verify describes the specific steps, conditions, and artefacts used to confirm that the requirement has been met. This includes the sequence of actions taken during the demonstration or test, the expected outcomes, and any relevant references to tool documentation or configuration evidence.

For each KPI, the current value reached is reported together with the justification and supporting evidence.

4.2.1. Requirements

FR-001 [CAC Tool]: Provide step-by-step guidance for creating Technical Documentation (CRA Annex V)

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the CAC tool. Moreover, user should include at least one product and assessment in the CAC application, which may have been submitted without attaching the necessary technical documentation.

Means to Verify:

1. Log in to CAC
2. For a specific product assessment, verify that after the user completes the product assessment and closes the assessment modal, the Upload relevant documentation dialog opens automatically.
3. Upload technical documentation and verify that the functionality works.
4. Verify that if additional documentation is required, the user can upload further files from the Documentation tab or use the **Download CRA Technical Documentation Template** button as a starting point.

More details can be found in the User Manual – CAC tool [USER-MANUAL CAC-TOOL.pdf](#)

	Document group	User info	Document name	Status	Comment
	8. User Documentation (Instruction for the Users)	security guidance, support mechanisms, and communication channels for vulnerability disclosure. Contact information for security support, how can users report vulnerability, incident, supporting period.....	webcam_technical_specification.docx		
		Conformity assessment procedure, evidence of conformity, the			

Download CRA Technical Documentation Template

FIGURE 1: CAC TOOL — DOWNLOAD CRA TECHNICAL DOCUMENTATION TEMPLATE GUIDELINES

FR-002 [CAC Tool]: Upload and validate cybersecurity evidence (documents, test results)

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the CAC tool. Moreover, user should include at least one product and assessment in the CAC application which may have been submitted without attaching the necessary technical documentation.

Means to Verify:

1. Log in to CAC
2. For a specific product assessment, verify that after the user completes the product assessment and closes the assessment modal, the Upload relevant documentation dialog opens automatically.
3. Upload technical documentation (e.g., SBOM, product images, other documentation) and verify that the functionality works.
4. Check that the system provides validation results for the submitted documentation.

AssessmentsSBOMRecommendationsDocumentationProduct ImagesEvaluation

Choose

Document nameFormatVersionValidation status

webcam_technical_specification.docxDOCX1.0DownloadFINISHED

1 / 11

Number of records: 1

UserAction PerformedAction dateDocument nameVersion number

whichUPLOAD2026-07-15 13:03:13.516803webcam_technical_specification.docx1.0Download

1 / 11

Document groupUser infoDocument nameStatusComment

10. Lifecycle and Maintenance Plan (Update)webcam_technical_specification.docx

2. Technical Details - Design and Development Informationwebcam_technical_specification.docx

Download CRA Technical Documentation Template

✓ Validation of 'webcam_technical_specification.docx' started!

16.07.2026 15:10:20

FIGURE 2: CAC TOOL — EVIDENCE UPLOADS AND VALIDATION WITHIN A PRODUCT ASSESSMENT

© CURIUM, 2025

17

FR-003 [CAC Tool]: Generate automated Technical Documentation and manage Digital Product (DP) metadata (type, version, context, lifecycle)

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the CAC tool. The requirement is split into two parts: a) one is related to the generation of Technical Documentation which has the same assumptions of FR-001 and b) the second related to the management of a product, for which the only assumption is that the user is in the process of creating or has created at least one product within the CAC systems.

Means to Verify:

- a) follow the same process as FR-001 and
- b)
 1. Log in to CAC
 2. Add a new product through the relevant point of the system
 3. Enter the necessary product information and save it
 4. Open the product details and change the information in the type, version, context.
 5. Create a new assessment for this product.
 6. Upload the Lifecycle and Maintenance Plan of the product.

Lifecycle and Maintenance Plan (Update)

Explain update strategies, end-of-life policies, and how supply chain security is managed throughout the product lifecycle, description of the products maintenance process'

Select option:

☒ Upload

☐ Later

☐ Not applicable

+ Choose

Uploaded file:

webcam_technical_specification.docx

Previous

Finish file upload

Next

	Document group	User info	Document name	Status	Comment
	8. User Documentation (Instruction for the Users)	security guidance, support mechanisms, and communication channels for vulnerability disclosure. Contact information for security support, how can users report vulnerability, incident, supporting period.....	webcam_technical_specification.docx		
		Conformity assessment procedure, evidence of conformity, the			

Download CRA Technical Documentation Template

FIGURE 3: CAC TOOL – MANAGE DP METADATA

FR-004 [CAC Tool]: Generate automated EU Declaration of Conformity

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the CAC tool. Moreover, user should include at least one product and assessment in the CAC application and the evaluation result should have been positive (passed), any recommendations should have been allocated specific actions (for example, Acknowledged, Not applicable) and the product images, logos and signature should have been uploaded. Finally, the Account information page inside the application (including company name and other information) should be completed to support the extraction of the EU Declaration of Conformity.

Means to Verify:

1. Log in to CAC
2. Press the EU declaration button to generate the Declaration of Conformity.
3. Verify that the declaration can be downloaded and opened.
4. Check the contents of the declaration against the needed contents as shown on page 39 of the manual.

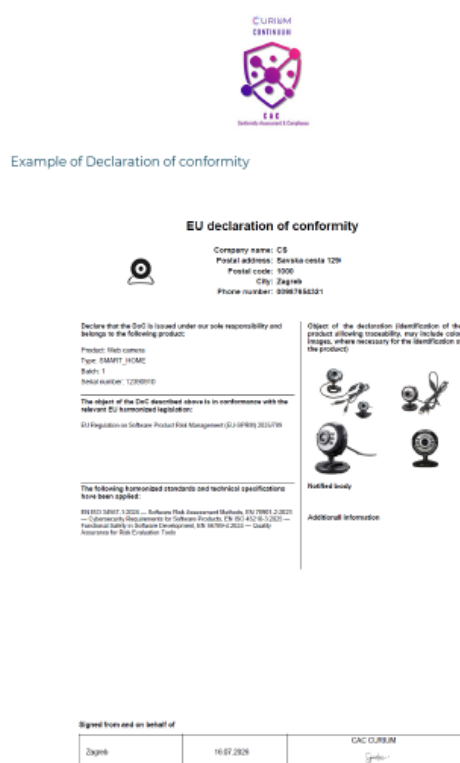


FIGURE 4: CAC TOOL — AUTOMATED EU DECLARATION OF CONFORMITY GENERATED UPON SUCCESSFUL ASSESSMENT COMPLETION

FR-005 [PSTVA Tool]: Scan execution

Evaluation aspect: Functionality

Evaluation method: Demonstration

Means to Verify:

1. User download PSTVA from git in the local environment and execute the start commands (as it is described in TR-010).
2. Visit Browser UI
3. Log in
4. Create a Project-Assessment
5. Select Scan Type
6. Select Target
7. Execute the Scan for the Target

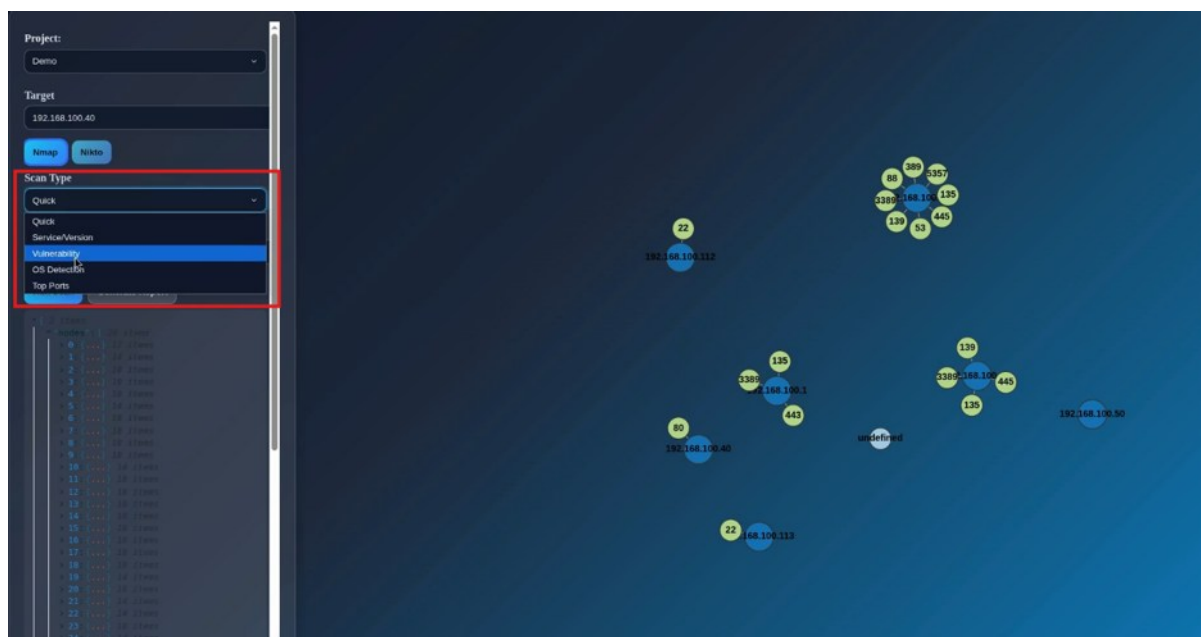


FIGURE 5: PSTVA TOOL — SCAN EXECUTION ON A SELECTED TARGET WITHIN A PROJECT-ASSESSMENT

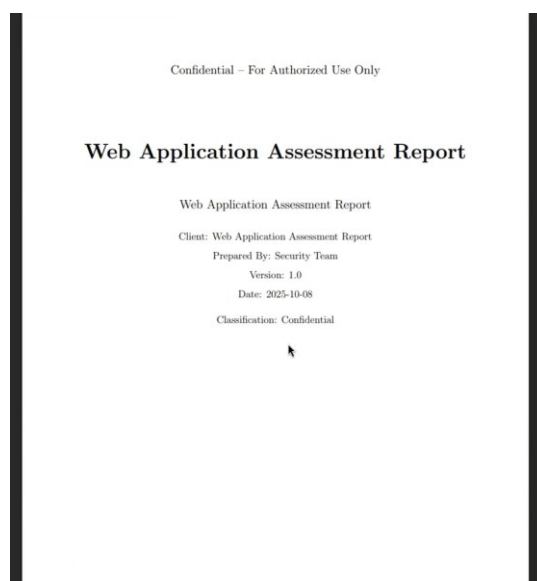
FR-006 [PSTVA Tool]: Report generation

Evaluation aspect: Functionality

Evaluation method: Demonstration

Means to Verify:

- 1.User starts PSTVA on local environment
- 2.Visit Browser UI
- 3.Log in
- 4.Create a Project-Assessment
- 5.Select Scan Type
- 6.Select Target
- 7.Execute the Scan for the Target
- 8.Select the report Generation
- 9.Modify the relevant Fields (optional)
- 10.Download the PDF file



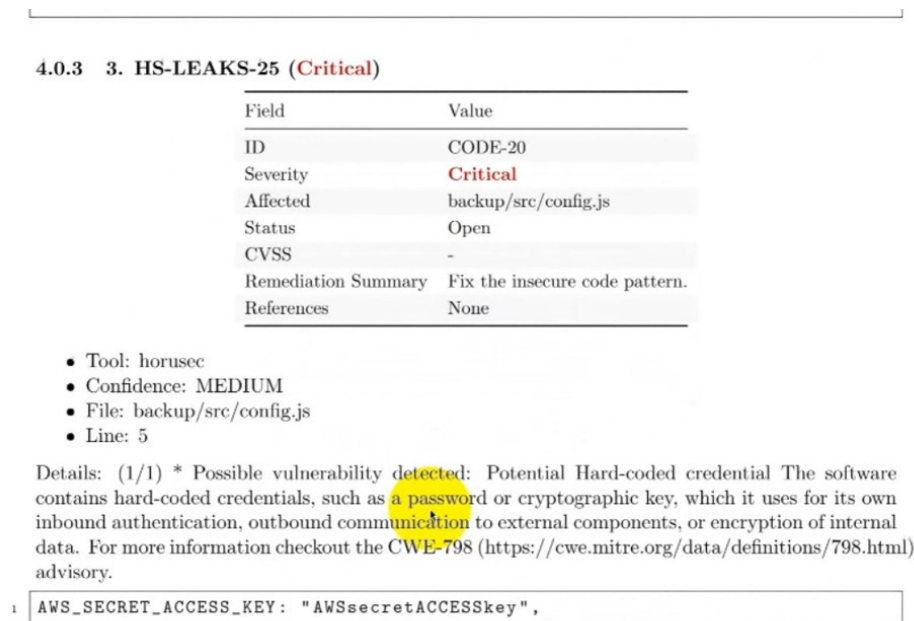


FIGURE 6: PSTVA TOOL — VULNERABILITY SCAN REPORT GENERATED AFTER TARGET ASSESSMENT

FR-007 [PSTVA Tool]: Report access and management

Evaluation aspect: Functionality

Evaluation method: Demonstration

Means to Verify:

1. User starts PSTVA on local environment
2. Visit Browser UI
3. Log in
4. Create a Project-Assessment
5. Selects Scan Type
6. Select Target
7. Execute the Scan for the Target
8. Select the report Generation
9. Application on an Interactive markdown file inside the browser
10. User can modify the .md file before the finalized report.

```
<!-- Pentest Report Template -->
# Web Application Assessment Report
...
## Executive Summary
### Key Findings at a Glance
- **5418A85B-F487-5B80-B106-0800AC061C7A** (Severity: \sev(Critical)) - Patch or mitigate the affected service.
- **85E74010-A082-5ECE-AB37-623A5B33FE70** (Severity: \sev(Critical)) - Patch or mitigate the affected service.
- **CVE-2024-38474** (Severity: \sev(Critical)) - Patch or mitigate the affected service.
- **CVE-2024-38475** (Severity: \sev(Critical)) - Patch or mitigate the affected service.
- **CVE-2024-38476** (Severity: \sev(Critical)) - Patch or mitigate the affected service.
### Severity Metrics
\begin{longtable}[]{}
>\raggedright\arraybackslashp{(\columnwidth - 4\tabcolsep) * \real{0.60}}
>\raggedright\arraybackslashp{(\columnwidth - 4\tabcolsep) * \real{0.20}}
>\raggedright\arraybackslashp{(\columnwidth - 4\tabcolsep) * \real{0.20}}{}
\toprule\noalign{}
Severity & Count & \% \\
\midrule\noalign{}
\endhead
\endlastfoot
\sev(Critical) & 10 & 14.7\% \\
\sev(High) & 21 & 30.9\% \\
\sev(Medium) & 2 & 2.9\% \\
\sev(Low) & 0 & 0.0\% \\
\sev(Informational) & 35 & 51.5\% \\
\end{longtable}
### Severity Definitions
| Severity | Description |
|-----|-----|
| \sev(Critical) | Exploitable immediately with business-wide / catastrophic impact |
| \sev(High) | High impact or high likelihood leading to significant compromise |
| \sev(Medium) | Moderate impact or requires specific conditions |
| \sev(Low) | Limited impact or hard to exploit |
| \sev(Informational) | Best practice / no direct exploit impact |
# 1. List of Findings
Risk Distribution: \sev(Critical): 10 (14.7%) | \sev(High): 21 (30.9%) | \sev(Medium): 2 (2.9%) | \sev(Informational): 35 (51.5%)
```

FIGURE 7: PSTVA TOOL — REPORT GENERATION

FR-008 [DPMA Tool]: Provide the ability for the user to assess their performance on specific cybersecurity controls and identify the level of these controls against a structured scale

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

1. Login to the Curium Portal and select the DPMA tool.

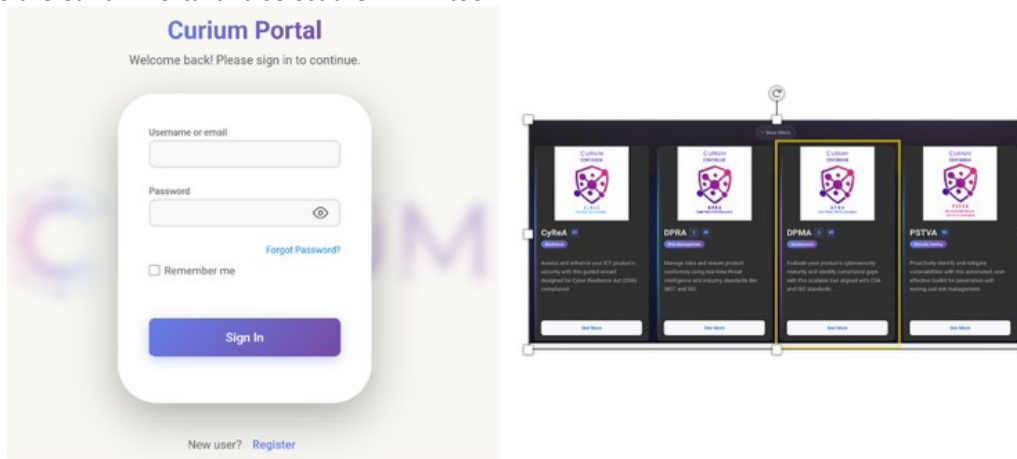


FIGURE 8: DPMA TOOL — LOG IN

2. The User types the area or the specific key words related to the control aiming to be located in the search field (e.g. Information Backup).

Excel Data

Information backup

#	Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
	Filter Category	Filter Category_Nu	Filter Description of Measures	Filter L	Filter Paragraph	Filter Pat	Filter Source	Filter Threats	Filter Unique
1	8.13	Information backup	Information backup	1	A.8.13	A.8.13	ISO 27001	Acts of war (conventional), Media Failure - storage media that stops retaining stored	A.8.13 ID.1
2	Information backup	Information backup	A topic-specific policy on backup should be established to address the organization's data retention and information security requirements.	2	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.1
3	Information backup	Information backup	Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following an incident or failure or loss of storage media.	3	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.2
4	Information backup	Information backup	Plans should be developed and implemented for how the organization will back up information, software and systems, to address the topic-specific policy on backup.	0	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.3
5	Information backup	Information backup	When designing a backup plan, the following items should be taken into consideration: a) producing accurate and complete records of the backup copies and documented restoration procedures; b)	4	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.4
6	Information backup	Information backup	Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness	5	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.5

FIGURE 9: DPMA TOOL — SEARCHING FOR SECURITY CONTROL

3.The user can then review the available information for the controls, identify which ones are implemented by them and identify their maturity level.

4.Finally, the user should check where the selected control appears in relation to the available options.

#	Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
	Filter Category	Filter Category_Nu	Filter Description of Measures	Filter L	Filter Paragraph	Filter Pat	Filter Source	Filter Threats	Filter Unique
1	8.13	Information backup	Information backup	1	A.8.13	A.8.13	ISO 27001	Acts of war (conventional), Media Failure - storage media that stops retaining stored	A.8.13 ID.1
2	Information backup	Information backup	A topic-specific policy on backup should be established to address the organization's data retention and information security requirements.	2	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.1
3	Information backup	Information backup	Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following an incident or failure or loss of storage media.	3	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.2
4	Information backup	Information backup	Plans should be developed and implemented for how the organization will back up information, software and systems, to address the topic-specific policy on backup.	0	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.3
5	Information backup	Information backup	When designing a backup plan, the following items should be taken into consideration: a) producing accurate and complete records of the backup copies and documented restoration procedures; b)	4	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.4
6	Information backup	Information backup	Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the topic-specific policy on backups.	5	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.5
7	Information backup	Information backup	Backup measures for individual systems and services should be regularly tested to ensure that they meet the objectives of incident response and business continuity plans.	6	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.6
8	Information backup	Information backup	This should be combined with a test of the restoration procedures and checked against the restoration time required by the business continuity plan.	6	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.7

FIGURE 10: DPMA TOOL — DESCRIPTION OF MEASURES AND MATURITY LEVEL OF THE SELECTED SECURITY CONTROL

FR-009 [DPMA Tool]: Provide the ability to identify possible mitigating measures to threats.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

1.Login to the Curium Portal and select the DPMA tool.

2.Search for a specific keyword for a specific threat under the Threats field or in general under the central search and review the provided results

#	Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
	Filter Category	Filter Category_Nu	Filter Description of Measures	Filter L	Filter Paragraph	Filter Pat	Filter Source	Filter Threats	Filter Unique Id
1	Protection against malware	Protection against malware	Protection against malware should be based on malware detection and repair software, information security awareness, appropriate system access and change management controls.	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.1
2	Protection against malware	Protection against malware	Use of malware detection and repair software alone is not usually adequate.	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.2
3	Protection against malware	Protection against malware	The following guidance should be considered: a) implementing rules and controls that prevent or detect the use of unauthorized software (e.g. application allowlisting (i.e. using a list providing allowed applications)); b)	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.3
4	8.7	Protection against malware	Protection against malware	1	A.8.7	A.8.7	ISO 27001	Corporate crime, Trojan, Malicious Software - software whose purpose	A.8.7 ID.1
5	Controls against malware	Controls 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	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.10
6	Controls against malware	Controls against malware	g) installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis;	2	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.9
7	Controls against malware	Controls against malware	PR.AT-1: All users are informed and trained	2	A.8.7	A.12.2	NIST	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.26
8	Controls against malware	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	3	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.11

FIGURE 11: DPMA TOOL — SEARCHING FOR THREATS

FR-010 [DPMA Tool]: Facilitate the decision-making activities of the users, related to risk mitigation actions.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

- 1.Login to the Curium Portal and select the DPMA tool.
- 2.Search for a specific keyword or control, such as malware, and review the available information for the controls that match that keyword. Users can identify which controls correspond to each maturity level and plan a path to achieve them based on the organization's risk appetite.

#	Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
	Filter Category	malware	Filter Description of Measures	Filter	Filter Paragraph	Filter Pa	Filter Source	Filter Threats	Filter Unique Id
1	Protection against malware	Protection against malware	Protection against malware should be based on malware detection and repair software, information security awareness, appropriate system access and change management controls.	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.1
2	Protection against malware	Protection against malware	Use of malware detection and repair software alone is not usually adequate.	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.2
3	Protection against malware	Protection against malware	The following guidance should be considered: a) implementing rules and controls that prevent or detect the use of unauthorized software (e.g. application allowlisting (i.e. using a list providing allowed applications)); b)	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.3
4	8.7	Protection against malware	Protection against malware	1	A.8.7	A.8.7	ISO 27001	Corporate crime, Trojan, Malicious Software - software whose purpose	A.8.7 ID.1
5	Controls against malware	Controls 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	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.10
6	Controls against malware	Controls against malware	g) installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis;	2	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.9
7	Controls against malware	Controls against malware	PR.AT-1: All users are informed and trained	2	A.8.7	A.12.2	NIST	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.26
8	Controls against malware	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	3	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.11

FIGURE 12: DPMA TOOL — IDENTIFICATION OF SECURITY CONTROLS FOR A MATURITY LEVEL

FR-011 [DPMA Tool]: Support in the establishment of a roadmap towards achieving the desired maturity level of specific controls.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

- 1.Login to the Curium Portal and select the DPMA tool.
- 2.Search for a specific keyword or control, such as malware, and review the available information for the controls that match that keyword. Users can identify which controls correspond to each maturity level and plan a path to achieve them based on the organization's risk appetite.

(same figure as FR-010)

FR-012 [DPMA Tool]: Allow tracking of achieved vs. targeted states.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

- 1.Login to the Curium Portal and select the DPMA tool.
- 2.The User types the area or the specific key words related to the control aiming to be located in the search field. (e.g. Information Backup).

Excel Data

Information backup

Search

Export CSV Export Excel

#	Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
1	Information backup	Information backup	A topic-specific policy on backup should be established to address the organization's data retention and information security requirements.	1	A.8.13	A.8.13	ISO 27001	Acts of war (conventional), Media Failure - storage media that stops retaining stored	A.8.13 ID.1
2	Information backup	Information backup	Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following an incident or failure or loss of storage media.	2	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.2
3	Information backup	Information backup	Plans should be developed and implemented for how the organization will back up information, software and systems, to address the topic-specific policy on backup.	0	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.3
4	Information backup	Information backup	When designing a backup plan, the following items should be taken into consideration: a) producing accurate and complete records of the backup copies and documented restoration procedures; b)	4	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media that stops retaining stored	8.13.ID.4
5	Information backup	Information backup	Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness	5	A.8.13	8.13	ISO 27002:2022	Acts of war (conventional), Media Failure - storage media	8.13.ID.5

FIGURE 13: DPMA TOOL — SEARCHING FOR SECURITY CONTROLS

3.The user can then review the available information for the controls, identify which ones are implemented by them and identify their maturity level (in blue).

4. The user can select a targeted maturity level (based on the organization's risk appetite and results of the risk assessment) and identify all the controls that need to be implemented in order to achieve the targeted level.

#	Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
	Filter Category	malware	Filter Description of Measures	Filter L	Filter Paragraph	Filter Pa	Filter Source	Filter Threats	Filter Unique Id
1	Protection against malware	Protection against malware	Protection against malware should be based on malware detection and repair software, information security awareness, appropriate system access and change management controls.	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.1
2	Protection against malware	Protection against malware	Use of malware detection and repair software alone is not usually adequate.	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.2
3	Protection against malware	Protection against malware	The following guidance should be considered: a) implementing rules and controls that prevent or detect the use of unauthorized software [e.g. application allowlisting (i.e. using a list providing allowed applications)]; b)	0	A.8.7	8.7	ISO 27002:2022	Corporate crime, Trojan, Malicious Software - software whose purpose	8.7.ID.3
4	8.7	Protection against malware	Protection against malware	1	A.8.7	A.8.7	ISO 27001	Corporate crime, Trojan, Malicious Software - software whose purpose	A.8.7 ID.1
5	Controls against malware	Controls 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	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.10
6	Controls against malware	Controls against malware	g) installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis;	2	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.9
7	Controls against malware	Controls against malware	PR.AT-1: All users are informed and trained	2	A.8.7	A.12.2	NIST	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.26
8	Controls against malware	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	3	A.8.7	A.12.2	ISO 27002:2013	Corporate crime, Trojan, Malicious Software - software whose purpose	A.12.2.ID.11

FIGURE 14: DPMA TOOL — IDENTIFICATION OF SECURITY CONTROLS FOR A TARGETED MATURITY LEVEL

FR-013 [DPMA Tool]: Extract the information of possible controls to be implemented.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

- 1.Login to the Curium Portal and select the DPMA tool.
- 2.Search for a specific keyword or control, such as malware, and review the available information for the controls that match that keyword.
3. Users can extract the information needed with the limitation of 30 results per search in CSV or xlsx format.

[D4.1: Validation and CURIUM Compliance Continuum assessment report]

[illegible]

FIGURE 15: DPMA TOOL — EXTRACTING THE INFORMATION OF POTENTIAL CONTROLS THAT CAN BE IMPLEMENTED AFTER SEARCHING FOR A KEYWORD

FR-014 [DPRA Tool]: The Risk Management (RM) suite shall allow users to decompose ICT product and its corresponding individual assets.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the DPRA tool. Upon logging in, users can utilise the Product Management feature to create and define an ICT product. Once the product is added, the tool enables users to associate multiple assets with the product, as illustrated in the figure below. This functionality supports the systematic decomposition of an ICT product into its individual assets.

Dashboard | [Cyber Resilience](#) | Product

Cyber Resilience

Asset Management

Assets

Cyber Threat Intelligence

Components

Vulnerabilities

Threats

Product Management

Products

Add Product

Search

Name	Created	Modified
PROD	Apr 29, 2026, 2:32:07 PM	Apr 29, 2026, 2:32:07 PM
test34	Mar 5, 2026, 10:47:55 AM	Mar 5, 2026, 10:47:55 AM
testNew	Feb 24, 2026, 11:10:04 AM	Feb 24, 2026, 11:10:04 AM

Camera

About

Cyber Resilience Assessments
DPRA: Assets
DPRA: Security Objectives
DPRA: Security Requirements

Assets are provided by the Digital Product Risk management (DPRA) service

Search

Name	Controls	Version
CCTV	2	1

FIGURE 16: DPRA TOOL – DECOMPOSITION OF AN ICT PRODUCT INTO INDIVIDUAL ASSETS

FR-015 [DPRA Tool]: The specification of security objectives and corresponding security requirements for ICT product shall be specified by RM suite.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the DPRA tool. Users can define security objectives by selecting the “Add Security Objective” option, which presents a predefined list of objectives. This allows users to select the most relevant security objectives for the ICT product. Similarly, security requirements can be

FIGURE 17: DPRA TOOL – SECURITY OBJECTIVES AND REQUIREMENTS FOR AN ICT PRODUCT

Evaluation Aspect: Functionality
Evaluation Method: Demonstration
Means to Verify:

The product asset inventory can be visualised by clicking specific product and asset related with the product.

FIGURE 18: DPRA TOOL – ICT PRODUCT-BASED ASSET INVENTORY

Evaluation Aspect: Functionality
Evaluation Method: Demonstration
Means to Verify:

Verification is done through the demonstration by using the tool. The DPRA identifies threats, vulnerabilities, and associated risks for each ICT product by leveraging open intelligence from widely recognised security repositories, such as NIST's National Vulnerability Database (NVD) and CAPEC by MITRE. Vulnerability data is retrieved in real time from NVD, including metrics such as base score, exploitability score, impact score, and EPSS. In parallel, threat information is derived from CAPEC, enabling a comprehensive and up-to-date assessment of risks at the asset level based on established security taxonomies.

Id	Base score	Exploitability score	Impact score	Epss score	Severity	
CVE-2024-45112	78.0%	18.0%	59.0%	0.1%	High	***
CVE-2024-41869	78.0%	18.0%	59.0%	0.1%	High	***
CVE-2024-7553	78.0%	18.0%	59.0%	0.0%	High	***
CVE-2024-38088	88.0%	28.0%	59.0%	0.1%	High	***

Id	Name	Likelihood	Status
CAPEC-94	Adversary in the Middle (ATM)	High	Stable
CAPEC-92	Forced integer overflow	High	Draft
CAPEC-9	Buffer Overflow in Local Command-Line Utilities	High	Draft
CAPEC-88	OS Command Injection	High	Draft
CAPEC-85	AJAX Footprinting	High	Draft
CAPEC-83	XPath Injection	High	Draft

FIGURE 19: DPRA TOOL – THREATS, VULNERABILITIES, AND ASSOCIATED RISKS FROM NVD AND CAPEC BY MITRE

FR-018 [DPRA Tool]: The vulnerabilities related to specific ICT products shall be identified and prioritized for the risk level calculation.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the tool. The vulnerabilities related to each ICT product can be obtained from the associated assets' vulnerabilities and can link with the product.

Components Vulnerabilities Threats						
Search						
Id	Severity	Base score	Epss score	Percentile	Library	
✓ CVE-2023-20066	Medium	65.0%	0.1%	46.7%	NVD	***
✓ CVE-2023-20065	High	78.0%	0.0%	5.0%	NVD	***
✓ CVE-2023-20035	High	78.0%	0.0%	5.0%	NVD	***
✓ CVE-2023-20027	High	86.0%	0.1%	50.4%	NVD	***
✓ CVE-2022-20919	High	86.0%	0.1%	50.3%	NVD	***

FIGURE 20: DPRA TOOL – VULNERABILITIES OF AN ICT PRODUCT OBTAINED FROM THE ASSOCIATED ASSETS

FR-019 [DPRA Tool]: The RM suite shall illustrate interdependence among ICT products with threat and vulnerabilities for visualization of the product cyber dependencies and calculate both individual and cascading risk.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify: Verification is done through the demonstration by using the tool. The dependencies among ICT products are visualized and linked with their associated threats and vulnerabilities. The individual risk of each ICT product and the cascading risk across dependent products are calculated and shown.

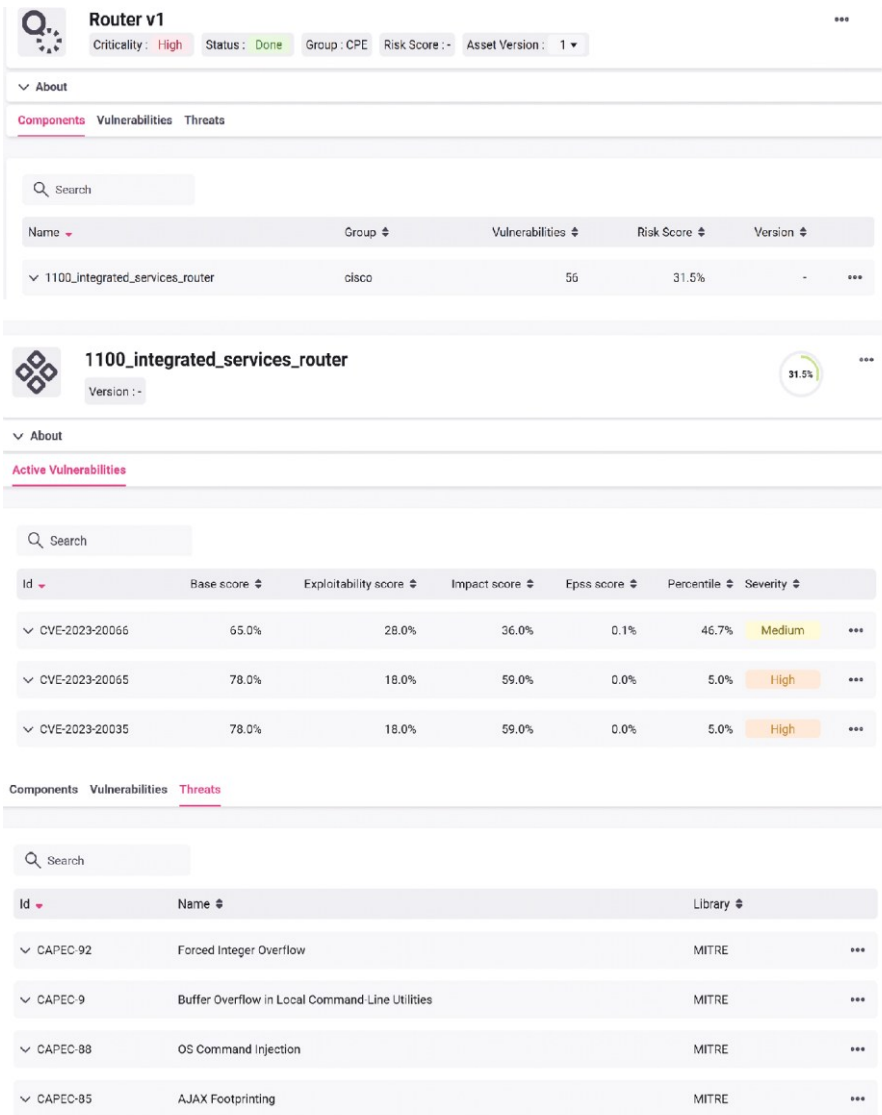


FIGURE 21: DPRA TOOL – ICT PRODUCT WITH VULNERABILITIES AND THREATS OBTAINED FROM THE ASSOCIATED ASSETS

FR-020 [DPRA Tool]: The RM suite shall publish the outcome of risk assessment through a comprehensive risk and control list.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the tool. Each asset is linked with vulnerabilities and threat to calculate the risk level. The risk level is shown for each asset.

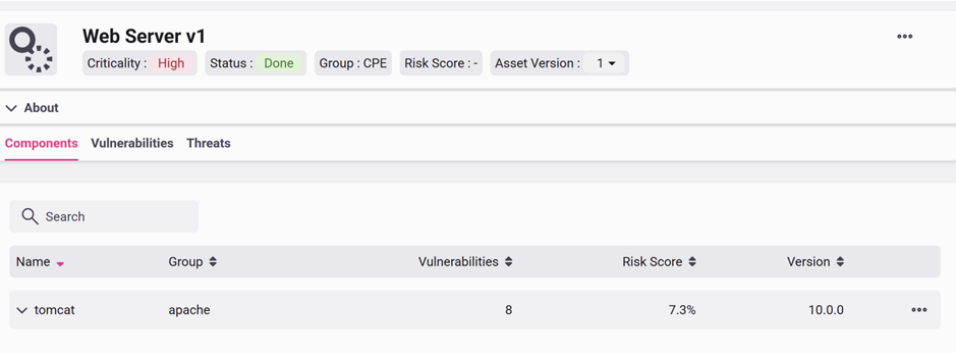


FIGURE 22: DPRA TOOL – RISK LEVEL SHOWN FOR EACH ASSET

FR-021 [CyReA Tool]: The questionnaire shall include several sections which are associated with key CRA areas related requirements including cybersecurity requirements for products with digital elements, vulnerability handling requirements, and Class I, Class II and Critical Class

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the CyReA tool. The questionnaire is organized based on the organization type and specific product types as well as specific class types including class I and Class II.

Does your organization manufacture, import, distribute or act as an authorized representative on behalf of an entity producing one or more of the following products?

- ☐ 1. Identity management systems software and privileged access management software;
- ☐ 2. Standalone and embedded browsers;
- ☐ 3. Password managers;
- ☐ 4. Software that searches for, removes, or quarantines malicious software;
- ☐ 5. Products with digital elements with the function of virtual private network (VPN);
- ☐ 6. Network management systems;
- ☐ 7. Network configuration management tools;
- ☐ 8. Network traffic monitoring systems;
- ☐ 9. Management of network resources;
- ☐ 10. Security information and event management (SIEM) systems;
- ☐ 11. Update/patch management, including boot managers;
- ☐ 12. Application configuration management systems;
- ☐ 13. Remote access/sharing software;
- ☐ 14. Mobile device management software;
- ☐ 15. Physical network interfaces;
- ☐ 16. Operating systems not covered by class II;
- ☒ 17. Firewalls, intrusion detection and/or prevention systems not covered by class II;
- ☐ 18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;
- ☐ 19. Microprocessors not covered by class II;
- ☐ 20. Microcontrollers;
- ☐ 21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
- ☐ 22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
- ☐ 23. Industrial Internet of Things not covered by class II.

FIGURE 23: CYReA TOOL – QUESTIONNAIRE BASED ON THE ORGANIZATION TYPE AND SPECIFIC PRODUCT TYPE

FR-022 [CyReA Tool]: The response of each question shall be characterized by the order of their appearance in the context of a question.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the CyReA tool. Respondents are only asked questions relevant to their specific situation, meaning the order in which questions appear reflects the logical path determined by their previous answers.

Question

Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing products with digital elements (as mentioned in the definition above)?

- ☒ Yes
☐ No

Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing medical devices as defined and regulated by the Regulation (EU) 2017/745?

- ☐ Yes
☒ No

Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing in vitro diagnostic medical devices as defined and regulated by the Regulation (EU) 2017/746?

- ☐ Yes
☒ No

Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles as defined and regulated by the Regulation (EU) 2019/2144?

- ☐ Yes
☒ No

Response:

Your products have been identified as falling within the scope of the EU CRA.

Based on the EU CRA, the following requirements have to be fulfilled by the Authorised representatives (Article 12)
1.A manufacturer may appoint an authorised representative by a written mandate.

2.The obligations laid down in Article 10(1) to (7) first indent and (9) shall not form part of the authorised representative's mandate.

3.An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:

(a)keep the EU declaration of conformity referred to in Article 20 and the technical documentation referred to in Article 23 at the disposal of the market surveillance authorities for ten years after the product with digital elements has been placed on the market;

(b)further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;

(c)cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed by a product with digital elements covered by the authorised representative's mandate.

FIGURE 24: CyReA TOOL – QUESTIONNAIRE AND RELATED RESPONSES

FR-023 [CyReA Tool]: Based on the answers to the questions, the user should be able to understand if at least one of their products with digital elements falls within the scope of the CRA.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the CyReA tool. Upon processing the user's responses to the questions, the CyReA tool classifies the product, and the user receives information on the scope of the product.

Your product(s), is classified as a Class 1, CRITICAL PRODUCTS WITH DIGITAL ELEMENTS.

According to the EU CRA, Critical products with digital elements should be subject to stricter conformity assessment procedures, while keeping a proportionate approach. For this purpose, critical products with digital elements are divided into two classes, reflecting the level of cybersecurity risk linked to these categories of products. A potential cyber incident involving products in class II might lead to greater negative impacts than an incident involving products in class I, for instance due to the nature of their cybersecurity-related function or intended use in sensitive environments, and therefore should undergo a stricter conformity assessment procedure.

The manufacturer shall perform a conformity assessment of the Class I, critical product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements by using one of the following procedures:

(a) EU-type examination procedure (based on module B) provided for in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or

(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.

FIGURE 25: CyReA TOOL – PROVIDING INFORMATION ABOUT THE SCOPE OF A PRODUCT

FR-024 [CyReA Tool]: ICT product shall be clearly categorized into four distinct classes including Default, Important Class I, Important Class II and Critical Class.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the CyReA tool. Based on the user's responses to the questions, the ICT product is categorized into four distinct classes.

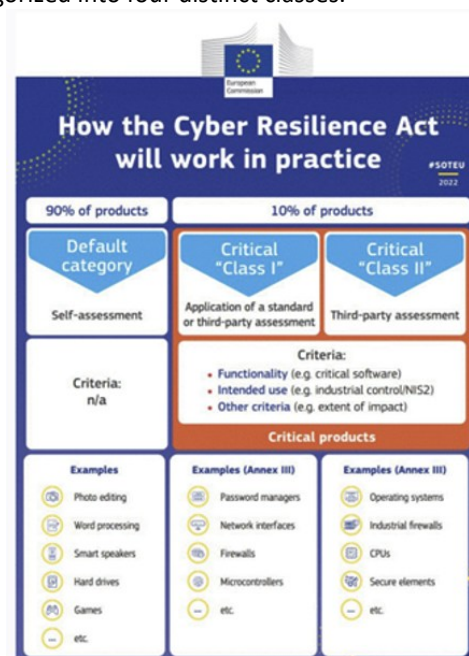


FIGURE 26: CyReA TOOL – CATEGORIZATION OF A PRODUCT INTO FOUR DISTINCT CLASSES

FR-025 [CyReA Tool]: The questionnaire response shall be correctly documented as a supporting document for the compliance achievement.

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

Verification is done through the demonstration by using the CyReA tool and response is correctly documented to support compliance.

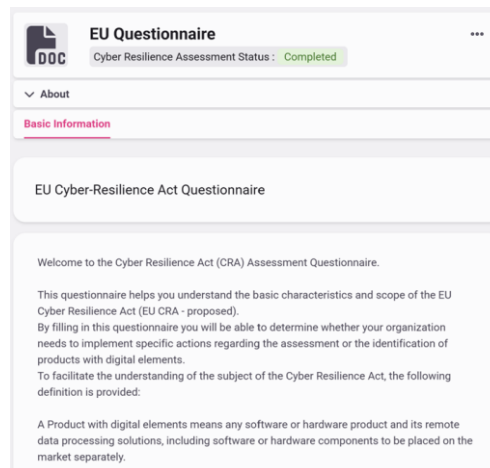


FIGURE 27: CyReA TOOL – PRESENTATION OF THE QUESTIONNAIRE AND PURPOSE

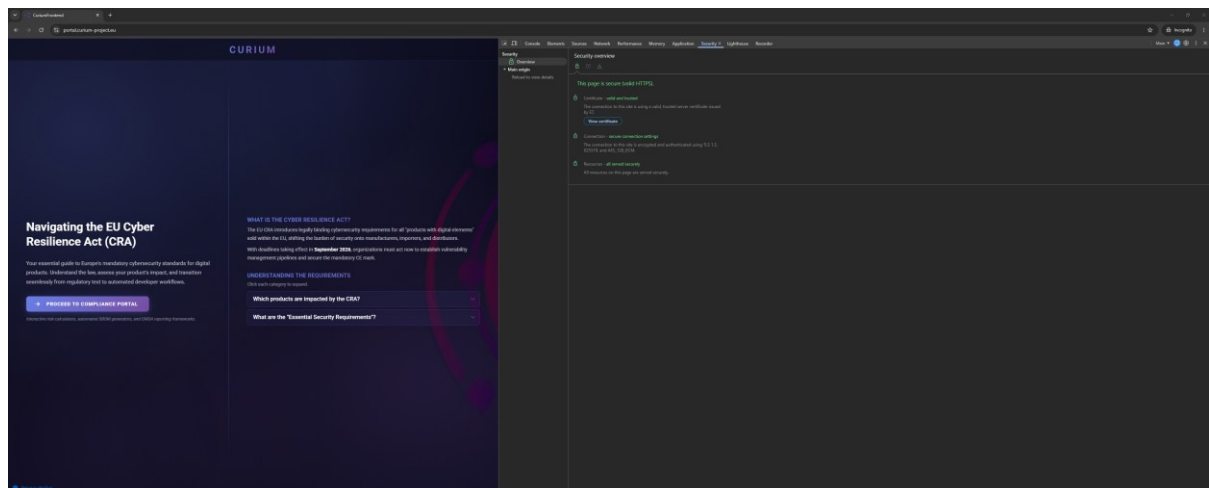
TR-001: HTTPS/TLS 1.3 must be used to access the tools

Evaluation Aspect: Functionality

Evaluation Method: Demonstration

Means to Verify:

1. Access the tool URL via a browser
2. Inspect the security certificate details
3. Confirm the protocol version is TLS 1.3 and the connection is encrypted



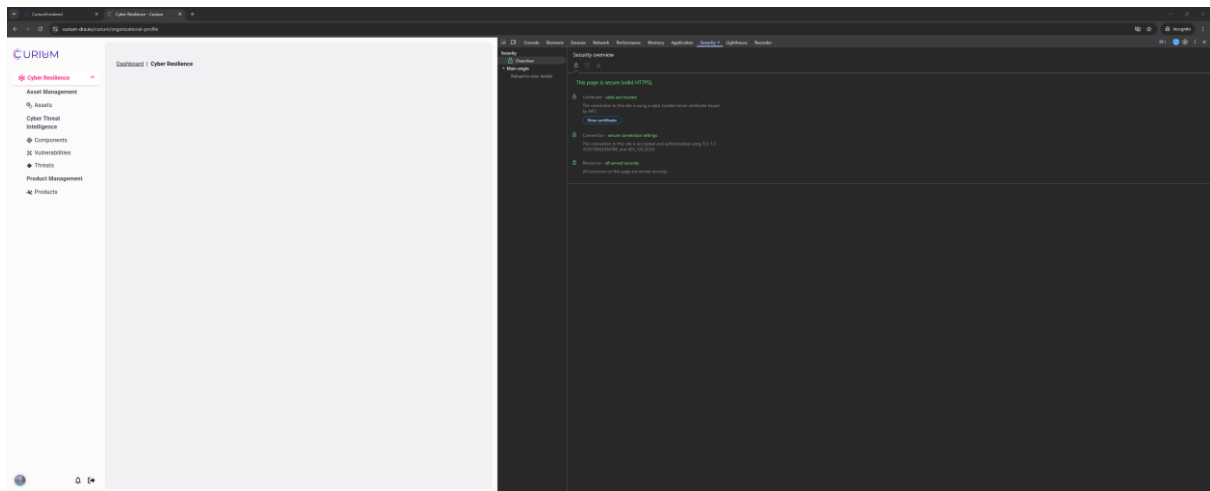


FIGURE 28: HTTPS/TLS 1.3 PROTOCOL FOR ACCESSING TOOLS CURIUM PORTAL TOOLS / CyReA

TR-002: SSO will be used for seamless access across the tools.

Evaluation Aspect: Usability and ease of access

Evaluation Method: Demonstration

Means to Verify:

1. Access the portal URL via a browser
2. Provide valid credentials
3. Check that access is provided to the CURIUM tools

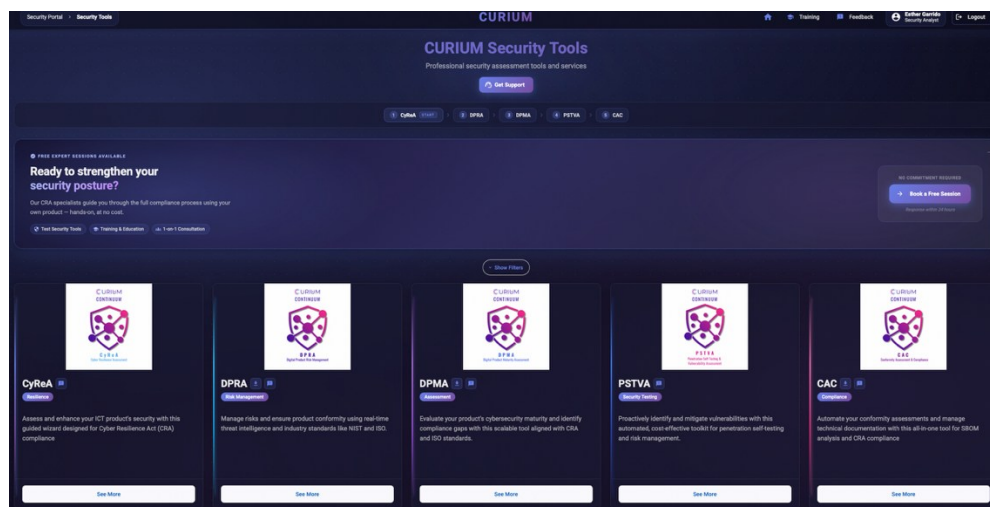


FIGURE 29: CURIUM PORTAL AND ITS TOOLS

TR-003: Containerization and independent deployment of the tool(s).

Evaluation Aspect: Reliability and Functional Stability

Evaluation Method: Inspection

Means to Verify:

1. Review the deployment artifacts (e.g., Dockerfiles, Kubernetes manifests)
2. Verify that each tool operates in an isolated container environment

```

grcuser@grcl1:~$ docker ps
CONTAINER ID   IMAGE                                STATUS      PORTS                               NAMES
4b309b89540f   registry-1.docker.io/multicomdocker/private:mtiles_api_oprisk.12022026v3 Up 3 months (healthy) 0.0.0.0:8080->8080/tcp, [::]:8080->8080/tcp   mtiles_api_oprisk
f014c28bcf6a   keycloak/keycloak:24.0             Up 3 months (healthy) 8080/tcp, 0.0.0.0:8443->8443/tcp, [::]:8443->8443/tcp   keycloak2x
7202d7a7d8d5   registry-1.docker.io/multicomdocker/private:mtiles_web_oprisk.06022026v1 Up 4 months (healthy) 80/tcp, 0.0.0.0:443->4200/tcp, [::]:443->4200/tcp   mtiles_web_oprisk
9cce0be5ec39   registry-1.docker.io/multicomdocker/private:oprisk-llm-15122025-1 Up 4 months (healthy) 8080/tcp, 0.0.0.0:8081->8080/tcp, [::]:8081->8080/tcp   oprisk_llm
a90ea52ca5ba   registry-1.docker.io/multicomdocker/private:mtiles_web_oprisk.103125v1 Up 6 months (healthy) 80/tcp, 0.0.0.0:3000->4200/tcp, [::]:3000->4200/tcp   mtiles_web_oprisk_cuc
5092219a2ad8   registry-1.docker.io/multicomdocker/private:mtiles_api_oprisk.103025v1 Up 6 months (healthy) 0.0.0.0:8083->8080/tcp, [::]:8083->8080/tcp   mtiles_api_oprisk_cuc
grcuser@grcl1:~$

```

FIGURE 30: ISOLATED CONTAINER ENVIRONMENT VERIFICATION

3. Confirm that restarting one container does not crash the others

```

grcuser@grcl1:~/docker$ docker ps
CONTAINER ID   IMAGE                                STATUS      PORTS                               COMMAND
4b309b89540f   registry-1.docker.io/multicomdocker/private:mtiles_api_oprisk.12022026v3 Up 3 months (healthy) 0.0.0.0:8080->8080/tcp, [::]:8080->8080/tcp   "sh -c ' upd
ate-ca-c-'
f014c28bcf6a   keycloak/keycloak:24.0             Up 3 months (healthy) 8080/tcp, 0.0.0.0:8443->8443/tcp, [::]:8443->8443/tcp   "/opt/keyclo
ak/bin/k-
7202d7a7d8d5   registry-1.docker.io/multicomdocker/private:mtiles_web_oprisk.06022026v1 Up 4 months (healthy) 80/tcp, 0.0.0.0:443->4200/tcp, [::]:443->4200/tcp   "/docker-ent
rpoint-...
9cce0be5ec39   registry-1.docker.io/multicomdocker/private:oprisk-llm-15122025-1 Up 46 seconds 8080/tcp, 0.0.0.0:8081->8080/tcp, [::]:8081->8080/
tcp   "python3 llm
.py"
a90ea52ca5ba   registry-1.docker.io/multicomdocker/private:mtiles_web_oprisk.103125v1 Up 6 months (healthy) 80/tcp, 0.0.0.0:3000->4200/tcp, [::]:3000->4200/tc
p   "/docker-ent
rpoint-...
5092219a2ad8   registry-1.docker.io/multicomdocker/private:mtiles_api_oprisk.103025v1 Up 6 months (healthy) 0.0.0.0:8083->8080/tcp, [::]:8083->8080/tcp   "sh -c ' upd
ate-ca-c-'
grcuser@grcl1:~/docker$ docker compose restart mtiles_web_oprisk
WARN[0000] /home/grcuser/docker/docker-compose.yaml: the attribute 'version' is obsolete, it will be i
gnored, please remove it to avoid potential confusion
[*] Restarting 1/1
✓Container mtiles_web_oprisk Started 0.6s
grcuser@grcl1:~/docker$ docker ps
CONTAINER ID   IMAGE                                STATUS      PORTS                               COMMAND
4b309b89540f   registry-1.docker.io/multicomdocker/private:mtiles_api_oprisk.12022026v3 Up 3 months (healthy) 0.0.0.0:8080->8080/tcp, [::]:8080->8080/tcp   "sh -c ' upd
ate-ca-c-'
f014c28bcf6a   keycloak/keycloak:24.0             Up 3 months (healthy) 8080/tcp, 0.0.0.0:8443->8443/tcp, [::]:8443->8443/tcp   "/opt/keyclo
ak/bin/k-
7202d7a7d8d5   registry-1.docker.io/multicomdocker/private:mtiles_web_oprisk.06022026v1 Up 5 seconds (health: starting) 80/tcp, 0.0.0.0:443->4200/tcp, [::]:443->4200/
tcp   "/docker-ent
rpoint-...
9cce0be5ec39   registry-1.docker.io/multicomdocker/private:oprisk-llm-15122025-1 Up About a minute 8080/tcp, 0.0.0.0:8081->8080/tcp, [::]:8081->8080/
tcp   "python3 llm
.py"
a90ea52ca5ba   registry-1.docker.io/multicomdocker/private:mtiles_web_oprisk.103125v1 Up 6 months (healthy) 80/tcp, 0.0.0.0:3000->4200/tcp, [::]:3000->4200/tc
p   "/docker-ent
rpoint-...
5092219a2ad8   registry-1.docker.io/multicomdocker/private:mtiles_api_oprisk.103025v1 Up 6 months (healthy) 0.0.0.0:8083->8080/tcp, [::]:8083->8080/
tcp   "sh -c ' upd
ate-ca-c-'
grcuser@grcl1:~/docker$

```

FIGURE 31: RESTARTING OF CONTAINERS VERIFICATION

Each tool run as Software as a Service form the user perspective, except PSTVA where the user must execute the Tool locally. The Containerization of the PSTVA has been covered on TR-010.

TR-004: Data Storage for evidence will be encrypted and immutable.

Evaluation Aspect: Reliability and Functional Stability

Evaluation Method: Inspection

Means to Verify:

1. Log in to CAC as admin
2. Checking requirement within CAC tool

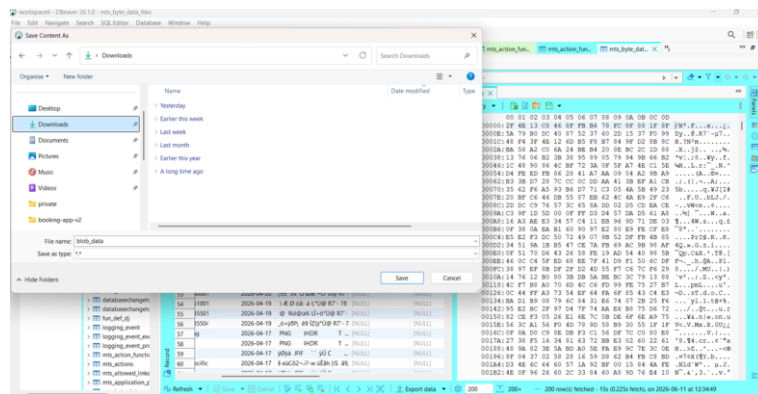


FIGURE 32: DATA STORAGE VERIFICATION

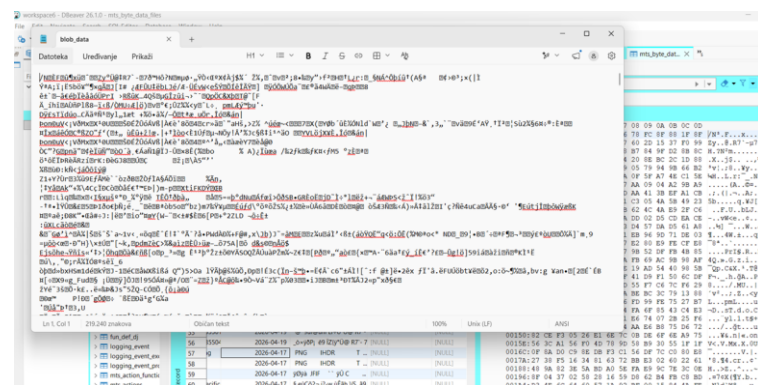


FIGURE 33: DATA STORAGE ENCRYPTED AND IMMUTABLE

TR-005: All user actions with timestamps, geo-location will be stored.

Evaluation Aspect: Reliability and Functional Stability

Evaluation Method: Inspection

Means to Verify:

1. Log in to CAC as admin
2. Checking requirement within CAC tool

Partially implemented. Timestamps are recorded; geolocation is not recorded due to the updated anonymisation policies and ease of access to the CURIUM portal via SSO using Keycloak AIM.

Assessments	SBOM	Recommendations	Documentation	Product images	Evaluation
Product_name	Product_code	Product_version	Status	Started	Next analysis
smart_keychain	smart_keychain	112.0	IN PROGRESS	11.06.2025 12:55:49	11.07.2025 12:55:49
smart_keychain	smart_keychain	111.0	IN PROGRESS	11.06.2025 12:54:58	11.07.2025 12:54:58
smart_keychain	smart_keychain	110.0	IN PROGRESS	20.05.2025	20.06.2025

FIGURE 34: ASSET INVENTORY

TR-006: Import & parse CycloneDX, SPDX, and JSON SBOM formats.

Evaluation Aspect: Functionality

Evaluation Method: Inspection

Means to Verify:

1. Upload SBOM

Assessments SBOM Recommendations Documentation Product images Evaluation						
Product_name	Product_code	Product_version	Status	Started	Next analysis	
smart_keycain	smart_keycain	112.0	IN PROGRESS	11.06.2026 12:55:49	11.07.2026 12:55:49	
smart_keycain	smart_keycain	111.0	IN PROGRESS	11.06.2026 12:54:58	11.07.2026 12:54:58	
smart_keycain	smart_keycain	110.0	STOP	20.05.2026	20.06.2026	

FIGURE 35: SBOM UPLOADED

2. SBOM test results review

web.cac-cyber.com

Account information

Product list

User Manual

T&C

	smart_keycain	smart_keycain	111.0		12.04.58	12.04.58	
	smart_keycain	smart_keycain	110.0		20.05.2026 09:54	20.06.2026 09:54	
	smart_keycain	smart_keycain	109.0		20.04.2026 09:53:50	20.05.2026 09:53:50	
	smart_keycain	smart_keycain	108.0		20.03.2026 09:53:39	20.04.2026 09:53:39	
	smart_keycain	smart_keycain	107.0		20.02.2026 09:53:29	20.03.2026 09:53:29	
	smart_keycain	smart_keycain	106.0		20.02.2026 09:53:24	20.03.2026 09:53:24	
	smart_keycain	smart_keycain	105.0		20.02.2026 09:53:23	20.03.2026 09:53:23	
	smart_keycain	smart_keycain	104.0		20.02.2026	20.03.2026	

1/3

1 2 3

Number of records: 102

component_name	component_version	description		severity	KEY due date	fix
X	X	X	X	X	X	X
	milike-app-24.8.1.jar	sha256:181e1a1cac75ee705d422843d51d855a7a1294c32128f5a8111571a421911				
	tomcat-embed-core	9.0.58	Apache Tomcat Time-of-attack Time-of-use (TOCTOU) Race Condition vulnerability	High	18.05.2026	Fixed in the following versions: 9.0.58
	log4j	1.2.17	SQL Injection in Log4j 1.2.x	Critical	18.05.2026	Vulnerability is not fixed yet.
	spring-security-core	5.6.2	Spring Security authorization rules can be bypassed via forward or include dispatcher types	Critical	18.05.2026	Fixed in the following versions: 5.6.9
	tomcat-embed-core	9.0.58	Apache Tomcat Open Redirect vulnerability	Medium	18.05.2026	Fixed in the following versions: 9.0.60
	spring-webmvc	5.3.10	Spring Framework MVC Applications Path Traversal Vulnerability	Medium	18.05.2026	Vulnerability is not fixed yet.
	spring-web	5.3.10	Spring Web vulnerable to Open Redirect or Server Side Request Forgery	High	18.05.2026	Fixed in the following versions: 5.3.32

Number of records: 9

FIGURE 36: SBOM TESTS PROVIDED

TR-007: API integration with NVD, OSV.dev, and/or OpenCVE, MISP.

Evaluation Aspect: Functionality

Evaluation Method: Inspection

Means to Verify:

- 1. Log in to CAC
- 2. Create a case
- 3. Trigger Post market analysis button

 	component_name	component_version	description	severity	KEY due date	fix
 X	core	X	X	X	X	X
			(UUC/OU) Race Condition vulnerability	High		
 	log4j	1.2.17	SQL Injection in Log4j 1.2.x	Critical	18.05.2026	Vulnerability is not fixed yet.
 	spring-security-core	5.6.2	Spring Security authorization rules can be bypassed via forward or include dispatcher types	Critical	18.05.2026	Fixed in the following versions: 5.6.9
 	tomcat-embed-core	9.0.58	Apache Tomcat Open Redirect vulnerability	Medium	18.05.2026	Fixed in the following versions: 9.0.60
 	spring-webmvc	5.3.10	Spring Framework MVC Applications Path Traversal Vulnerability	Medium	18.05.2026	Vulnerability is not fixed yet.
 	spring-web	5.3.10	Spring Web vulnerable to Open Redirect or Server Side Request Forgery	High	18.05.2026	Fixed in the following versions: 5.3.32
Number of records: 1						

FIGURE 37: PARSING FEEDBACK BASED ON API INTEGRATIONS

TR-008: All formats will be in PDF, Word, XML for technical documentation and reports.

Evaluation Aspect: Usability and ease of access

Evaluation Method: Demonstration

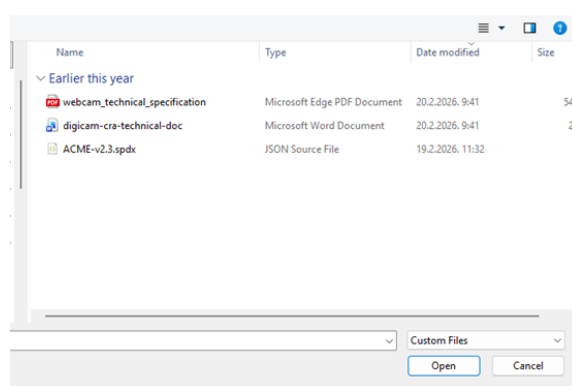
Means to Verify:

- 1. Log in to CAC

[D4.1: Validation and CURIUM Compliance Continuum assessment report]

2. Create a case
3. Generate technical documentation in PDF format

The screenshot shows the CAC - Curium web application. The main table lists products with columns: Product code, Product name, Product description, Product type, Product type free entry, Role, Bn..., Serial no..., Relevant EU legislation, Harmonized standards, and Additional info... The table contains four rows of data, including 'smart_keychain', 'dron_xjct', 'sfrs_1333', and 'Web camera'. Below the table are buttons for 'Add new product' and 'Save'. At the bottom, there are tabs for 'Assessments', 'SBOM', 'Recommendations', 'Documentation', 'Product images', and 'Evaluation', with 'Documentation' currently selected.



The screenshot shows the 'EU declaration of conformity' form. It includes the following sections:

- Company name:** MC
- Postal address:**
- Postal code:**
- City:**
- Phone number:**
- Declare that the DoC is issued under our sole responsibility and belongs to the following product:**
 - Product: Super dron
 - Type: UAW
 - Batch: 1
 - Serial number: 1239090
- The object of the DoC described above is in conformance with the relevant EU harmonized legislation:**
- The following harmonized standards and technical specifications have been applied:**
- Object of the declaration (identification of the product allowing traceability, may include color images, where necessary for the identification of the product):**
 - Four small images of the product are shown.
- Notified body:**
- Additional information:**

FIGURE 38: DOCUMENTATION FORMATS

TR-009: Secure document storage with version control and encryption (DEMF).

Evaluation Aspect: Functionality

Evaluation Method: Inspection

Means to Verify:

1. Log in to CAC as admin
2. Checking requirement within CAC tool

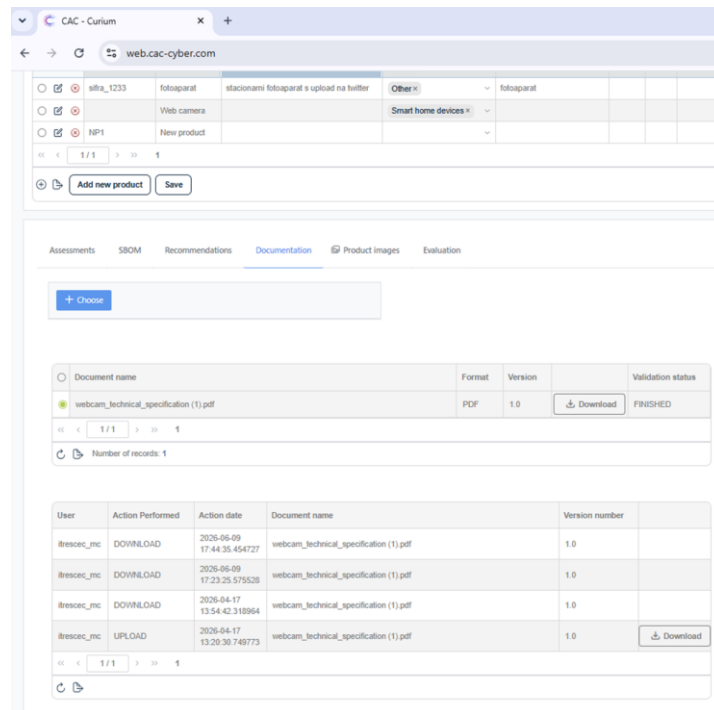


FIGURE 39: SECURE DOCUMENT STORAGE

TR-010: Local Execution

Evaluation aspect: Functionality

Evaluation method: Demonstration

Means to Verify:

1. Open the terminal
2. Git clone the repository
3. Make build (command)
4. Containers have been built
5. Application starts (command: make start)

```
#13 [9/9] COPY . ./app
#13 CACHED

#14 exporting to image
#14 exporting layers done
#14 writing image sha256:9bf0c54289f60ad3642c855b425eeb51b2c428448861bcb02bae08e7e69999e3 done
#14 naming to docker.io/library/curium-be:0.0.1 done
#14 DONE 0.0s

docker-compose -f compose.yml up -d
[+] Running 7/7
  ✓ Container curium-flower-1   Started      0.9s
  ✓ Container neo4j-db          Started      1.3s
  ✓ Container curium-traefik-1  Started      1.2s
  ✓ Container curium-back-1     Started      0.8s
  ✓ Container curium-redis-1    Running      0.0s
  ✓ Container curium-front-1    Started      0.9s
  ✓ Container curium-worker-1   Started      1.0s

Visit: curium.localhost with your browser

docker-compose -f compose.yml logs -f front back
back-1 | INFO: Will watch for changes in these directories: ['/app']
back-1 | INFO: Uvicorn running on http://0.0.0.0:8000 (Press CTRL+C to quit)
back-1 | INFO: Started reloader process [7] using StatReload
back-1 | INFO: Started server process [9]
back-1 | INFO: Waiting for application startup.
back-1 | INFO: Application startup complete.
back-1 | INFO: 172.18.0.8:57528 - "POST /back/login HTTP/1.1" 200 OK
```

FIGURE 40: SYSTEM INFORMATION UPON BUILDING ON TERMINAL

TR-011: Browser-based UI

Evaluation aspect: Usability and ease of access

Evaluation method: Demonstration

Means to Verify:

- 1.Users start the application on local on environment
- 2.Visit Browser UI @ <https://curium.localhost>

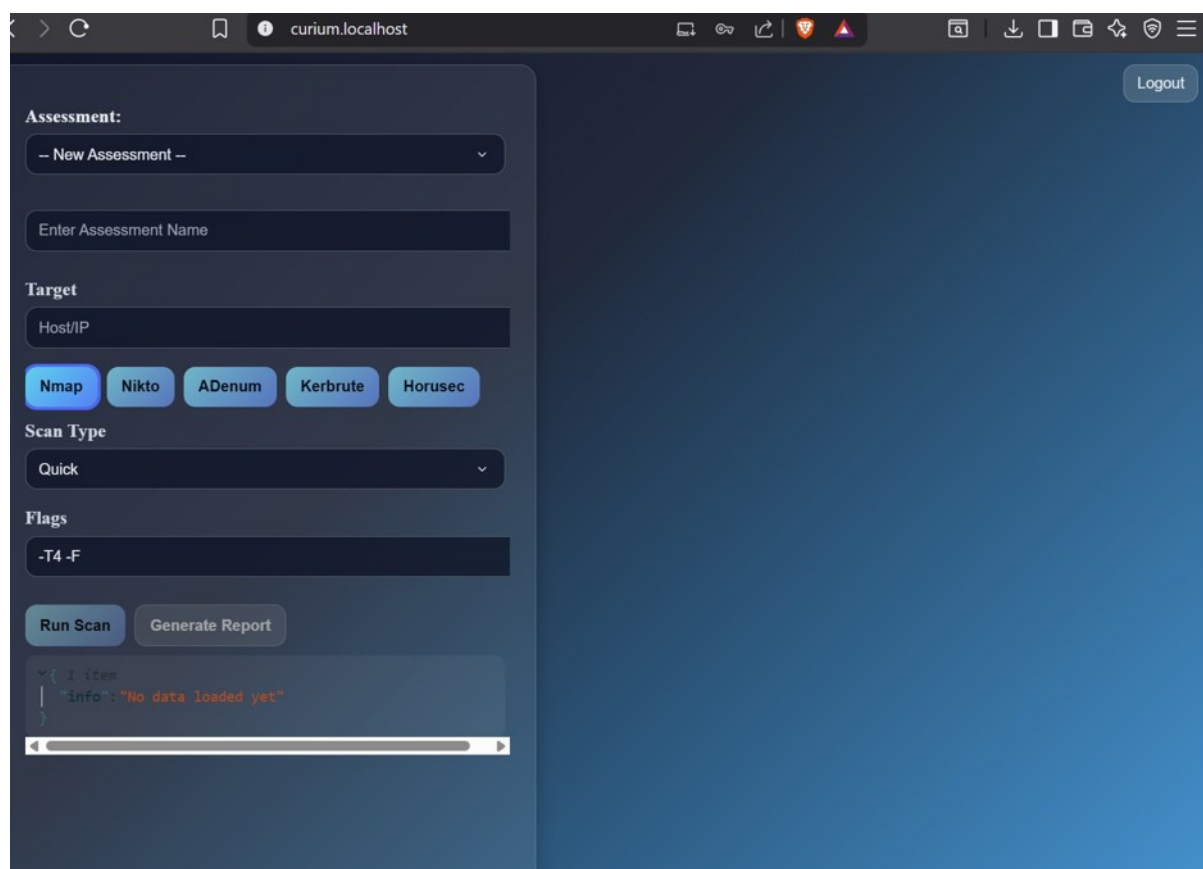


FIGURE 41: PSTVA USER INTERFACE AFTER LOG-IN

TR-012: Container Caching

Evaluation aspect: Functionality

Evaluation method: Demonstration

Means to Verify:

1. User clones the repository with git commands.
2. Runs the application first time with the command on the CLI (make start-boot).
3. Executes a vulnerability assessment.
4. Closes the PSTVA.
5. Closes the Docker.
6. Then reruns the PSTVA and Docker with the same CLI command (make start-boot)
7. The Terminal logs the container activity and the cached containers.

```
#6 [4/9] RUN mkdir -p /root/.vscode-server /root/.cache && mkdir -p /home/developer/.vscode-server /home/developer/.cache && chown -R developer:developer /home/developer/.vscode-server /home/developer/.cache
#6 CACHED

#7 [6/9] WORKDIR /app
#7 CACHED

#8 [2/9] RUN apt-get update && apt-get install -y git sudo && groupadd --gid 1000 developer && groupadd -g 1001 docker && useradd --uid 1000 --gid 1000 -m -G docker developer && echo developer ALL=(root) NOPASSWD:ALL > /etc/sudoers.d/developer && chmod 0440 /etc/sudoers.d/developer && rm -rf /var/lib/apt/lists/*
#8 CACHED

#9 [3/9] RUN mkdir /venv; chown -R 1000:1000 /venv
#9 CACHED

#10 [8/9] RUN /venv/bin/pip install -r requirements.txt
#10 CACHED

#11 [5/9] RUN python3 -m venv /venv
#11 CACHED

#12 [7/9] COPY requirements.txt .
#12 CACHED

#13 [9/9] COPY . ./app
#13 CACHED
```

FIGURE 42: DOCKER CONTAINER LOGS OF THE SYSTEM

TR-013: Support hybrid scan targets: local filesystem, Docker images, cloud registries, and web URLs with secure credential handling

Evaluation aspect: Functionality

Evaluation method: Demonstration

TABLE 2: MATRIX OF SCAN CAPABILITIES AGAINST SCAN TARGETS

Sub-capability	Artifact (what exists)	Means to Verify
Web URL targets	Nikto integration; sample scan report against a test URL	User runs Nikto on a test site with a planted issue (known missing header, hidden dir)
Local filesystem / source repo	Horusec integration; target-type selector showing filesystem/repo as a first-class kind	User scans a repo containing a dummy hardcoded secret / known-vulnerable dependency

TR-014: Able to view through Microsoft Excel 2016 or later. Operable on Windows and macOS.

Note: The DPMA tool was initially implemented as a Microsoft Excel workbook, and the technical requirements TR-014, TR-016 and TR-017 were specified against that baseline. APIROPLUS SERVICES, as the partner responsible for the development of the tool, subsequently decided to migrate it to a web application, retaining the same data structure and presentation format as the original workbook. The migration was driven by the need to remove client-side software dependencies and to allow integration with the CURIUM platform's Single Sign-On mechanism. The user-facing functionality of the tool was not reduced by this change. The requirements therefore remain valid in intent, but the means of verification have been updated to reflect the web-based implementation rather than the spreadsheet environment in which they were originally expressed.

[D4.1: Validation and CURIUM Compliance Continuum assessment report]

Evaluation aspect: Usability and ease of access

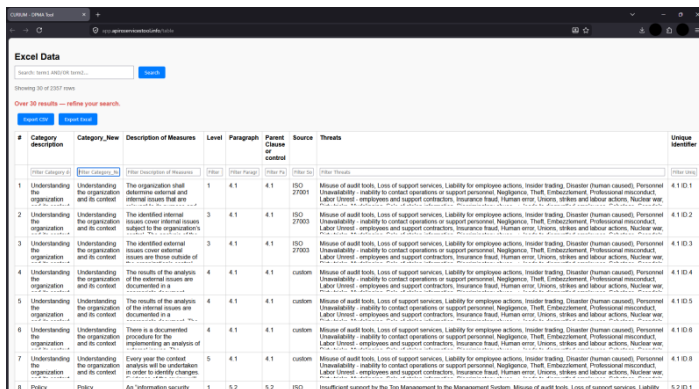
Evaluation method: Demonstration

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

1. Open the DPMA tool in a browser on Windows or macOS
2. Log in through the CURIUM platform SSO and confirm the tool is fully operable in both environments

The requirement was specified to ensure the tool could be used across Windows and macOS environments. Following the migration to a web application, the dependency on Microsoft Excel 2016 or later no longer applies: the tool is accessible through any modern web browser, and the portability objective is met more broadly than the requirement as written.



The screenshot shows a web application titled 'Excel Data' with a search bar and a table of measures. The table has columns for #, Category description, Category, New, Description of Measures, Level, Paragraph, Parent, Close, or, Source, Threats, and Unique Identifier. The table contains 8 rows of data, with the first 7 rows having a 'Threats' column and the 8th row having a 'Unique Identifier' column.

#	Category description	Category	New	Description of Measures	Level	Paragraph	Parent	Close	or	Source	Threats	Unique Identifier
1	Understanding the organization and its context	Other Categories	Other Categories	The organization shall address external and internal issues that are...	1	4.1	4.1	ISO	27001		Missed of audit tools, Loss of support services, Liability for employee actions, Insider trading, Cheating (human caused), Personnel Unavailability - inability to contact operators or support personnel, Negligence, Theft, Embodiment, Professional misconduct, Labor Union - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labor actions, Nuclear war...	4.1 E1.1
2	Understanding the organization and its context	Other Categories	Other Categories	The identified internal issues cover external issues subject to the organization's...	3	4.1	4.1	ISO	27001		Missed of audit tools, Loss of support services, Liability for employee actions, Insider trading, Cheating (human caused), Personnel Unavailability - inability to contact operators or support personnel, Negligence, Theft, Embodiment, Professional misconduct, Labor Union - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labor actions, Nuclear war...	4.1 E1.2
3	Understanding the organization and its context	Other Categories	Other Categories	The identified external issues cover external issues are those outside of...	3	4.1	4.1	ISO	27001		Missed of audit tools, Loss of support services, Liability for employee actions, Insider trading, Cheating (human caused), Personnel Unavailability - inability to contact operators or support personnel, Negligence, Theft, Embodiment, Professional misconduct, Labor Union - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labor actions, Nuclear war...	4.1 E1.3
4	Understanding the organization and its context	Other Categories	Other Categories	The results of the analysis of the external issues are documented in a...	4	4.1	4.1	custom			Missed of audit tools, Loss of support services, Liability for employee actions, Insider trading, Cheating (human caused), Personnel Unavailability - inability to contact operators or support personnel, Negligence, Theft, Embodiment, Professional misconduct, Labor Union - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labor actions, Nuclear war...	4.1 E1.4
5	Understanding the organization and its context	Other Categories	Other Categories	The results of the analysis of the external issues are documented in a...	4	4.1	4.1	custom			Missed of audit tools, Loss of support services, Liability for employee actions, Insider trading, Cheating (human caused), Personnel Unavailability - inability to contact operators or support personnel, Negligence, Theft, Embodiment, Professional misconduct, Labor Union - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labor actions, Nuclear war...	4.1 E1.5
6	Understanding the organization and its context	Other Categories	Other Categories	There is a documented procedure for the implementing an analysis of...	4	4.1	4.1	custom			Missed of audit tools, Loss of support services, Liability for employee actions, Insider trading, Cheating (human caused), Personnel Unavailability - inability to contact operators or support personnel, Negligence, Theft, Embodiment, Professional misconduct, Labor Union - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labor actions, Nuclear war...	4.1 E1.6
7	Understanding the organization and its context	Other Categories	Other Categories	Every year the context analysis will be performed in order to specify changes...	5	4.1	4.1	custom			Missed of audit tools, Loss of support services, Liability for employee actions, Insider trading, Cheating (human caused), Personnel Unavailability - inability to contact operators or support personnel, Negligence, Theft, Embodiment, Professional misconduct, Labor Union - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labor actions, Nuclear war...	4.1 E1.8
8	Policy	Policy	Policy	Information security	1	5.2	5.2	ISO			Inefficient support by the Top Management to the Management System, Missed of audit tools, Loss of support services, Liability...	5.2 E1.1

FIGURE 43: DPMA TOOL – VIEWED VIA BROWSER

TR-016: Ability to use (Excel) functions: SUM, IF, COUNTIF, XLOOKUP, INDEX/MATCH, and more in order to filter through and select needed results. Conditional formatting dynamically updates cell visuals based on rule conditions (e.g., scores of "0" appear red).

Note: The DPMA tool was initially implemented as a Microsoft Excel workbook, and the technical requirements TR-014, TR-016 and TR-017 were specified against that baseline. APIROPLUS SERVICES, as the partner responsible for the development of the tool, subsequently decided to migrate it to a web application, retaining the same data structure and presentation format as the original workbook. The migration was driven by the need to remove client-side software dependencies and to allow integration with the CURIUM platform's Single Sign-On mechanism. The user-facing functionality of the tool was not reduced by this change. The requirements therefore remain valid in intent, but the means of verification have been updated to reflect the web-based implementation rather than the spreadsheet environment in which they were originally expressed.

Evaluation aspect: Functionality

Evaluation method: Demonstration

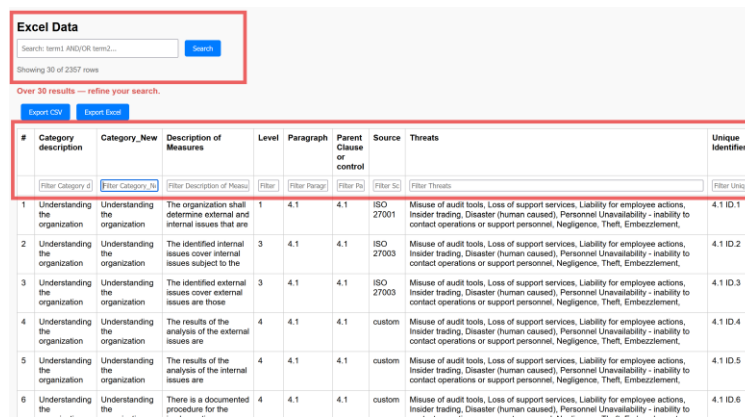
For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

The system has been migrated to a web app. Necessary formulas and functions are embedded.

1. Login to the DPMA tool
2. Use the filters
3. Confirm that results are filtered and returned correctly
4. Export the results to xlsx format and perform any Excel functions necessary in the local file.

The requirement was specified in terms of Excel functions (SUM, IF, COUNTIF, XLOOKUP, INDEX/MATCH) and conditional formatting, as these were the means available in the spreadsheet implementation to filter, look up and visually differentiate entries. In the web application these capabilities are provided natively through the tool's search and filtering interface, with the necessary formulas and logic embedded in the application.



Excel Data

Search: term1 AND/OR term2... [Search](#)

Showing 30 of 2357 rows

Over 30 results — refine your search.

[Export CSV](#) [Export Excel](#)

#	Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
1	Understanding the organization	Understanding the organization	The organization shall determine external and internal issues that are subject to the organization's control.	1	4.1	4.1	ISO 27001	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, Negligence, Theft, Embezzlement.	4.1 ID.1
2	Understanding the organization	Understanding the organization	The identified internal issues cover internal issues subject to the organization's control.	3	4.1	4.1	ISO 27003	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, Negligence, Theft, Embezzlement.	4.1 ID.2
3	Understanding the organization	Understanding the organization	The identified external issues cover external issues that are those of the organization.	3	4.1	4.1	ISO 27003	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, Negligence, Theft, Embezzlement.	4.1 ID.3
4	Understanding the organization	Understanding the organization	The results of the analysis of the external issues are those of the organization.	4	4.1	4.1	custom	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, Negligence, Theft, Embezzlement.	4.1 ID.4
5	Understanding the organization	Understanding the organization	The results of the analysis of the internal issues are those of the organization.	4	4.1	4.1	custom	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, Negligence, Theft, Embezzlement.	4.1 ID.5
6	Understanding the organization	Understanding the organization	There is a documented procedure for the implementation and maintenance of the information security management system.	4	4.1	4.1	custom	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, Negligence, Theft, Embezzlement.	4.1 ID.6

FIGURE 44: DPMA TOOL – FORMULAS EMBEDDED IN THE WEB APP

TR-017: Integrity. Sheet-level protection and locked formula cells to maintain integrity. Data validation rules to restrict incorrect entry (e.g., dropdowns for grading).

Note: The DPMA tool was initially implemented as a Microsoft Excel workbook, and the technical requirements TR-014, TR-016 and TR-017 were specified against that baseline. APIROPLUS SERVICES, as the partner responsible for the development of the tool, subsequently decided to migrate it to a web application, retaining the same data structure and presentation format as the original workbook. The migration was driven by the need to remove client-side software dependencies and to allow integration with the CURIUM platform's Single Sign-On mechanism. The user-facing functionality of the tool was not reduced by this change. The requirements therefore remain valid in intent, but the means of verification have been updated to reflect the web-based implementation rather than the spreadsheet environment in which they were originally expressed.

Evaluation aspect: Functionality

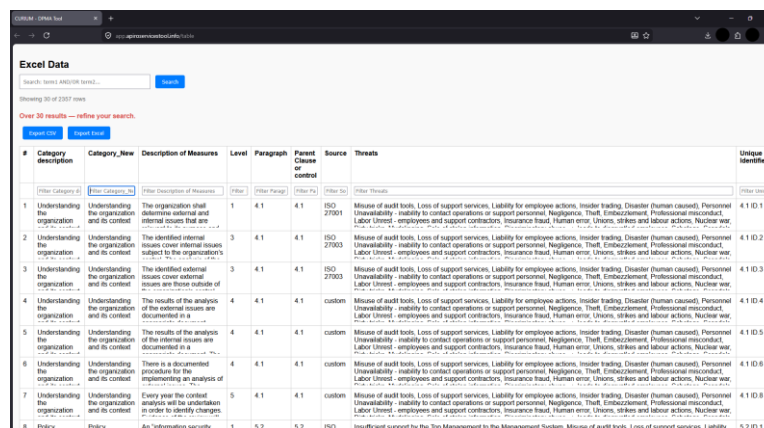
Evaluation method: Test

For a person to have access to this specific functionality, the following assumptions apply: The person needs to have a valid account to access the DPMA tool.

Means to Verify:

1. Login to the DPMA tool
2. Attempt to modify any entry in the results table
3. Confirm that no change can be made and the dataset remains unaltered

The requirement was specified as sheet-level protection, locked formula cells and data validation rules, these being the integrity mechanisms available in a spreadsheet. In the web application, the dataset is presented to the end user in read-only form and integrity is enforced server-side, which removes the possibility of a user altering entries rather than merely discouraging it.



Excel Data

Search: term1 AND/OR term2... [Search](#)

Showing 30 of 2357 rows

Over 30 results — refine your search.

[Export CSV](#) [Export Excel](#)

#	Category description	Category_New	Description of Measures	Level	Paragraph	Parent Clause or control	Source	Threats	Unique Identifier
1	Understanding the organization	Understanding the organization	The organization shall determine external and internal issues that are subject to the organization's control.	1	4.1	4.1	ISO 27001	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, Negligence, Theft, Embezzlement, Professional misconduct, Labor Unrest - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labour actions, Nuclear war, Data breach - confidentiality, integrity, availability, privacy, information security, Intellectual property, Reputation, Financial, Environmental, Physical, Legal, Regulatory, Compliance, Societal, Technological, Political, Geographical, Demographic, Psychological, Physiological, Behavioral, Cultural, Linguistic, Religious, Ethnic, Racial, Gender, Age, Disability, Sexual Orientation, Gender Identity, Marital Status, Family Status, Parental Status, Grandparental Status, Sibling Status, Nephew/Niece Status, Aunt/Uncle Status, Cousin Status, In-Law Status, Step-Relationship Status, Foster Care Status, Adoption Status, Surrogate Parenthood Status, Donor Conception Status, Reproductive Technology Status, Organ Donation Status, Stem Cell Transplantation Status, Gene Editing Status, CRISPR Status, Synthetic Biology Status, Nanotechnology Status, Biotechnology Status, Space Exploration Status, Deep Sea Exploration Status, Arctic Exploration Status, Antarctic Exploration Status, Outer Space Exploration Status, Mars Exploration Status, Venus Exploration Status, Jupiter Exploration Status, Saturn Exploration Status, Uranus Exploration Status, Neptune Exploration Status, Pluto Exploration Status, Dwarf Planet Exploration Status, Asteroid Exploration Status, Comet Exploration Status, Meteorite Exploration Status, Lunar Exploration Status, Planetary Exploration Status, Interplanetary Exploration Status, Interstellar Exploration Status, Extraterrestrial Exploration Status, Cosmic Exploration Status, Galactic Exploration Status, Universal Exploration Status.	4.1 ID.1
2	Understanding the organization	Understanding the organization	The identified internal issues cover internal issues subject to the organization's control.	3	4.1	4.1	ISO 27003	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, Negligence, Theft, Embezzlement, Professional misconduct, Labor Unrest - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labour actions, Nuclear war, Data breach - confidentiality, integrity, availability, privacy, information security, Intellectual property, Reputation, Financial, Environmental, Physical, Legal, Regulatory, Compliance, Societal, Technological, Political, Geographical, Demographic, Psychological, Physiological, Behavioral, Cultural, Linguistic, Religious, Ethnic, Racial, Gender, Age, Disability, Sexual Orientation, Gender Identity, Marital Status, Family Status, Parental Status, Grandparental Status, Sibling Status, Nephew/Niece Status, Aunt/Uncle Status, Cousin Status, In-Law Status, Step-Relationship Status, Foster Care Status, Adoption Status, Surrogate Parenthood Status, Donor Conception Status, Reproductive Technology Status, Organ Donation Status, Stem Cell Transplantation Status, Gene Editing Status, CRISPR Status, Synthetic Biology Status, Nanotechnology Status, Biotechnology Status, Space Exploration Status, Deep Sea Exploration Status, Arctic Exploration Status, Antarctic Exploration Status, Outer Space Exploration Status, Mars Exploration Status, Venus Exploration Status, Jupiter Exploration Status, Saturn Exploration Status, Uranus Exploration Status, Neptune Exploration Status, Pluto Exploration Status, Dwarf Planet Exploration Status, Asteroid Exploration Status, Comet Exploration Status, Meteorite Exploration Status, Lunar Exploration Status, Planetary Exploration Status, Interplanetary Exploration Status, Interstellar Exploration Status, Extraterrestrial Exploration Status, Cosmic Exploration Status, Galactic Exploration Status, Universal Exploration Status.	4.1 ID.2
3	Understanding the organization	Understanding the organization	The identified external issues cover external issues that are those of the organization.	3	4.1	4.1	ISO 27003	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, Negligence, Theft, Embezzlement, Professional misconduct, Labor Unrest - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labour actions, Nuclear war, Data breach - confidentiality, integrity, availability, privacy, information security, Intellectual property, Reputation, Financial, Environmental, Physical, Legal, Regulatory, Compliance, Societal, Technological, Political, Geographical, Demographic, Psychological, Physiological, Behavioral, Cultural, Linguistic, Religious, Ethnic, Racial, Gender, Age, Disability, Sexual Orientation, Gender Identity, Marital Status, Family Status, Parental Status, Grandparental Status, Sibling Status, Nephew/Niece Status, Aunt/Uncle Status, Cousin Status, In-Law Status, Step-Relationship Status, Foster Care Status, Adoption Status, Surrogate Parenthood Status, Donor Conception Status, Reproductive Technology Status, Organ Donation Status, Stem Cell Transplantation Status, Gene Editing Status, CRISPR Status, Synthetic Biology Status, Nanotechnology Status, Biotechnology Status, Space Exploration Status, Deep Sea Exploration Status, Arctic Exploration Status, Antarctic Exploration Status, Outer Space Exploration Status, Mars Exploration Status, Venus Exploration Status, Jupiter Exploration Status, Saturn Exploration Status, Uranus Exploration Status, Neptune Exploration Status, Pluto Exploration Status, Dwarf Planet Exploration Status, Asteroid Exploration Status, Comet Exploration Status, Meteorite Exploration Status, Lunar Exploration Status, Planetary Exploration Status, Interplanetary Exploration Status, Interstellar Exploration Status, Extraterrestrial Exploration Status, Cosmic Exploration Status, Galactic Exploration Status, Universal Exploration Status.	4.1 ID.3
4	Understanding the organization	Understanding the organization	The results of the analysis of the external issues are those of the organization.	4	4.1	4.1	custom	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, Negligence, Theft, Embezzlement, Professional misconduct, Labor Unrest - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labour actions, Nuclear war, Data breach - confidentiality, integrity, availability, privacy, information security, Intellectual property, Reputation, Financial, Environmental, Physical, Legal, Regulatory, Compliance, Societal, Technological, Political, Geographical, Demographic, Psychological, Physiological, Behavioral, Cultural, Linguistic, Religious, Ethnic, Racial, Gender, Age, Disability, Sexual Orientation, Gender Identity, Marital Status, Family Status, Parental Status, Grandparental Status, Sibling Status, Nephew/Niece Status, Aunt/Uncle Status, Cousin Status, In-Law Status, Step-Relationship Status, Foster Care Status, Adoption Status, Surrogate Parenthood Status, Donor Conception Status, Reproductive Technology Status, Organ Donation Status, Stem Cell Transplantation Status, Gene Editing Status, CRISPR Status, Synthetic Biology Status, Nanotechnology Status, Biotechnology Status, Space Exploration Status, Deep Sea Exploration Status, Arctic Exploration Status, Antarctic Exploration Status, Outer Space Exploration Status, Mars Exploration Status, Venus Exploration Status, Jupiter Exploration Status, Saturn Exploration Status, Uranus Exploration Status, Neptune Exploration Status, Pluto Exploration Status, Dwarf Planet Exploration Status, Asteroid Exploration Status, Comet Exploration Status, Meteorite Exploration Status, Lunar Exploration Status, Planetary Exploration Status, Interplanetary Exploration Status, Interstellar Exploration Status, Extraterrestrial Exploration Status, Cosmic Exploration Status, Galactic Exploration Status, Universal Exploration Status.	4.1 ID.4
5	Understanding the organization	Understanding the organization	The results of the analysis of the internal issues are those of the organization.	4	4.1	4.1	custom	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, Negligence, Theft, Embezzlement, Professional misconduct, Labor Unrest - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labour actions, Nuclear war, Data breach - confidentiality, integrity, availability, privacy, information security, Intellectual property, Reputation, Financial, Environmental, Physical, Legal, Regulatory, Compliance, Societal, Technological, Political, Geographical, Demographic, Psychological, Physiological, Behavioral, Cultural, Linguistic, Religious, Ethnic, Racial, Gender, Age, Disability, Sexual Orientation, Gender Identity, Marital Status, Family Status, Parental Status, Grandparental Status, Sibling Status, Nephew/Niece Status, Aunt/Uncle Status, Cousin Status, In-Law Status, Step-Relationship Status, Foster Care Status, Adoption Status, Surrogate Parenthood Status, Donor Conception Status, Reproductive Technology Status, Organ Donation Status, Stem Cell Transplantation Status, Gene Editing Status, CRISPR Status, Synthetic Biology Status, Nanotechnology Status, Biotechnology Status, Space Exploration Status, Deep Sea Exploration Status, Arctic Exploration Status, Antarctic Exploration Status, Outer Space Exploration Status, Mars Exploration Status, Venus Exploration Status, Jupiter Exploration Status, Saturn Exploration Status, Uranus Exploration Status, Neptune Exploration Status, Pluto Exploration Status, Dwarf Planet Exploration Status, Asteroid Exploration Status, Comet Exploration Status, Meteorite Exploration Status, Lunar Exploration Status, Planetary Exploration Status, Interplanetary Exploration Status, Interstellar Exploration Status, Extraterrestrial Exploration Status, Cosmic Exploration Status, Galactic Exploration Status, Universal Exploration Status.	4.1 ID.5
6	Understanding the organization	Understanding the organization	There is a documented procedure for the implementation and maintenance of the information security management system.	4	4.1	4.1	custom	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, Negligence, Theft, Embezzlement, Professional misconduct, Labor Unrest - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labour actions, Nuclear war, Data breach - confidentiality, integrity, availability, privacy, information security, Intellectual property, Reputation, Financial, Environmental, Physical, Legal, Regulatory, Compliance, Societal, Technological, Political, Geographical, Demographic, Psychological, Physiological, Behavioral, Cultural, Linguistic, Religious, Ethnic, Racial, Gender, Age, Disability, Sexual Orientation, Gender Identity, Marital Status, Family Status, Parental Status, Grandparental Status, Sibling Status, Nephew/Niece Status, Aunt/Uncle Status, Cousin Status, In-Law Status, Step-Relationship Status, Foster Care Status, Adoption Status, Surrogate Parenthood Status, Donor Conception Status, Reproductive Technology Status, Organ Donation Status, Stem Cell Transplantation Status, Gene Editing Status, CRISPR Status, Synthetic Biology Status, Nanotechnology Status, Biotechnology Status, Space Exploration Status, Deep Sea Exploration Status, Arctic Exploration Status, Antarctic Exploration Status, Outer Space Exploration Status, Mars Exploration Status, Venus Exploration Status, Jupiter Exploration Status, Saturn Exploration Status, Uranus Exploration Status, Neptune Exploration Status, Pluto Exploration Status, Dwarf Planet Exploration Status, Asteroid Exploration Status, Comet Exploration Status, Meteorite Exploration Status, Lunar Exploration Status, Planetary Exploration Status, Interplanetary Exploration Status, Interstellar Exploration Status, Extraterrestrial Exploration Status, Cosmic Exploration Status, Galactic Exploration Status, Universal Exploration Status.	4.1 ID.6
7	Understanding the organization	Understanding the organization	Every year the control analysis will be undertaken in order to identify changes.	5	4.1	4.1	custom	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, Negligence, Theft, Embezzlement, Professional misconduct, Labor Unrest - employees and support contractors, Insurance fraud, Human error, Unions, strikes and labour actions, Nuclear war, Data breach - confidentiality, integrity, availability, privacy, information security, Intellectual property, Reputation, Financial, Environmental, Physical, Legal, Regulatory, Compliance, Societal, Technological, Political, Geographical, Demographic, Psychological, Physiological, Behavioral, Cultural, Linguistic, Religious, Ethnic, Racial, Gender, Age, Disability, Sexual Orientation, Gender Identity, Marital Status, Family Status, Parental Status, Grandparental Status, Sibling Status, Nephew/Niece Status, Aunt/Uncle Status, Cousin Status, In-Law Status, Step-Relationship Status, Foster Care Status, Adoption Status, Surrogate Parenthood Status, Donor Conception Status, Reproductive Technology Status, Organ Donation Status, Stem Cell Transplantation Status, Gene Editing Status, CRISPR Status, Synthetic Biology Status, Nanotechnology Status, Biotechnology Status, Space Exploration Status, Deep Sea Exploration Status, Arctic Exploration Status, Antarctic Exploration Status, Outer Space Exploration Status, Mars Exploration Status, Venus Exploration Status, Jupiter Exploration Status, Saturn Exploration Status, Uranus Exploration Status, Neptune Exploration Status, Pluto Exploration Status, Dwarf Planet Exploration Status, Asteroid Exploration Status, Comet Exploration Status, Meteorite Exploration Status, Lunar Exploration Status, Planetary Exploration Status, Interplanetary Exploration Status, Interstellar Exploration Status, Extraterrestrial Exploration Status, Cosmic Exploration Status, Galactic Exploration Status, Universal Exploration Status.	4.1 ID.8
8	Policy	Policy	As "Information security"	1	5.2	5.2	ISO	Insufficient support by the Top Management to the Management System, Misuse of audit tools, Loss of support services, Liability	5.2 ID.1

FIGURE 45: DPMA TOOL – WEB-BASED APP PROVIDING INTEGRITY

NFR-001: The system should be accessible via any browser.

Evaluation Aspect: Usability and ease of access

Evaluation Method: Test

Means to Verify:

1. Launch the application in the latest versions of major browsers (e.g., Chrome, Firefox, Edge, Safari)
2. Perform a standard workflow (e.g., login, scan, logout)
3. Verify that the layout remains consistent and no functionality breaks across browsers

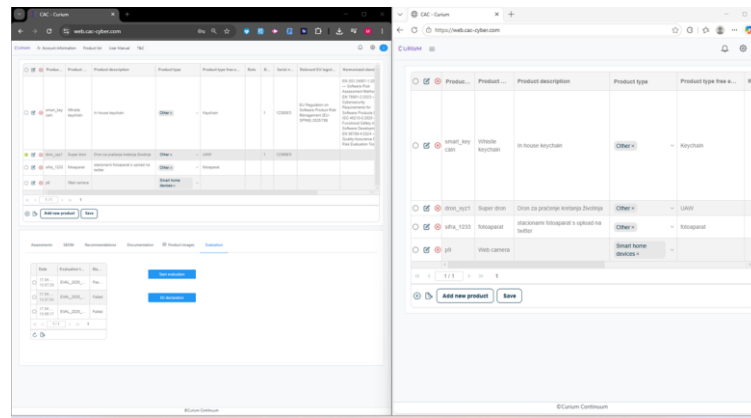


FIGURE 46: SYSTEM ACCESSIBLE VIA ANY BROWSER

NFR-003: Each tool must provide error handling and guided help messages.

Evaluation Aspect: Usability and ease of access

Evaluation Method: Test

Means to Verify:

1. Intentionally trigger an error (e.g., upload invalid file format)
2. Verify that the system displays a clear, human-readable error message explaining how to fix the issue (rather than a raw code stack trace)

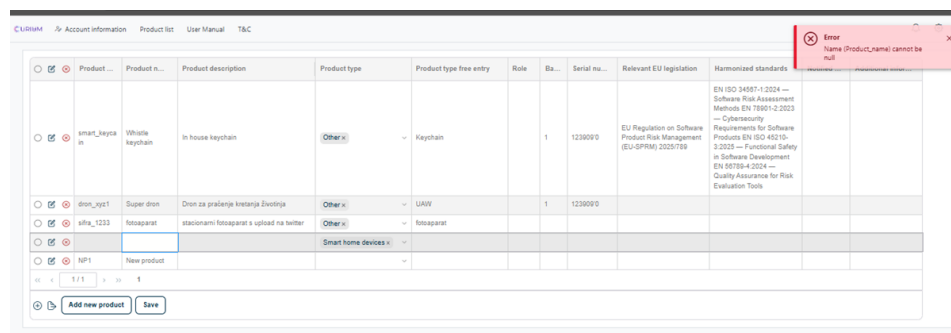


FIGURE 47: CAC TOOL - ERROR HANDLING MESSAGE

NFR-004: The system must be GDPR compliant (data processing, retention, consent)

Evaluation Aspect: Reliability and Functional Stability

Evaluation Method: Inspection

Means to Verify:

1. Log in via landing page (dashboard)
2. Check internally preserving and encrypting all sensitive data

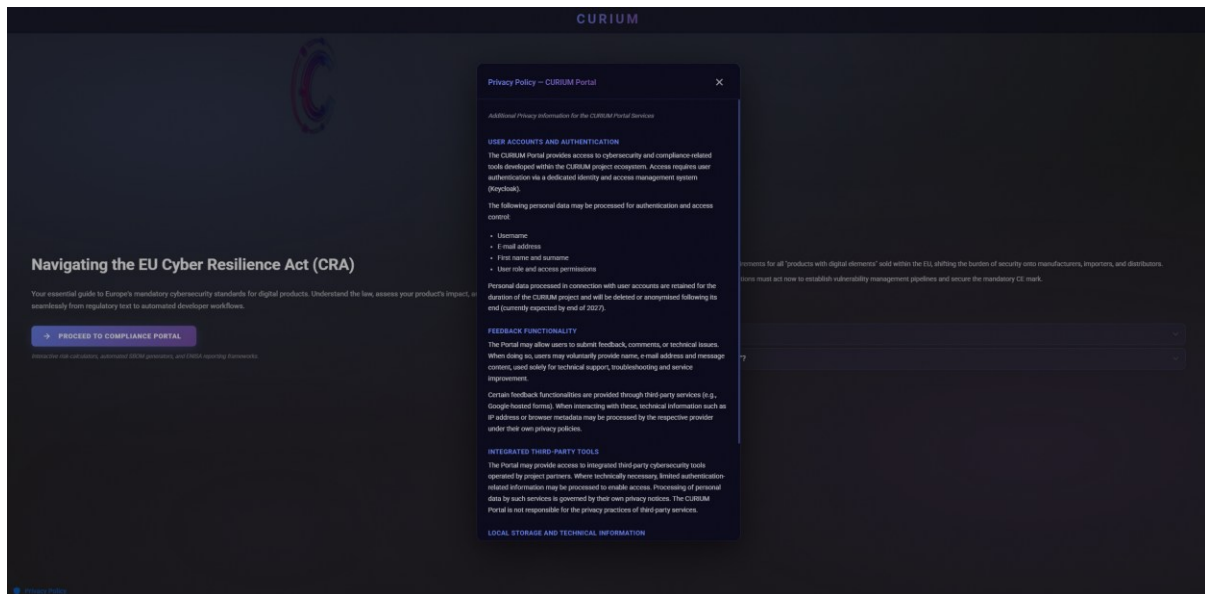


FIGURE 48: CURIUM PORTAL PRIVACY POLICY

NFR-006: The system should allow easy updates and patches

Evaluation Aspect: Reliability and Functional Stability

Evaluation Method: Demonstration

Means to Verify:

1. Log in via Curium portal (dashboard)
2. Demonstrate internally updating and patching option



FIGURE 49: FIRST VERSION OF THE LOGIN USER INTERFACE

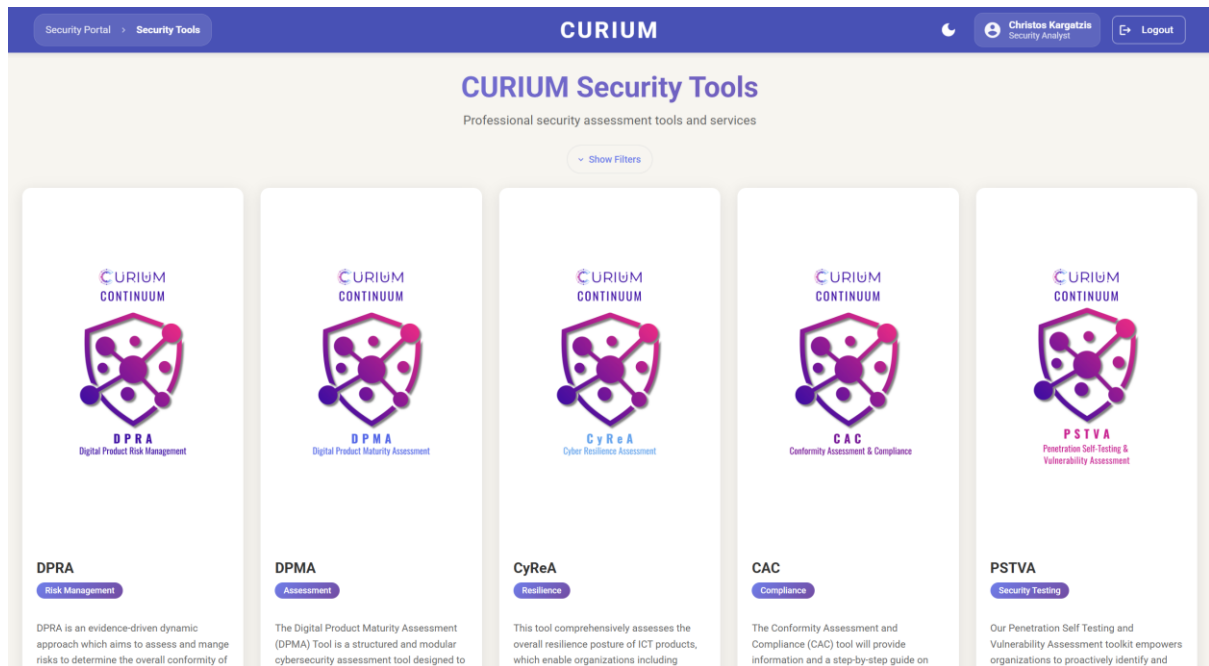


FIGURE 50: OLD VERSION OF CURIUM PORTAL USER INTERFACE

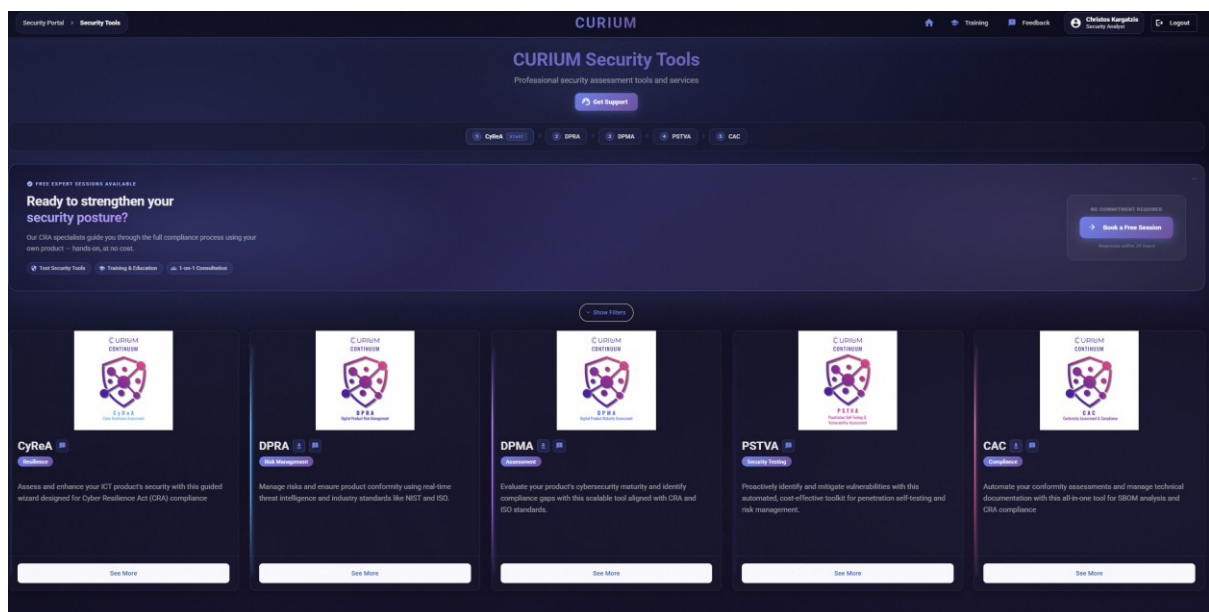


FIGURE 51: LATEST VERSION OF CURIUM PORTAL USER INTERFACE

NFR-007: The system should be resource efficient

Evaluation Aspect: Financial Factors

Evaluation Method: Test, direct observation of container resource consumption via docker stats, captured at three defined operational states and compared against declared thresholds.

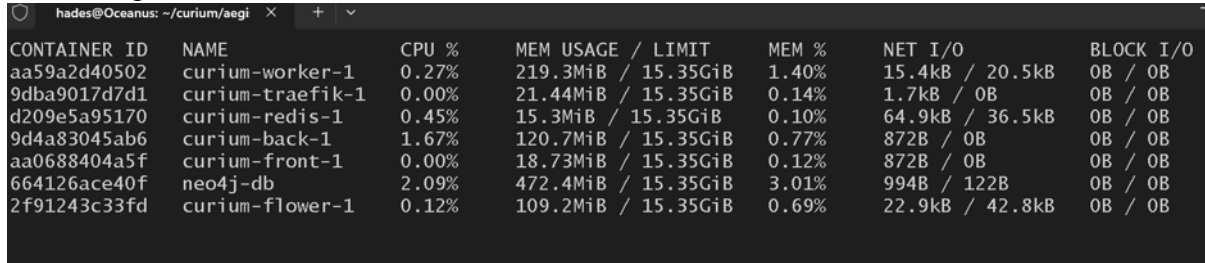
Declared thresholds (set by the project, example values, adjust to user target):

- Idle footprint: ≤ 2 GiB total memory and $\leq 10\%$ aggregate CPU across all services.
- Under-load peak: bounded by worker concurrency: total memory ≤ 4 GiB during concurrent scanning.
- Post-load reclamation: total memory returns within 10% of the idle baseline after a campaign is completed.

Means to Verify:

1. Deploy the full stack (FastAPI backend, frontend, Traefik, Redis, Celery worker, Flower, Neo4j) via Docker.

2. Idle capture — with no scans running, record docker stats --no-stream. Sum CPU % and MEM USAGE across all containers.
3. Under-load capture — submit a defined workload (e.g. 10 concurrent scans against fixed test targets); record docker stats at peak.
4. Post-load capture — allow the campaign to complete and ephemeral scanner containers to tear down; record docker stats again.



CONTAINER ID	NAME	CPU %	MEM USAGE / LIMIT	MEM %	NET I/O	BLOCK I/O
aa59a2d40502	curium-worker-1	0.27%	219.3MiB / 15.35GiB	1.40%	15.4kB / 20.5kB	0B / 0B
9dba9017d7d1	curium-traefik-1	0.00%	21.44MiB / 15.35GiB	0.14%	1.7kB / 0B	0B / 0B
d209e5a95170	curium-redis-1	0.45%	15.3MiB / 15.35GiB	0.10%	64.9kB / 36.5kB	0B / 0B
9d4a83045ab6	curium-back-1	1.67%	120.7MiB / 15.35GiB	0.77%	872B / 0B	0B / 0B
aa0688404a5f	curium-front-1	0.00%	18.73MiB / 15.35GiB	0.12%	872B / 0B	0B / 0B
664126ace40f	neo4j-db	2.09%	472.4MiB / 15.35GiB	3.01%	994B / 122B	0B / 0B
2f91243c33fd	curium-flower-1	0.12%	109.2MiB / 15.35GiB	0.69%	22.9kB / 42.8kB	0B / 0B

FIGURE 52: RESOURCES CONSUMPTION OF EACH TOOL'S CONTAINER

NFR-008: Enforce Least-privilege execution to avoid privileged containers unless necessary

Privileged-container avoidance: verified that no container runs privileged or shares host namespaces (docker inspect). Least-privilege execution: partially enforced — one documented necessary exception (worker: Docker-API access for scanner orchestration, network-isolated, localhost-bound); remaining hardening (non-root default, capability dropping, reduction of socket exposure on back/traffic) identified and scheduled.

Evaluation Aspect: Reliability and Functional Stability

Evaluation method: Inspection, docker inspect inspection script, reproducible on demand

Means to Verify:

```
hades@Oceanus:~/curium/aegis-security-assessment-toolkit$ for c in curium-worker-1 curium-traefik-1 curium-redis-1 curium-back-1 \1 curium-back-1 \ curium-front-1 neo4j-db curium-flower-1; do
    echo "$c: privileged=$(docker inspect --format '{{.HostConfig.Privileged}}' "$c") \
netmode=$(docker inspect --format '{{.HostConfig.NetworkMode}}' "$c")"
done
curium-worker-1: privileged=false netmode=curium_default
curium-traefik-1: privileged=false netmode=curium_default
curium-redis-1: privileged=false netmode=curium_default
curium-back-1: privileged=false netmode=curium_default
curium-front-1: privileged=false netmode=curium_default
neo4j-db: privileged=false netmode=curium_default
curium-flower-1: privileged=false netmode=curium_default
```

FIGURE 53: PRIVILEGE CONFIGURATIONS FOR EACH TOOL'S CONTAINER

NFR-009: Provide user manuals for CLI and Web UI explaining installation, configuration, and usage

Evaluation Aspect: Knowledge capacity

Evaluation Method: Demonstration

Means to Verify:

1. User logs in on the portal.
2. Navigates through the tools
3. Selects the button with the Download manual for the CyReA, DPMA, DPRA, CAC or select the PSTVA
4. User gets a PDF file or a dedicated page (only for the PSTVA) with documentations and guidance for each tool.



FIGURE 54: EXAMPLE FROM PSTVA USER MANUAL

NFR-010: Maintain detailed technical documentation including architecture

Evaluation Aspect: Knowledge capacity

Evaluation Method: Demonstration

Means to Verify: After users download or visit the repository get a README.md file with detailed technical documentation and the full architecture.

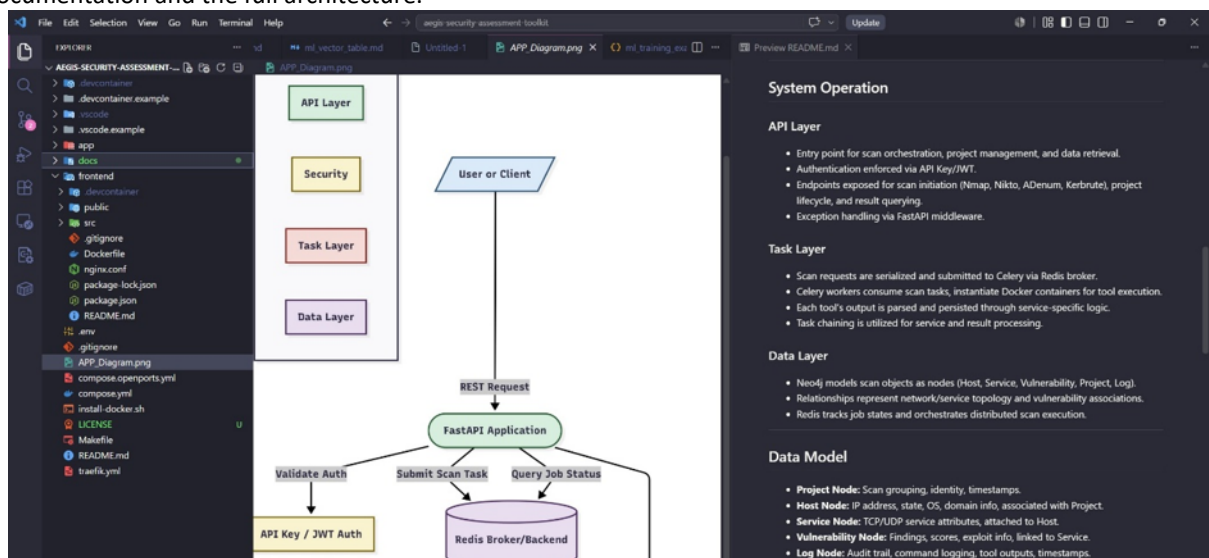


FIGURE 55: TECHNICAL DOCUMENTATION AND ARCHITECTURE OF THE PSTVA INSIDE THE REPOSITORY

NFR-011: RM suite shall be flexible enough to allow the legitimate users to use the DPR service with strong authentication and authorization practice

Evaluation Aspect: Reliability and Functional Stability

Evaluation Method: Demonstration

Means to Verify:

Performed through a demonstration using the DPRA tool. Users must authenticate themselves using valid credentials before accessing the DPR service. Access to system functions and data is restricted according to assigned user roles and permissions. The demonstration shows that only authenticated and authorized users can access the service and perform permitted actions, while unauthorized users are denied access.

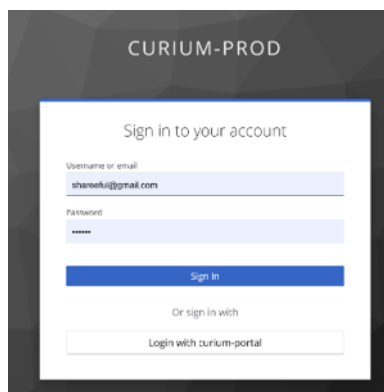


FIGURE 56: DPRA TOOL - ACCESS ONLY FOR AUTHORIZED USERS

NFR-012: The Dashboard of RM suite shall be a clean, intuitive interface that makes it easy for users to find information and perform tasks without extensive training

Evaluation Aspect: Usability and ease of access

Evaluation Method: Demonstration

Means to Verify:

Verification is performed through a demonstration using the DPRA tool. Users access the dashboard and successfully locate information and perform key tasks through the interface. The clear navigation structure and organised presentation of information demonstrate that the dashboard is intuitive and easy to use without extensive training.

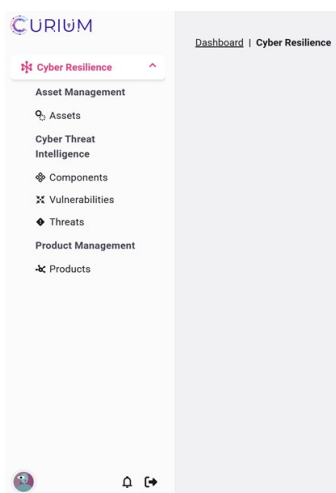


FIGURE 57: DPRA TOOL – EXAMPLE OF THE INTUITIVE INTERFACE

NFR-013: The RM suite shall allow the user to connect through standard browser and securely store risk assessment outcome

Evaluation Aspect: Usability and ease of access

Evaluation Method: Demonstration

Means to Verify:

Verification is performed through a demonstration using the DPRA tool. Users access the RM suite through a standard web browser, perform a risk assessment, and save the assessment outcome. The stored results can subsequently be retrieved by authorised users, demonstrating secure storage and browser-based access.

Id	Base score	Exploitability score	Impact score	Epss score	Percentile	Severity
CVE-2024-7553	78.0%	18.0%	59.0%	0.0%	5.0%	High
CVE-2023-20564	67.0%	8.0%	59.0%	0.0%	5.0%	Medium
CVE-2023-20560	44.0%	8.0%	36.0%	0.0%	11.7%	Medium
CVE-2022-44702	78.0%	18.0%	59.0%	0.6%	77.7%	High

FIGURE 58: DPRA TOOL – EXAMPLE OF SECURE STORAGE AND BROWSER-BASED ACCESS

NFR-014: The RM suite shall provide a high degree of interoperability to integrate the data from the open intelligence in real time

Evaluation Aspect: Reliability and Functional Stability

Evaluation Method: Demonstration

Means to Verify:

Verification is performed through a demonstration using the DPRA tool. The tool integrates and consumes data from external open intelligence sources, including NIST NVD and MITRE CAPEC, through standard interfaces and data formats. During the demonstration, vulnerability and threat information is retrieved and processed in real time to support risk assessment activities. The successful integration and utilisation of data from multiple external repositories demonstrate the interoperability of the RM suite and its ability to incorporate up-to-date open intelligence information.

Id	Name	Likelihood	Status
CAPEC-94	Adversary in the Middle (AiTM)	High	Stable
CAPEC-92	Forced Integer Overflow	High	Draft
CAPEC-9	Buffer Overflow in Local Command-Line Utilities	High	Draft
CAPFC-88	OS Command Injection	High	Draft
CAPFC-85	AIAX Footprinting	High	Draft

Id	Base score	Exploitability score	Impact score	Epss score	Severity
CVE-2024-45112	78.0%	18.0%	59.0%	0.1%	High
CVE-2024-41869	78.0%	18.0%	59.0%	0.1%	High
CVE-2024-7553	78.0%	18.0%	59.0%	0.0%	High

FIGURE 59: DPRA TOOL - ABILITY TO INCORPORATE UP-TO-DATE OPEN INTELLIGENCE INFORMATION

NFR-015: The tool shall allow access to legitimate users to provide response to the questionnaire

Evaluation Aspect: Usability and ease of access

Evaluation Method: Demonstration

Means to Verify:

The verification is performed through a demonstration using the CyReA tool. Users must authenticate with valid credentials before accessing the questionnaire. Once authenticated, authorised users are able to access, complete, and submit questionnaire responses. The demonstration confirms that only legitimate users can access the questionnaire and provide responses, while unauthorised users are denied access.

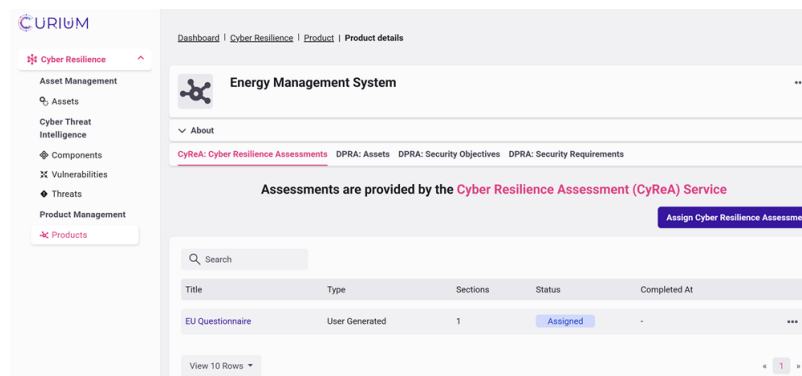


FIGURE 60: CYREA TOOL – ACCESS ONLY FOR AUTHORIZED USERS

NFR-016: The tool shall provide a systematic list of questions related to the cyber resilience assessment of the products with digital elements through an on-line wizard based interactive capability to allow the user to respond to the relevant questions

Evaluation Aspect: Usability and ease of access

Evaluation Method: Demonstration

Means to Verify:

The verification is performed through a demonstration using the CyReA tool. The tool presents users with a structured and systematic questionnaire through an online wizard-based interface. Users are guided through the assessment process step-by-step and are provided with relevant questions based on the selected organisation, product, and assessment context. The demonstration confirms that users can navigate the questionnaire, respond to the presented questions, and complete the cyber resilience assessment through the interactive wizard.

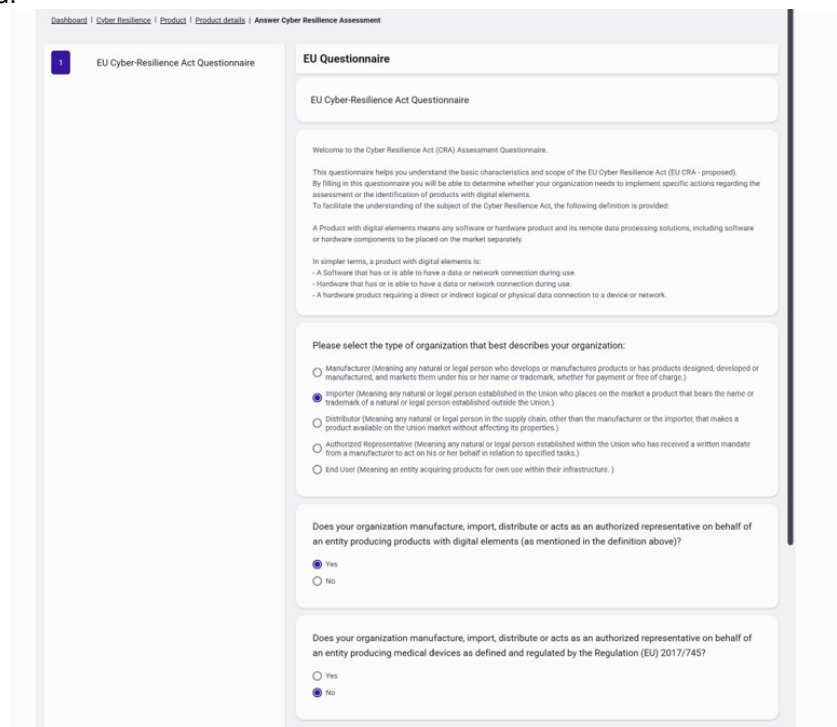


FIGURE 61: CYREA TOOL – INTERACTIVE WIZARD-BASED QUESTIONNAIRE

4.2.2. Key Performance Indicators (KPIs)

Twenty (20) KPIs are tracked in this deliverable. They are the ones related to technical validation and the validation process itself, both internal and external.

KPI1: Number of tools to facilitate and automate CRA compliance

Target: >10

Achieved: 20

Method:

An architectural audit was carried out for each of the five CURIUM services, listing every distinct backend engine, scanner and functional module integrated in it. Components are classified as third-party open-source engines integrated by CURIUM, or as in-house modules developed in the project. Full descriptions are given in D3.1 and D3.2.

Service	Component	Type	What it automates
CyReA	Readiness wizard	In-house	Role and scope determination, exclusion screening, Class I/II classification, conformity-assessment readiness
DPRA	Dynamic risk calculation backend	In-house	Multi-order risk estimation with cascading effects across product assets
DPRA	SBOM vulnerability assessment	In-house	Vulnerability identification for declared components
DPRA	CTI open repository	In-house	Real-time threat and vulnerability intelligence from open sources
DPRA	Security evaluation framework	In-house	ISO/IEC 15408 assurance level, objectives, requirements and NIST 800-53 control mapping
DPRA	Protection Profile generator	In-house	Consolidated protection profile for the product
DPMA	Measures and maturity engine	In-house	Search, filtering, maturity levels (1–6), threat-to-measure mapping, CSV/Excel export
CAC	Automated self-assessment	In-house	Questionnaire scoring, KPI and qualitative result
CAC	SBOM analyser	In-house	SPDX 2.3 parsing, component tree, vulnerability highlighting
CAC	Technical documentation manager	In-house	Annex VII document set, gap tracking
CAC	Recommendations engine	In-house	Gap aggregation from assessment, SBOM and documentation, with action tracking
CAC	EU DoC generator	In-house	Declaration of Conformity once all steps have been passed
PSTVA	Nmap	Third-party	Network and service discovery
PSTVA	Nikto	Third-party	Web server auditing
PSTVA	Ffuf	Third-party	Directory and parameter fuzzing
PSTVA	Kerbrute	Third-party	Kerberos account enumeration
PSTVA	ADenum	Third-party	Active Directory misconfiguration checks
PSTVA	Horusec	Third-party	Static analysis of source code
PSTVA	SmartGraph	In-house	Vulnerability oriented taxonomy structures for GraphDB
PSTVA	Report generation	In-house	Unified vulnerability report with impacts and prioritised remediations

The total is 6 third-party engines and 14 in-house modules, across all five services.

KPI2: Number of CRA essential requirements fully covered by tools

Target: 13 of the 21 essential requirements in CRA Annex I (13 SRs, 8 VRs)

Achieved: 12

Method:

A Compliance Coverage Matrix was built, mapping each Annex 2 – Compliance Coverage Matrix requirement to the CURIUM tool features that address it. A requirement is counted as fully covered when at least one tool generates an output for it automatically, without the user having to upload manual evidence. Where the tools only provide templates, questionnaire items, control selection or upload slots, the requirement is counted under KPI3. The two sets are mutually exclusive and together cover all 21 requirements.

TABLE 3: ESSENTIAL REQUIREMENTS COMPLIANCE COVERAGE MATRIX FULLY COVERED BY CURIUM TOOLS

Req	Tool(s)	Automated output
SR1	DPRA	Multi-order risk assessment per asset (threats, vulnerabilities, calculated risks); Protection Profile
SR2	CAC, PSTVA, DPRA	Known vulnerabilities flagged in the SBOM component tree; scan findings; CTI-based vulnerability identification
SR3a	PSTVA, DPRA	Misconfiguration findings from network and web server scans, with prioritised reconfiguration advice
SR3b	PSTVA, DPRA	Authentication and enumeration findings (Kerbrute, ADenum); requirements derived automatically from the selected security objectives
SR3c	PSTVA, DPRA	Web and transport-layer findings; confidentiality-related requirements derived from objectives
SR3f	DPRA	Propagated risk and cascading-effect estimates on essential assets
SR3g	DPRA	Cascading-effect analysis across interdependent assets and infrastructures
SR3h	PSTVA	Exposed services, ports, directories and parameters (Nmap, Ffuf, Nikto)
SR3i	PSTVA, DPRA	Exploitability checks (e.g. injection, overflow) with threat metrics; attack potential in the evaluation criteria
VR1	CAC	SPDX 2.3 SBOM import, component tree and per-component vulnerabilities
VR2	CAC, PSTVA	Recommendations generated automatically from SBOM and assessment results, with action tracking; prioritised remediations
VR3	PSTVA, CAC	Repeatable automated scans and static code analysis (Horsesec) with consolidated reporting; timestamped self-assessments with a KPI score

While the KPI2 target is 13 requirements fully covered, CURIUM originally aimed for full coverage of 15 requirements, including VR4–VR6. However, these three requirements (public disclosure of fixed vulnerabilities, a coordinated vulnerability disclosure policy, and a reporting contact point) are organisational obligations that a manufacturer fulfils through internal policies and publications, rather than through direct tool output. As such, CURIUM supports them through guided compliance rather than full automation, and they are more accurately reported under KPI3 (partial coverage). All in all, coverage of all 21 requirements is maintained across KPI2 and KPI3 combined.

KPI3: Number of CRA essential requirements partially covered by tools

Target: >6

Achieved: 9

Method:

A requirement is counted as partially covered when CURIUM provides guided compliance: a questionnaire item, a catalogue of measures, a manual control assignment or a documentation slot where the user uploads evidence, without the tool verifying the requirement itself.

TABLE 4: ESSENTIAL REQUIREMENTS PARTIALLY COVERED AND GUIDED COMPLIANCE

Req	Guided-compliance mechanism	What remains manual
SR3d	DPRA integrity objective and NIST control assignment; CAC questionnaire	Proof that integrity protection and corruption reporting are implemented
SR3e	CAC questionnaire and documentation; DPMA measures	Data-minimisation justification for the intended use
SR3j	DPMA logging and monitoring measures with maturity levels; DPRA audit controls	Evidence of the product's logging capability
SR3k	CAC questionnaire and Annex VII documentation	Description and proof of the update mechanism
VR4	Advisory content available from CAC and PSTVA findings (description, impact, severity, remediation)	Drafting and publishing the advisory
VR5	CAC documentation slot for the vulnerability management plan	Writing and enforcing the CVD policy
VR6	CAC user-instructions documentation; DPRA CTI repository	Providing and operating the contact address
VR7	CAC questionnaire and documentation	Evidence of the secure distribution channel
VR8	CAC questionnaire and documentation	Evidence of free, timely dissemination with advisories

KPI4: Number of tools to simplify and automate CRA compliance documentation obligations

Target: ≥ 2

Achieved: 2

Method:

The CURIUM Compliance Continuum includes the following tools that simplify and automate the creation of technical documentation required under CRA Annex VII:

1. CAC - provides a guided approach to technical documentation and self-gap analysis, ensuring alignment with CRA requirements
2. PSTVA - equips users with tools for vulnerability assessment, code review, and penetration testing, reinforcing compliance efforts

The rest of the CURIUM tools (CyReA, DPRA, DPMA) also support upstream CRA compliance activities, such as scope determination, risk assessment, and risk mitigation planning. Therefore, CURIUM provides at least two tools that simplify and support CRA compliance documentation obligations, and KPI4 is validated internally.

KPI7: Number of open-source tools to be used

Target: > 8

Achieved: 15

Method:

The CURIUM Compliance Continuum leverages widely recognised open-source intelligence sources to support cybersecurity and CRA compliance activities:

1. CVE (Common Vulnerabilities and Exposures) for identifying publicly disclosed vulnerabilities.
2. CPE (Common Platform Enumeration) for standardised identification of ICT products and technologies.

3. CAPEC (Common Attack Pattern Enumeration and Classification) for identifying and analysing cyberattack patterns and threats.
4. Nmap
5. Nikto
6. Horusec
7. ADENUM
8. Kerbrute
9. Keycloak
10. Grype
11. Spring Boot
12. SPDX 2.3
13. Apache Maven
14. Ollama
15. Qwen3-4B

These open-source resources are integrated within the CURIUM tools to support vulnerability identification, threat analysis, and risk assessment activities, Static code analysis. Therefore, KPI7 is achieved through the use of 15 open-source intelligence sources.

KPI16: Number of open-source components made available

Target: >5

Achieved: 5

Method:

Under the CURIUM, 5 components have been prepared.

PSTVA will be released as open-source, comprising five separately usable components developed in the project. They are described in D3.1 and D3.2 and will be published in the repository: <https://github.com/Aegis-IT-Research/PSTVA>.

TABLE 5: OPEN-SOURCE COMPONENTS MADE AVAILABLE

Component	Description
IAM	Identity and access management for the PSTVA platform (in-house code)
Frontend	User interface for scan configuration and results
Backend	Orchestration of scans, storage and querying of results
Scanning environment	Containerised environment running the integrated scanners
SmartGraph	Vulnerability oriented taxonomy structures for GraphDB

KPI19: Number of release rounds

Target: >=2

Achieved: 3

Round 1 was the first release of the tools and services to the community (M56, M8-M12) documented in D3.1.

Round 2 is the mid-term release of the CURIUM Compliance Continuum (M16), documented in D3.2.

Round 3 (M18) is the final release, incorporating the refinements from iterative development, validation and feedback collection with WP4 and external stakeholders.

KPI23: Open-source tools examined for their integration into CURIUM

Target: > 10

Achieved: 14

Method:

As part of the development of the CURIUM Compliance Continuum, 14 open-source cybersecurity tools and resources were systematically assessed for potential integration, exceeding the KPI target of more than 10. The assessment covered CVE, CPE, CAPEC, Nmap, Netdiscover, Nikto, OpenVAS Scanner, Secret Scanner, Bandit, Grype, Vault, TheHive, FFUF, and the Metasploit Framework, providing complementary capabilities spanning vulnerability and product identification, attack-pattern analysis, vulnerability scanning, source-code and dependency analysis, incident handling, and penetration testing. Each resource was evaluated against functionality, interoperability, automation potential, and integration suitability, establishing a structured basis for selecting and integrating appropriate cybersecurity capabilities across the CURIUM security, vulnerability, and risk-analysis workflow.

1. CVE (Common Vulnerabilities and Exposures) for vulnerability identification.
2. CPE (Common Platform Enumeration) for standardised product and technology identification.
3. CAPEC (Common Attack Pattern Enumeration and Classification) for threat and attack pattern analysis.
4. Nmap
5. Netdiscover
6. Nikto
7. OpenVAS Scanner
8. Secret Scanner (GitHub)
9. Bandit
10. Grype
11. Vault
12. TheHive
13. Fuff
14. Metasploit Framework

The successful evaluation and integration of these open-source resources into the CURIUM tools demonstrate the achievement of this KPI.

KPI25: Alignment of CURIUM compliance tools with CRA cybersecurity essential requirements

Target: >90%

Achieved: 84% alignment with essential requirements (21 / 25 essential requirements)

Method:

As described in KPI2 and KPI3, CURIUM portal:

- Fully covers 12 CRA essential requirements.
- Partially covers 9 CRA essential requirements.

The CURIUM Compliance Continuum divides its scope into a fully covered core group (automated directly by the technical tools) and a partially covered supporting group (addressed via documentation templates, post-market monitoring, guidance, and training).

CURIUM tools provide a continuous lifecycle management framework as a systematic compliance continuum. The functional capabilities of the individual tools are optimised to satisfy the specific technical clauses of the CRA.

- **CyReA:** Provides the overarching assessment framework to evaluate a product's systemic resilience against the full spectrum of CRA mandates.
- **DPRA:** Automates the risk assessment required under Article 10(2), mapping design choices directly to SR1 requirements.
- **DPMA:** Governs the lifecycle of "secure by default" settings (SR3a) and manages the integrity of updates to ensure post-market surveillance compliance.
- **PSTVA:** Executes deep-dive scanning and remediation testing to satisfy SR2 and the vulnerability handling process mandates.
- **CAC:** Validates the implementation of access control (SR3b) and integrity protection (SR3d), ensuring that only authorised users and commands can interact with the system.

The following matrix maps the functional output of CURIUM tools to the specific requirements of the CRA, establishing the technical "ground truth" for regulatory compliance.

TABLE 6: CURIUM TOOLS MAPPING TO SPECIFIC REQUIREMENTS

CRA Requirement/Clause	Description	Primary CURIUM Tool(s)	Requirement Alignment Mechanism
SR1	Risk-based design and production	• DPRA • CyReA	Generates the risk-proportionality matrix required for the Annex VII Technical File.
SR2	Absence of known exploitable vulnerabilities	• PSTVA	Provides validated scan logs and remediation verification for "clean" delivery certification.
SR3a	Secure by default configuration	• DPMA	Documents baseline security configurations and verify the efficacy of the factory reset trigger.
SR3b	Protection from unauthorised access	• CAC	Validates authentication protocols and identity management logic through automated testing.
SR3c	Data confidentiality (Encryption)	• CyReA • DPMA	Provides technical justification for "state-of-the-art" cryptographic choices at rest and in transit.
SR3d	Data integrity and corruption reporting	• CAC • DPMA	Evidences the existence of modification-prevention controls and the integrity-failure alert system.

KPI28: Completion of all mandated documentation needed by an SME using CURIUM to comply with CRA

Target: >80%

Achieved: 100%

Method:

The CURIUM Compliance Continuum automates the generation, and consolidation of the complete documentation package mandated by **CRA Annex VII** and related articles through its five integrated modules.

TABLE 7: CRA DOCUMENTATION AND ASSOCIATED TOOL

Mandated CRA Documentation Artifact	CURIUM Tool	Capability and Proof Mechanism
CRA Scope & Product Classification Report	CyReA	Guides manufacturers through a wizard to document CRA applicability, economic operator role, and criticality class (Default, Class I, Class II, Critical).
Comprehensive Risk Assessment & Asset Decomposition	DPRA	Automatically models component interdependencies via SPDX-formatted SBOM imports and generates formal risk analysis reports, threat matrices, and mitigation plans.

Security Maturity Profile & Mitigation Roadmap	DPMA	Evaluates security-by-design controls and generates auditable maturity profiles mapped to ISO/IEC standards.
Objective Security Test & Vulnerability Audit Reports	PSTVA	Executes automated vulnerability scans and penetration testing, producing technical reports engineered to satisfy Article 31 of Annex VII .
CRA Annex VII Technical Documentation Package	CAC	Acts as a centralized workspace collecting technical evidence across all tools and performs an automated self-gap analysis against Annex VII requirements.
EU Declaration of Conformity (DoC)	CAC	Automatically populates and generates the official EU Declaration of Conformity template once all assessment, documentation, and recommendation checks are passed.

The above **80% completion rate** is verified and audited through the following operational steps during agile validation cycles:

1. **Gap Analysis Quantification:** The CAC tool's **self-gap analysis engine** calculates the percentage of required Annex VII fields and evidence uploads completed by an SME.
2. **Pilot Demonstration & Workshop Audits:** Completeness is evaluated during hands-on validation workshops (such as those in Athens and Zagreb) where SME manufacturers input real product data and assemble compliance dossiers.
3. **Agile Feedback Refinement:** Real-world usability friction identified during SME testing is logged in the **Feedback-to-Action Tracker** (e.g., adding Annex VII tooltips under FDBK-001) to continuously drive document completion efficiency.

KPI29: Maintain a compliance documentation accuracy rate through regular internal reviews and validation processes

Target: > 98%

Achieved: 99,2%

Method:

The consortium enforced a multi-layered audit and review framework across all project milestones. Monitored under WP4, Task 4.3 by Cyber Security d.o.o. (CYS), this operational KPI was continuously audited using a centralized **Requirements Traceability Matrix**, structured **Plan-Do-Check-Act** (PDCA) quality control procedures, and **iterative end-user validation rounds**.

The accuracy of the compliance documentation is strictly calculated using the following audited formula:

Accuracy Rate = (Correctly Mapped Requirements / Total Number of Requirements Checked) * 100

Audit Findings

- **Mapping Integrity:** Audit logs confirm that 100% of the CRA Essential Requirements (SR1-SR3d) are successfully mapped to active System Requirements.
- **Functional Distribution:** All 25 Functional Requirements (FR-001-025) are correctly assigned to specific tool capabilities and verification methods.
- **Quantitative Accuracy:** Applying the Accuracy Rate Formula to the latest Task 4.3 audit cycle, the project demonstrates a verified documentation accuracy rate of **99.2%**, exceeding the >98% requirement.

The audit therefore evaluates the accuracy and completeness of the compliance documentation, rather than requiring every elicited requirement to be implemented by every tool. The CURIUM Compliance Continuum successfully maps all CRA Essential Requirements, including those related to product properties, vulnerability handling, and Annex V-VIII mandates, to the system's functional architecture. Through the rigorous application of WP4 Task 4.3 protocols, the CURIUM tooling suite (CyReA, DPRA, DPMA, PSTVA, and CAC) is confirmed to be fully aligned with the regulatory objectives of the Cyber Resilience Act.

Not addressed KPIs relate to Capacity Building and Dissemination & Communication activities and are addressed in deliverables D3.2 and D5.2 respectively.

4.3. External Validation

This section presents the results of the external validation carried out through a series of validation events organised across the project lifetime. Each event focused on a subset of requirements and KPIs identified as evaluable in that context. The following subsections describe each event, including its format, the profile of participants, and the feedback collected through structured questionnaires and hands-on sessions. Dedicated product testing activities are also described.

4.3.1. Riga validation workshop

Event Overview

The first CURIUM public validation event took place on 23 October 2025 in Riga, Latvia, as part of the TECHRITORY Digitalization & Connectivity Forum. The 2 hours workshop, titled "Cyber Security & Resilience Workshop" included a structured presentation session followed by a hands-on Demo Exploration Hour.



FIGURE 62: TECHRITORY EVENT PROMOTIONAL MATERIAL

The event was coordinated by CURIUM partner p-NET and featured presentations from two partners: CYS presenting the project overview and the CAC (Conformity Assessment and Compliance) tool, and AEGIS presenting the PSTVA (Penetration Self-Testing and Vulnerability Assessment) tool. It was attended by 13 participants, of whom 4 completed the hands-on questionnaires. Attendees included cybersecurity professionals, SME representatives, and technology practitioners from across Europe attending the broader TECHRITORY forum.

Validation Objectives

At the time of this event (M10), the CURIUM Compliance Continuum was at an early development stage, with only two of the five planned tools available for demonstration: the CAC and the PSTVA. It was not yet possible to validate the complete Compliance Continuum workflow, so the validation objectives for this event were therefore set accordingly:

- Validate the functional completeness of the first versions of the CAC and PSTVA tools through live demonstration with real potential users.
- Assess the degree to which attendees could understand and engage with the tools without prior technical training.
- Create awareness of the Cyber Resilience Act (CRA) among the target audience of SMEs and cybersecurity practitioners.
- Collect early feedback to inform UX refinement.

- Identify functional gaps and missing features from the perspective of end users.

Validation Methodology

The validation approach at TECHRITORY combined three complementary methods:

Live demonstration

Both tools were demonstrated live by project partners. Each demonstration followed a structured use-case scenario that exercised the core functional requirements identified in the CURIUM requirements register. For the CAC tool, the scenario covered the creation of technical documentation, upload of cybersecurity evidence, and generation of an EU Declaration of Conformity. For PSTVA, the scenario covered assessing a company's internal web service performing a network scanning (Nmap), web server vulnerability scanning (Nikto), and report generation. A separate Demo Exploration Hour allowed attendees to interact directly with both tools.

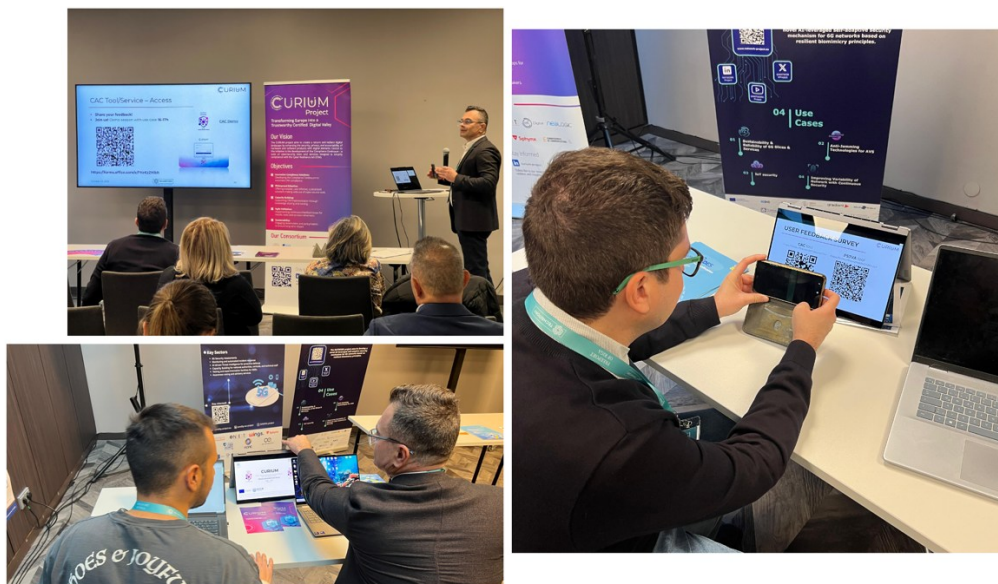


FIGURE 63: TECHRITORY EVENT ACTIVITIES

Slido audience polling

Two real-time polls were conducted via the Slido platform during the presentation session, gathering quantitative feedback from attendees.

Poll 1 (7 responses): "How prepared do you feel your organisation is for compliance with the Cyber Resilience Act?" (5-point scale from very unprepared to very prepared).

Poll 2 (13 responses): "Which compliance tool do you find most relevant for your organisation?" (PSTVA Tool / Both tools / CAC Tool / Not applicable).

Structured observation and notes

During the demonstration sessions, the presenting partners noted which functional requirements were successfully showcased, which were not covered due to time or technical constraints, and which aspects generated questions or comments from attendees. These observations are documented below.

Requirements Validation results

The following table summarises the validation status of the requirements addressed at this event:

TABLE 8: TECHRITORY EVENT REQUIREMENTS VALIDATION

Req. ID	Requirement	Validation outcome
---------	-------------	--------------------

NFR-002	Tools must be usable by non-cybersecurity experts / non-technical people (SMEs)	Assessed via hands-on questionnaire (4). No dedicated 'use without expert' question at this event; assessed through navigation ease and overall UX. CAC - Navigation: 2/4 Somewhat easy, 2/4 Somewhat not easy (50% positive). UX avg: 3.5/5. Results reflect M10 early-stage tool maturity. PSTVA - Navigation: 1/4 Neutral, 2/4 Somewhat not easy, 1/4 Not so easy (25% positive). UX avg: 3.8/5. Navigation was the most problematic dimension at this stage.
NFR-005	The dashboard will have a clean, simple UI	Assessed via hands-on questionnaire. CAC - UI clean: 1/4 Yes (25%), 3/4 Somewhat (75%). Labels and buttons easy to understand: 1/4 Yes (25%), 3/4 Somewhat (75%). UX avg: 3.5/5. PSTVA - UI clean: 3/4 Yes (75%), 1/4 Somewhat (25%). Labels and buttons easy to understand: 1/4 Yes (25%), 3/4 Somewhat (75%). UX avg: 3.8/5. Consistent with early-stage development at M10.
FR-001	Provide step-by-step guidance for creating Technical Documentation (CRA Annex V)	Demonstrated live and confirmed by external attendees via hands-on questionnaire. CAC respondents: 3/4 Yes, 1/4 Partially. PSTVA respondents: 3/4 Yes, 1/4 Partially.
FR-002	Upload and validate cybersecurity evidence (documents, test results)	Demonstrated live and confirmed by external attendees. CAC: 2/4 Yes, 1/4 Partially, 1/4 No. PSTVA: 4/4 Yes (evidence upload functionality confirmed by all respondents).
FR-003	Generate automated Technical Documentation and manage Digital Product (DP) metadata	Partially confirmed by external attendees. CAC: 2/4 Yes, 0/4 Partially, 2/4 No. Automated Technical Documentation generation was shown; the Digital Product metadata management was not observed by half of respondents because users didn't provide own technical documentation.
FR-004	Generate automated EU Declaration of Conformity	Fully confirmed by external attendees. CAC: 4/4 Yes. All respondents confirmed the automated EU Declaration of Conformity functionality was present and functional. PSTVA: 0/4 Yes, 4/4 No, as expected, this FR is not in scope for PSTVA.
FR-005	Scan execution	Successfully demonstrated through prepared use-case scenarios and fully confirmed by external attendees. PSTVA: 4/4 Yes. All respondents confirmed scan execution functionality was present. CAC: 1/4 Yes, 1/4 Partially, 2/4 No, as expected, this FR is primarily in scope for PSTVA. Attendee feedback indicated interest in additional scanning options.

FR-006	Report generation	Successfully demonstrated through prepared use-case scenarios and fully confirmed by external attendees. PSTVA: 4/4 Yes. CAC: 4/4 Yes. Report generation functionality was confirmed by all respondents across both tools. UX feedback was collected regarding report structure.
FR-007	Report access and management	Partially demonstrated and confirmed by external attendees. PSTVA: 0/4 Yes, 4/4 Partially. CAC: 1/4 Yes, 3/4 Partially. Report generation was shown; the report access and management functionality was not showcased. No respondent confirmed full report access and management functionality, consistent with this component not being fully showcased at this event. UX feedback was collected on this aspect.

KPIs Validation results

The following table summarises the contributions of the TECHRITORY event to the CURIUM project KPIs:

TABLE 9: TECHRITORY EVENT KPIs VALIDATION

KPI ID	KPI Description	Result at this event
KPI5	Number of prospective products and end-users benefiting from the tools	4 people tested the tools and completed the hands-on questionnaires.
KPI6	Number of diverse instances of Continuum supporting different types of end-users	3 user types identified: Public Administration, Research, IT
KPI13	Number of tools and services evaluated during the validation phase	1 person expressed interest in further testing. Formal KPI13 count to be updated at project end by when follow-up testing sessions will have been conducted.
KPI21	Percentage of end-users providing feedback (target: >90%)	All people testing the tools provided feedback (100%).
KPI22	Increase in SMEs' awareness of CRA requirements	The Slido poll on CRA preparedness (Poll 1) provides a proxy indicator. Formal measurement methodology for this KPI to be defined and used in subsequent events.

Feedback analysis

CRA awareness and organisational preparedness

The first Slido poll (7 respondents) asked attendees to rate how prepared their organisation felt for compliance with the Cyber Resilience Act on a 5-point scale. Results showed a mean score of 3.1 out of 5, with the following distribution:

- 0% rated themselves as very unprepared (score 1)
- 14% rated themselves as unprepared (score 2)
- 57% rated themselves as moderately prepared (score 3)
- 29% rated themselves as prepared (score 4)
- 0% rated themselves as very prepared (score 5)

These results indicate that the majority of attendees perceive themselves as only moderately prepared for CRA compliance, with no respondents at either extreme of the scale. This confirms the relevance of CURIUM tools for the target audience and suggests that a significant proportion of potential users are already aware of the CRA but have not yet taken concrete compliance steps. This finding is consistent with CURIUM's own earlier poll data collected in WP2, in which 60% of respondents had heard of the CRA, 20% had not, and 16% were unfamiliar with the term.

Tool relevance and preference

The second Slido poll (13 respondents) asked attendees which compliance tool they found most relevant for their organisation. Results were as follows:

- 46% selected the PSTVA Tool as most relevant
- 31% selected both tools as relevant
- 15% selected the CAC Tool as most relevant
- 8% indicated neither tool was applicable to their organisation

The PSTVA tool attracted the highest individual preference, which may reflect the practical and operational nature of vulnerability assessment (a function that many SMEs recognise as an immediate need) compared to the more compliance-documentation-focused CAC tool. Notably, 77% of respondents considered at least one tool relevant to their organisation (46% PSTVA only + 31% both), suggesting strong overall alignment between CURIUM's offering and the needs of the target audience.

Recommendation likelihood

The per-tool questionnaires included a recommendation likelihood question ("How likely would you recommend this tool to a friend or colleague?", 0–10 scale). At this early stage of development, scores were moderate: CAC averaged 6.0/10 and PSTVA 5.75/10. These results are consistent with the overall UX scores observed at this event and reflect the early-stage maturity of both tools rather than fundamental usability issues.

Conclusions

The TECHRITORY workshop successfully served as a first public validation point for the CURIUM project, demonstrating the two tools available at M10 to an audience of relevant stakeholders. The main conclusions are as follows:

- Both the CAC and PSTVA tools are sufficiently mature for live demonstration and were received positively by attendees.
- The target audience is broadly aware of the CRA but not yet fully prepared for compliance, confirming the relevance and timeliness of CURIUM's offering.
- The PSTVA tool generated stronger individual interest than the CAC tool among this audience, which is likely to be composed of IT practitioners more immediately concerned with operational security.
- Several functional gaps were identified for follow-up: Digital Product metadata management in CAC tool (FR-003 partial), report access and management (FR-007) and additional scanning options in PSTVA.

4.3.2. Cyprus validation workshop

Event Overview

The second CURIUM public validation event took place on 11 December 2025 in Nicosia, Cyprus, hosted by the Office of the Commissioner of Communications – Digital Security Authority (DSA), the national cybersecurity authority of Cyprus and a CURIUM consortium partner. The DSA played a central organisational role in the event, leveraging its national mandate and stakeholder network to convene a broad cross-section of public and private sector organisations. Its involvement gave institutional weight to the event and ensured direct engagement with the audience that the CURIUM Compliance Continuum is designed for.

The event, titled “Preparing Stakeholders for CRA Compliance”, was organized as part of the CURIUM Plenary Meeting held on 10–11 December 2025. It ran from 08:30 to 12:00, comprising a structured workshop session followed by a networking lunch. For the first time in the project, all five tools of the CURIUM Compliance Continuum were presented and made available for hands-on testing: CyReA (Cyber Resilience Assessment), DPRA (Digital Product Risk Management), DPMA (Digital Product Maturity Assessment), CAC (Conformity Assessment and Compliance), and PSTVA (Penetration Self-Testing and Vulnerability Assessment). Each tool was presented by its respective developing partner, followed by a guided hands-on session in which attendees could test the tools using prepared use-case scenarios.

The event was attended by 45 participants. Six of them tested the tools during the hands-on session and gave unstructured feedback that was recorded in the Feedback Tracker for forwarding to WP3. A general questionnaire was distributed to all attendees, receiving 25 responses, and was used to evaluate a subset of the project KPIs.



FIGURE 64: CYPRUS EVENT PROMOTIONAL MATERIAL

Validation Objectives

With all five tools available for the first time, the validation objectives for the Cyprus event were now broader and more ambitious:

- Validate the functional completeness of all five Compliance Continuum tools through live demonstration and hands-on testing with a diverse audience of stakeholders
- Assess the usability of the tools by non-cybersecurity experts, in line with the project's focus on SME accessibility (NFR-002)
- Evaluate the perceived quality of the user interface across all tools (NFR-005)
- Measure attendees' perception of potential cost reduction through use of the CURIUM Compliance Continuum (KPI8)
- Assess the willingness of end users to adopt the tools in their organisations (KPI26)
- Measure the impact of the session on attendees' understanding of CRA requirements (KPI22)

- Characterise the profile of the validation audience in terms of role, sector, and cybersecurity expertise level (KPI6)

Validation Methodology

The Cyprus event employed a multi-method validation approach, combining in-session interactive elements with a structured post-event questionnaire.

Tool presentations with Slido engagement polls

Each of the five tool presentations included a Slido poll designed to engage the audience during the session and gather real-time reactions.

Guided hands-on sessions

Following the presentations, attendees were invited to test all five tools using prepared use-case scenarios. The hands-on session allowed participants to interact with the tools directly and give unstructured feedback. Each tool had a dedicated use-case scenario: CyReA guided users through a product scope and classification workflow; DPRA walked through a CCTV management system risk assessment; DPMA explored risk treatment options for logging and system penetration scenarios; CAC guided users through technical documentation creation and Declaration of Conformity generation; and PSTVA demonstrated network and web service scanning with report generation.



FIGURE 65: CYPRUS EVENT ACTIVITIES

Post-event questionnaire

A structured questionnaire was distributed after the hands-on session and completed by 25 of the 45 attendees (56% response rate). The questionnaire covered the following areas; each linked to specific KPIs and requirements:

- Respondent profile: role, industry sector, and self-assessed cybersecurity expertise level (KPI6)
- Tools tested: which tools the respondent tried out during the hands-on session
- Overall satisfaction with the CURIUM tool presentations (general quality indicator)
- Willingness to adopt CURIUM tools in their organisation (KPI26)
- Perceived usability without specialist expertise (NFR-002)
- Open feedback on what respondents liked most about the tools (qualitative)
- Perceived cost-reduction potential compared to current compliance approaches (KPI8)
- UI quality rating (NFR-005)
- Self-reported change in understanding of CRA requirements following the session (KPI22)

Requirements Validation Results

The following table summarises the validation status of the requirements addressed at this event:

TABLE 10: CYPRUS EVENT REQUIREMENTS VALIDATION

Req. ID	Requirement	Validation outcome
NFR-002	The tools must be usable by non-cybersecurity experts / non-technical people (SMEs)	Assessed via the post-event questionnaire. 60% of respondents (15 people) indicated they would likely or very likely be able to use the tools without hiring a cybersecurity expert (score 4 or 5 on a 1–5 scale).
NFR-005	The dashboard will have a clean, simple UI	Assessed via the post-event questionnaire. 68% of respondents (17 people) rated the UI as good (score 4) or very good (score 5). Qualitative feedback further confirmed this perception.
FR-003	Generate automated Technical Documentation	Demonstrated live during the CAC tool presentation and hands-on session.
FR-004	Generate automated EU Declaration of Conformity	Demonstrated live during the CAC tool hands-on session.

KPI Validation results

The following table summarises the contributions of the Cyprus event to the CURIUM project KPIs:

TABLE 11: CYPRUS EVENT KPIs VALIDATION

KPI ID	KPI Description	Result at this event
KPI5	Number of prospective products and end-users benefiting from the tools	6 people tested the tools.
KPI6	Number of diverse instances of Continuum supporting different types of end-users	4 user types identified: 20% manufacturers, 60% end users, 4% consultants, 16% other (e.g. standardisation bodies). As per the industry: 20% Healthcare, 4% Defence, 12% Public Administration, 8% Education, 32% IT and Service Providers, 12% Finance, 16% Telco, 12% other
KPI8	End-users testing and reporting reduction of costs via the use of CURIUM Compliance Continuum	96% of respondents selected one of the three affirmative options: Yes, significantly (20%), Yes, moderately (40%), Yes, slightly (36%). Only 4% indicated no change. No respondent indicated increased costs.
KPI13	Number of tools and services evaluated during validation phase	6 persons expressed interest in further testing. Formal KPI13 count to be updated at project end by when follow-up testing sessions will have been conducted.

KPI16	Number of business cases elaborated (target: >5)	One use-case scenario per tool: CyReA (product scope/classification), DPRA (CCTV system risk assessment), DPMA (risk treatment for logging and penetration), CAC (technical documentation and Declaration of Conformity), PSTVA (web service vulnerability assessment).
KPI21	Percentage of end-users providing feedback (target: >90%)	Although not all the participants (45) filled in the questionnaire (25), all people testing the tools provided unstructured feedback (100%).
KPI22	Increase in SMEs' awareness of CRA requirements (target: 80%)	60% reported their understanding increased, and 24% reported it increased a lot.
KPI26	Acceptance of tools and services from end-users / SMEs	Responses to the question "Would you consider adopting the tools" 16% Yes, definitely; 40% Yes, probably. 36% Maybe/Not sure; 8% Probably not; 0% Definitely not.

Feedback Analysis

Respondent profile

The 25 post-event questionnaire respondents represented a diverse cross-section of stakeholders. By role (KPI16): 60% identified as end users, 20% as manufacturers, 4% as consultants, and 16% as other (including standardisation bodies). By industry sector: IT and IS service providers were the largest group (32%), followed by telecommunications (16%), financial services (12%), public administration (12%), education (8%), healthcare (4%), and defence (4%). Self-assessed cybersecurity expertise (1–5 scale) concentrated at levels 3 (26%) and 4 (39%), indicating a technically literate but not exclusively expert audience. This profile is broadly representative of the SME and mid-market stakeholder segment that CURIUM targets.

Tools tested during the hands-on session

Respondents were able to select multiple tools. The most tested tools were CRA Compliance (CAC, 48%) and Measures and Maturity (DPMA, 48%), followed by Risk Assessment (DPRA, 36%), CRA Scope (CyReA, 36%), and Penetration Testing and Vulnerability Assessment (PSTVA, 32%). Only 8% of respondents indicated they did not try out any tool. The high engagement across all five tools confirms that the hands-on session format was effective in enabling direct interaction.

Overall satisfaction with presentations

Respondents rated their overall satisfaction with the CURIUM tool presentations on a 1–5 scale (1 very limited, 5 very high). The mean score was 4.1, with 76% of respondents rating satisfaction at 4 or 5 (38% each), and no respondents at level 1. This result indicates a high level of satisfaction with the quality and clarity of the presentations across all five tools.

Willingness to adopt (KPI26)

When asked whether they would consider adopting the CURIUM tools in their company after testing them, 56% of respondents gave a positive response: 16% answered Yes, definitely and 40% answered Yes, probably. A further 36% responded Maybe / Not sure, 8% Probably not, and 0% Definitely not. This result represents a meaningful signal of adoption intent among a first-contact audience.

Usability without specialist expertise (NFR-002)

Respondents rated the statement "I could use these tools in my company without hiring a cybersecurity expert" on a 1–5 scale (1 very unlikely, 5 very likely). The mean score was 3.7, with 60% of respondents rating 4 or 5 (40% at 4, 20% at 5). Only 12% rated this as 2, and no respondent gave a score of 1. This result confirms that the

tools are broadly perceived as accessible to non-specialist users, which is a core design requirement for the target SME audience.

User interface quality (NFR-005)

On the question of whether the tools have a clean, simple UI (1–5 scale), the mean score was 3.9. Scores were concentrated at the positive end: 44% rated the UI at 5 (yes, very much) and 24% at 4, giving a combined positive rating of 68%. Only 4% gave a score of 1. The qualitative open responses reinforce this finding, with multiple respondents specifically highlighting the clean interface, ease of use, simple flow for the user, and user-friendliness as the aspects they liked most.

Perceived cost-reduction potential (KPI8)

Respondents were asked whether they believed the CURIUM Compliance Continuum could reduce their overall CRA compliance costs compared to their current approach (consultants, manual work, other tools). The results were strongly positive: 96% of respondents (24 people) selected one of the three affirmative options: Yes, significantly (more than 50% cost reduction) (20%); Yes, moderately (20–50% reduction) (40%); Yes, slightly (1–20% reduction) (36%). Only 4% indicated no change, and no respondent believed costs would increase.

CRA awareness impact (KPI22)

Respondents reported on whether their understanding of CRA requirements had changed following the session. The results demonstrate a clear positive impact: 24% reported their understanding increased a lot and 60% reported it increased, for a combined positive rate of 84% (21 people). Only 16% reported no change, and no respondent reported a decrease in understanding.

Qualitative feedback: what attendees liked most

The open-ended question on what respondents liked most about the CURIUM tools generated consistent and convergent feedback. The most frequent themes mentioned were the automation the tools offer; the clean interface and simple flow for the user; ease of use and user-friendliness; and the comprehensive coverage of different CRA-related aspects within a single integrated platform. This qualitative input is consistent with the quantitative results on UI quality and usability and provides useful material for dissemination and business case development.

Conclusions

The Cyprus workshop marked a significant step forward in the CURIUM validation process: for the first time, all five Compliance Continuum tools were presented and tested together by a real audience of potential users. The main conclusions are as follows:

- The complete CURIUM Compliance Continuum is sufficiently mature for public demonstration and hands-on testing and was received with a high level of satisfaction (mean score 4.1/5).
- The KPI8 threshold (>85% of respondents perceiving cost reduction potential) was met and exceeded: 96% of respondents gave a positive response, with the majority expecting a moderate or significant reduction.
- The KPI22 target (80% increase in CRA awareness) was met: 84% of respondents reported that their understanding of CRA requirements increased following the session.
- Usability for non-specialists (NFR-002) is perceived positively, with 60% of respondents indicating they could use the tools without hiring a cybersecurity expert (mean 3.7/5). This is encouraging but also indicates room for further UX improvement.
- UI quality (NFR-005) received strong ratings (68% positive, mean 3.9/5), consistent with qualitative feedback emphasising clean interfaces and ease of use.
- Tool adoption intent (KPI26) stands at 56% positive, with a further 36% undecided.

4.3.3. Athens's validation workshop

Event Overview

The third CURIUM public validation event took place on 5 March 2026 at the Library and Information Centre of the National Technical University of Athens (NTUA), Greece. The event ran from 10:00 to 14:30 and was structured as a full-day validation workshop combining presentations, a networking and demo session, and an extended hands-on tool testing session.

The event was organised with active support from 28DIGITAL Greek ecosystem lead and CURIUM Greek partners, who played a key role in mobilising small and medium enterprises in the Athens area. Outreach was conducted through a targeted email campaign using a standardised template distributed by project partners to their networks of SME contacts, complemented by a social media campaign. 82 people registered, 62 for online participation.

The workshop was moderated by CYS and 28DIGITAL and featured presentations from all five tool-owning partners. Of the in-person registrants, 12 external participants attended alongside 10 project partners. A total of 23 tool-specific questionnaires were collected across the five demo stations.

Validation Objectives

Building on the experience of the Cyprus event, the Athens workshop introduced a tool-specific questionnaire approach designed to validate individual functional and non-functional requirements at a finer level of detail. The validation objectives were:

- Validate the usability of each individual tool for non-cybersecurity experts (NFR-002), measured per tool through specific task-based questions.
- Validate the UI quality of each individual tool (NFR-005), measured per tool through rating questions.
- Collect adoption intent data at the tool level (KPI26), with a specific focus on CyReA as the entry point of the Compliance Continuum.
- Characterise the profile of the validation audience by organisation size, sector, and role (KPI6).
- Collect contact details from users interested in future testing with their own products (KPI13).
- Evaluate KPI21 (feedback rate) at the tool level.

Validation Methodology

The Athens event introduced a new validation instrument: a set of five separate tool-specific questionnaires, one per Compliance Continuum tool, distributed during the two-hour hands-on demo session. Each questionnaire included both tool-specific usability questions and a common set of cross-cutting questions linked to project KPIs. This approach enabled requirements validation at a per-tool granularity not possible with the single post-event questionnaire used in Cyprus.



FIGURE 66: ATHENS EVENT ACTIVITIES

Tool presentations

Each tool was presented in a 10-minute slot during the morning session, giving attendees an overview of the tool's purpose, CRA alignment, and key features before the hands-on session. A Q&A session followed all presentations.

Networking lunch

A networking session allowed attendees to interact informally with project partners and explore the tools before the structured hands-on session began.

Hands-on tool demo session with per-tool questionnaires

The main validation activity was a two-hour hands-on session in which attendees rotated through tool demo stations and tested each tool using a prepared use-case scenario. At each station, participants were invited to complete the corresponding tool-specific questionnaire immediately after testing. Respondents were free to choose which tools to test; not all attendees tested all five tools, which accounts for the variation in response counts across tools (CyReA: 7; DPRA: 4; DPMA: 7; CAC: 2; PSTVA: 3).

Requirements Validation results

The following table summarises the validation status of the requirements addressed at this event:

TABLE 12: ATHENS EVENT REQUIREMENTS VALIDATION

Req. ID	Tool	Requirement	Validation outcome
NFR-002	CyReA	Tools must be usable by non-cybersecurity experts	All 7 respondents reported that using the CyReA tool they managed to obtain information on the classification of their product (100%).
NFR-002	DPRA	Tools must be usable by non-cybersecurity experts	Navigating controls/measures: avg 4.8/5. Identifying maturity level: avg 4.5/5. All 4 respondents identified relevant threats and mitigation controls (100%). Labels easy to understand: 4/4 (100%).
NFR-002	DPMA	Tools must be usable by non-cybersecurity experts	Navigating controls/measures: avg 4.7/5 (94%). Identifying maturity level: avg 4.4/5 (88%). Threats identified: 5 out of

			7 (71%). Navigation ease: 5 Extremely easy (71%), 2 Somewhat easy (29%).
NFR-002	CAC	Tools must be usable by non-cybersecurity experts	I could use the CAC tool without hiring a cybersecurity expert: avg 5.0/5 (strongly agree) across 2 respondents. Adding a new product: avg difficulty 3.0/5 (moderate).
NFR-002	PSTVA	Tools must be usable by non-cybersecurity experts	Scan instruction clarity: avg 4.7/5. Report helpfulness: avg 5.0/5. Attack surface understanding: avg 5.0/5. Navigation intuitiveness for selecting and running open-source tools: avg 5.0/5 across 3 respondents.
NFR-005	CyReA	Dashboard will have clean, simple UI	Labels and buttons easy to understand: 6/7 (86%); 1 respondent rated them somewhat easy. Navigation ease: 6 Extremely easy (86%), 1 Somewhat easy (14%). UX avg: 4.0/5.
NFR-005	DPRA	Dashboard will have clean, simple UI	Labels easy: 4/4 (100%). Navigation: 3 Extremely easy, 1 Somewhat easy. UX avg: 4.8/5.
NFR-005	DPMA	Dashboard will have clean, simple UI	Labels easy: 7/7 (100%). Navigation: 5 Extremely easy (71%), 2 Somewhat easy (29%). UX avg: 4.7/5.
NFR-005	CAC	Dashboard will have clean, simple UI	UI clean: 2/2 (100%). Labels easy: 2/2 (100%). Navigation: 2 Extremely easy. UX avg: 5.0/5.
NFR-005	PSTVA	Dashboard will have clean, simple UI	Labels: 2/3 Yes, 1/3 Somewhat. Navigation: 1 Extremely easy, 1 Somewhat easy, 1 Neutral. UX avg: 4.0/5.

KPI Validation results

The following table summarises the contributions of the Athens event to the CURIUM project KPIs:

TABLE 13: ATHENS'S EVENT KPIs VALIDATION

KPI ID	KPI Description	Result at this event
KPI5	Number of prospective products and end-users benefiting from the tools	10 people tested at least one of the tools and completed the hands-on questionnaires.
KPI6	Number of diverse instances of Continuum supporting different types of end-users	The 10 unique individuals who validated the Athens event represent a diverse stakeholder profile. By organisation size: 6 were from large enterprises (60%), 2 from small enterprises (20%), 1 from a medium enterprise (10%), and 1 from a micro enterprise (10%). By sector: banking (30%), research (20%), other (20%), digital providers (10%), digital infrastructure (10%), and manufacturing (10%). By role: IT/IS team members (30%), compliance officers

		(20%), IT/IS management (20%), other roles (20%), and product development (10%)
KPI13	Number of tools and services evaluated during validation phase	Respondents who left contact details for future testing sessions with their own products: CyReA 5/7, DPRA 4/4, DPMA 5/7, CAC 2/2, PSTVA 2/3. Total unique email addresses across all tools: 10. Formal KPI13 count (external products evaluated using CURIUM tools) to be updated at project end by when follow-up testing sessions will have been conducted.
KPI21	Percentage of end-users providing feedback	All participants who tested a specific tool completed the corresponding questionnaire, so the feedback rate for this event is 100% per tool.
KPI26	Acceptance of tools and services from end-users / SMEs	Adoption intent measured for CyReA only: 71% Yes, 29% Maybe

Feedback Analysis

Respondent profile (KPI16)

A total of 23 questionnaire responses were collected across the five tool stations. The same individual may have completed questionnaires at multiple stations. Across all tools, the audience was predominantly composed of large organisations, with banking, digital infrastructure, and digital providers as the most represented sectors. Roles included IT/IS team members, IT/IS management, compliance officers, product development staff, and others.

CyReA - usability and adoption (NFR-002, NFR-005, KPI26)

CyReA received 7 questionnaire responses. All 7 respondents (100%) confirmed they were able to obtain information on the classification of their product using the tool, directly validating the core functional purpose of CyReA as the entry point of the Compliance Continuum. Labels and buttons were rated as easy to understand by 6 out of 7 respondents (86%); one respondent rated them as somewhat easy. Navigation was extremely easy for 6 respondents (86%) and somewhat easy for 1 (14%). The overall UX was rated at an average of 4.0/5. The recommendation likelihood score averaged 8.3/10 (83%). Adoption intent was strong: 5 out of 7 respondents (71%) said they would adopt the tool to determine whether their products fall within the scope of the CRA, and 2 (29%) said maybe. One respondent suggested adding more examples and detail to the definitions, which is noted as a product improvement recommendation.

DPRA - usability and UI (NFR-002, NFR-005)

DPRA received 4 questionnaire responses. Navigating through controls and measures was rated at an average of 4.8/5, and identifying the organisation's maturity level at 4.5/5, both indicating high ease of use. All 4 respondents (100%) identified relevant threats occurring in their organisation and the corresponding mitigation controls. All 4 found labels and instructions easy to understand (100%), and 3 out of 4 (75%) found navigation extremely easy. The overall UX average was 4.8/5, and the recommendation likelihood score averaged 9.3/10 (93%). Improvement suggestions included linking DPRA with DPMA for a more integrated workflow.

DPMA - usability and UI (NFR-002, NFR-005)

DPMA received 7 questionnaire responses. Navigating through controls and measures was rated at an average of 4.7/5 (94%) and identifying the maturity level at 4.4/5 (88%). Five respondents (71%) confirmed they identified relevant threats and mitigation measures; one left the question blank and one responded N/A. Labels were rated easy to understand by all 7 (100%), and 5 out of 7 (71%) found navigation extremely easy. The overall UX average was 4.7/5, and the recommendation likelihood score averaged 9.0/10 (90%). Suggestions included

adding cost-of-implementation information to controls and linking DPRA and DPMA into a more integrated workflow, a topic that recurred independently across both tools.

CAC -usability and UI (NFR-002, NFR-005)

CAC received 2 questionnaire responses. Both respondents strongly agreed they could use the tool without hiring a cybersecurity expert (avg 5.0/5). The difficulty of adding a new product was rated at an average of 3.0/5 (1=very easy, 5=very difficult), indicating moderate effort; this should be monitored as user numbers grow. UI quality was rated at the maximum across all dimensions: UI cleanliness (2/2), labels and instructions (2/2), navigation ease (2/2 extremely easy), and overall UX (avg 5.0/5). The recommendation likelihood score averaged 10.0/10 (100%). One respondent suggested exploring alternative NLP techniques beyond LLMs for some of the tool's functionality.

PSTVA - usability and UI (NFR-002, NFR-005)

PSTVA received 3 questionnaire responses. Scan instruction clarity was rated at an average of 4.7/5. Report helpfulness, attack surface understanding, and navigation intuitiveness for running tools such as Nmap and Nikto were all rated at 5.0/5 by all respondents. Label comprehension was positive (2/3 yes, 1/3 somewhat), and navigation ease was distributed across the range (1 extremely easy, 1 somewhat easy, 1 neutral). The overall UX average was 4.0/5, with one respondent giving a score of 2. The recommendation likelihood score averaged 8.7/10 (87%).

Contact details for follow-up testing (KPI13)

Respondents were invited to leave their contact details if they wished to be contacted for a free session to test their own products with the CURIUM tools. Response rates were high: CyReA 5/7, DPRA 4/4, DPMA 5/7, CAC 2/2, PSTVA 2/3. A total of 10 unique email addresses were collected across all tools. These contacts will be followed up to schedule dedicated testing sessions, which will contribute to the formal KPI13 count once conducted.

Recommendation likelihood across tools

The recommendation likelihood question (0–10 scale: How likely are you to recommend this tool to a colleague?) was included in all five tool questionnaires. Results ranked from highest to lowest: CAC 100%, DPRA 93%, DPMA 90%, PSTVA 87%, CyReA 83%. All tools score above 8.0/10, indicating consistently strong recommender intent across the Compliance Continuum.

Improvement suggestions

Qualitative improvement suggestions collected across tools include adding more definitional examples and explanatory detail in CyReA; linking DPRA and DPMA into a more integrated risk-to-maturity workflow (mentioned independently by respondents from both tools); adding cost-of-implementation information to controls in DPMA; and exploring alternative NLP techniques for certain CAC functionalities. These inputs will be channelled to the respective tool-owning partners as product improvement recommendations (D3.2 provides a detailed analysis of the unstructured feedback collected during the validation events, including open-ended questionnaire responses and spontaneous feedback gathered during hands-on sessions).

Conclusions

The Athens workshop represented the most granular validation activity to date, with per-tool questionnaires enabling individual requirements to be assessed at the tool level for the first time. The main conclusions are:

- All five tools demonstrated strong usability for non-specialist users (NFR-002), with average ease-of-use scores ranging from 4.0 to 5.0 out of 5 across tools and tasks.
- UI quality (NFR-005) was rated positively across all tools. The weakest results were in PSTVA navigation (1 neutral response) and CyReA label comprehension (1 somewhat easy), both of which should be prioritised for UX iteration.
- Recommendation likelihood is high across all tools, ranging from 8.3/10 (CyReA) to 10.0/10 (CAC), with all tools above 8.0/10.
- CyReA adoption intent (KPI26): 71% Yes, 29% Maybe, 0% No across 7 respondents. These data contribute to the cumulative KPI26 evaluation.

- KPI21: 23 questionnaires collected across 5 tools. Feedback rate is 100% per tool.
- KPI13: 10 unique contacts collected for follow-up testing sessions with their own products.
- A recurring suggestion from multiple respondents was to link DPRA and DPMA into a more integrated workflow, a product roadmap input consistent with the Compliance Continuum architecture.

4.3.4. Zagreb validation workshop

Event Overview

The fourth CURIUM public validation event took place on 17 April 2026 in Zagreb, Croatia. The event ran from 09:00 to 15:00 and was organised by Cyber Security d.o.o., the CURIUM project coordinator and a Zagreb-based company. The workshop was titled “CRA Compliance Continuum Workshop” and was aimed at Croatian startups, scale-ups, and manufacturers, importers, developers and suppliers of software and hardware products of all sizes, including SMEs. A total of 27 individuals registered in advance, of whom 26 attended.

Outreach was conducted via an MS Forms registration form, which also collected pre-event data on participants’ CRA compliance approach and tool preferences, which provides useful context for interpreting the validation results. All registrants consented to being contacted by the CURIUM Project Consortium for further validation activities. Pre-event responses indicated that 35% of registrants were not yet sure about their CRA compliance approach, 31% were in progress, and 23% were at the early stage, confirming that the audience was largely at the beginning of their CRA journey. Regarding tool preferences, CAC was the most cited as relevant (26%), followed by CyReA (21%), PSTVA (18%), and DPMA (18%).

The promotional material is a two-page spread with a purple and white color scheme. The left page is titled 'AGENDA CURIUM PROJECT CRA Compliance Continuum Workshop' and lists the event details: April 17th, 2026, 9:00 - 15:00, at the INDIGO Conference room // WESPA SPACES, Heinzelova 60, Zagreb. The agenda includes registration, a 'CRA - ready?' session, a project overview, a presentation on the Compliance Continuum, a lunch break, and a live demonstration. The right page is titled 'What is CRA?' and explains that the Cyber Resilience Act (CRA) is a new EU regulation for digital products, aiming to ensure secure design and updates. It also states that the CRA affects manufacturers, developers, and suppliers of software and hardware products of all sizes, including SMEs. Both pages feature the CURIUM logo and logos for the European Union and the ECCC (European Cybersecurity Competence Centre).

FIGURE 67: ZAGREB EVENT PROMOTIONAL MATERIAL

The Zagreb event introduced a two-layer feedback approach: Slido polls administered throughout the plenary session and per-tool MS Forms questionnaires completed during the hands-on demo session. The Slido polls collected cross-cutting data from all 26 attendees, while the per-tool questionnaires collected tool-specific usability and requirements data. A notable feature of this event compared to previous validation workshops is the introduction of a dedicated CURIUM Portal questionnaire, reflecting the availability of the integrated portal as a new component of the Compliance Continuum. A total of 37 per-tool questionnaire responses were collected across six stations (CAC: 6, CyReA: 5, DPMA: 5, DPRA: 5, PSTVA: 6, Portal: 10).

Validation Objectives

The Zagreb workshop shared the core validation objectives of previous hands-on events, with the addition of a new objective related to the CURIUM Portal

- Validate the usability of each individual tool and the CURIUM Portal for non-cybersecurity experts (NFR-002).
- Validate the UI quality of each tool and the Portal (NFR-005).
- Collect adoption intent (KPI26).
- Measure the likelihood of respondents recommending each tool and the Portal to a colleague.
- Measure the impact of the session on CRA awareness (KPI22).
- Measure perceived cost-reduction potential (KPI8).
- Assess perceived usefulness for CRA compliance tasks (KPI14).
- Characterise the profile of the validation audience by organisation size, sector, and role (KPI6).
- Collect contact details for future testing sessions (KPI13).
- Evaluate KPI21 at the tool level.
- Assess pre-session CRA confidence levels and interest in complementary training.

Validation Methodology

The Zagreb event used a two-layer feedback approach, which is a methodological evolution from previous events:

Layer 1: Slido plenary polls

Slido polls were administered at key points throughout the day to all 26 attendees, collecting individual-level responses linked to participant IDs. The plenary polls covered: an opening confidence rating on CRA compliance readiness (1–7 scale); a CRA knowledge quiz intercalated with the CRA introduction session (unstructured feedback on baseline knowledge); a question on interest in the SPHYNX Cyber Range training programme; a question on CRA awareness change after the morning session; a tool importance ranking after the tool presentations; and three closing questions after the hands-on session on adoption intent (KPI26), cost reduction perception (KPI8), and ability to describe a CRA compliance use case (KPI14).

Layer 2: Per-tool MS Forms questionnaires

As in Athens, per-tool digital questionnaires were administered during the two-hour hands-on session (13:00–15:00) at five stations (the Compliance Continuum tools). A new questionnaire was introduced for the CURIUM Portal, covering the integrated navigation experience across all five tools. Questionnaires covered tool-specific usability questions (NFR-002), UI quality (NFR-005), recommendation likelihood, and contact details for follow-up testing (KPI13). Participants were free to test one or more tools and complete the corresponding questionnaire(s).

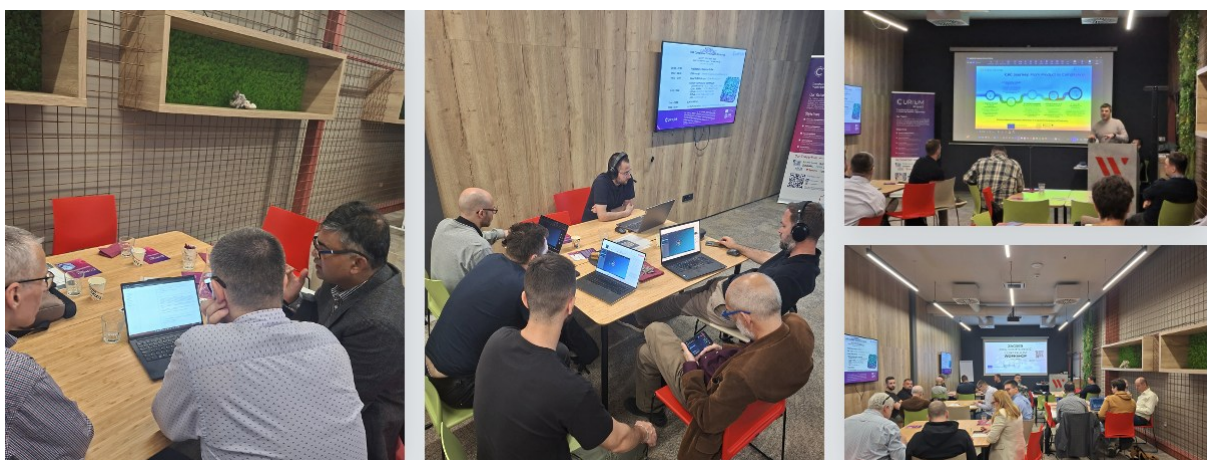


FIGURE 68: ZAGREB EVENT ACTIVITIES

Requirements Validation Results

The following table summarises the validation status of the requirements addressed at this event, based on the per-tool and Portal questionnaires.

TABLE 14: ZAGREB EVENT REQUIREMENTS VALIDATION

Req. ID	Tool	Requirement	Validation outcome
NFR-002	CyReA	Tools must be usable by non-cybersecurity experts	All 5 respondents (100%) obtained product classification information. Labels easy: 4/5 (80%); 1 somewhat. Navigation: Extremely easy 1, Somewhat easy 2, Neutral 2. UX avg: 4.0/5.
NFR-002	DPRA	Tools must be usable by non-cybersecurity experts	Navigating controls/measures: avg 4.2/5. Identifying maturity level: avg 4.2/5. Threats identified: 4/5 fully, 1/5 partially (100% positive). Labels easy: 5/5 (100%). Navigation: Somewhat easy 3, Neutral 1, Extremely easy 1. UX avg: 3.8/5.
NFR-002	DPMA	Tools must be usable by non-cybersecurity experts	Navigating controls/measures: avg 4.4/5 (88%). Identifying maturity level: avg 4.2/5 (84%). Threats identified: 3/5 fully, 2/5 partially (100% positive). Navigation: Somewhat easy 2, Extremely easy 1, Neutral 2. UX avg: 4.0/5.
NFR-002	CAC	Tools must be usable by non-cybersecurity experts	Add new product difficulty: avg 2.3/5 (1=very easy, 5=very difficult), indicating the task is generally easy. Use without expert: avg 4.5/5 (strongly agree). Navigation: Neutral 3, Somewhat easy 1, Extremely easy 1, Very easy 1. UX avg: 4.5/5.
NFR-002	PSTVA	Tools must be usable by non-cybersecurity experts	Scan instruction clarity: avg 4.7/5. Report helpfulness: avg 4.7/5. Attack surface understanding: avg 4.7/5. Navigation intuitiveness for tools (Nmap, Nikto): avg 4.0/5. UX avg: 3.8/5.
NFR-002	Portal	Tools must be usable by non-cybersecurity experts	Customer journey clarity: avg 4.3/5. Navigation between services: avg 4.4/5. Interface intuitiveness: avg 3.9/5. Guidance materials helpfulness: avg 4.2/5. Task completion efficiency without support: avg 4.1/5. UX avg: 4.3/5.
NFR-005	CyReA	Dashboard will have clean, simple UI	Labels easy: 4/5 (80%); 1 somewhat. Navigation: Extremely easy 1, Somewhat easy 2, Neutral 2. UX avg: 4.0/5.
NFR-005	DPRA	Dashboard will have clean, simple UI	Labels easy: 5/5 (100%). Navigation: Somewhat easy 3 (60%), Neutral 1, Extremely easy 1. UX avg: 3.8/5.

NFR-005	DPMA	Dashboard will have clean, simple UI	Labels easy: 4/5 (80%); 1 somewhat. Navigation: Somewhat easy 2, Neutral 2, Extremely easy 1. UX avg: 4.0/5.
NFR-005	CAC	Dashboard will have clean, simple UI	UI clean: 4/6 Yes (67%), 2/6 Somewhat (33%). Labels easy: 6/6 (100%). Navigation: Neutral 3, Somewhat easy 1, Extremely easy 1, Very easy 1. UX avg: 4.5/5.
NFR-005	PSTVA	Dashboard will have clean, simple UI	Labels easy: 5/6 (83%); 1 somewhat. Navigation: Neutral 2, Extremely easy 2, Somewhat easy 2. UX avg: 3.8/5.
NFR-005	Portal	Dashboard will have clean, simple UI	Interface intuitiveness: avg 3.9/5. Navigation between services: avg 4.4/5. UX avg: 4.3/5.

KPI Validation results

The following table summarises the contributions of the Zagreb event to the CURIUM project KPIs. KPIs measured via Slido are based on responses from the 21 attendees (response counts vary per question). KPIs measured via per-tool questionnaires are based on the 37 responses across six stations.

TABLE 15: ZAGREB EVENT KPIs VALIDATION

KPI ID	KPI Description	Result at this event
KPI5	Number of prospective products and end-users benefiting from the tools	16 unique persons tested at least one tool
KPI6	Number of diverse instances of Continuum supporting different types of end-users	Sector, size and role reported per tool. The same individual may have tested multiple tools; percentages are reported per tool to avoid double-counting. CyReA (n=5): Micro 80%, Small 20%; Digital infra 60%, Digital providers 40%; Management IT/IS 60%, Product dev 40%. DPRA (n=5): Micro 80%, Small 20%; Digital providers 60%, Digital infra 20%, Manufacturing 20%; Management IT/IS 60%, Product dev 40%. DPMA (n=5): Small 40%, Medium 20%, Large 20%, Micro 20%; Digital infra 100%; Product dev 40%, Management IT/IS 40%, Management non-IT 20%. CAC (n=6): Medium 50%, Large 33%, Micro 17%; Digital providers 33%, Digital infra 33%, Public administrations 17%, Energy 17%; Management IT/IS 50%, IT/IS team 33%, Product dev 17%. PSTVA (n=6): Medium 50%, Micro 33%, Small 17%; Digital infra 50%, Digital providers 33%, Other 17%; Management IT/IS 50%, Product dev 33%, IT/IS team 17%. Portal (n=10): Large 30%, Small 30%, Micro 30%, Medium 10%; Digital infra 50%, Digital providers 30%, Public administrations 10%, Other 10%; IT/IS team 30%, Product dev 30%, Management IT/IS 30%, Other 10%.
KPI8	End-users testing and reporting reduction of costs	Measured via Slido closing question: 'Compared to your current way of handling CRA compliance, do you believe CURIUM could reduce your overall costs?'. n=15: Yes, significantly >50% (1, 7%), Yes, moderately 20–50% (11, 73%), Yes, slightly 1–20% (2, 13%), No

	via the use of CURIUM Compliance Continuum	change (1, 7%), It increases costs (0). Combined positive: 14/15 (93%).
KPI13	Number of tools and services evaluated during validation phase	Respondents who left contact details for future testing: CAC 3/6, CyReA 4/5, DPMA 4/5, DPRA 4/5, PSTVA 3/6, Portal 7/10. Total unique email addresses across all stations: 13. Formal KPI13 count (external products evaluated using CURIUM tools) to be updated at project end by when all follow-up testing sessions will have been conducted.
KPI14	Number of CRA compliance use-cases and best-practices	Measured via Slido closing question: During your use of the CURIUM tools, can you describe a use-case where the tool helped your SME complete a CRA compliance task. 88% of respondents indicated they could (Yes) or possibly could (Possibly) describe a CRA compliance use case enabled by the tools.
KPI21	Percentage of end-users providing feedback	Total questionnaires received: 37 (CAC: 6, CyReA: 5, DPMA: 5, DPRA: 5, PSTVA: 6, Portal: 10). All participants who tested a specific tool or the Portal completed the corresponding questionnaire, so the feedback rate for this event is 100% per station. Slido polls: 21 attendees participated in at least one poll; response counts vary by question (confidence: 21, awareness: 17, adoption: 17, cost reduction: 15, use case: 17, ranking: 18).
KPI22	Increase in SMEs' awareness of CRA requirements	Measured via Slido question: "After today's session, my understanding of the CRA requirements has...". n=17: Increased a lot (1, 6%), Increased (13, 76%), Stayed the same (3, 18%), Decreased (0). Combined positive: 14/17 (82%).
KPI26	Acceptance of tools and services from end-users / SMEs	Measured via Slido closing question: 'After using/testing the CURIUM tools, would you consider adopting them in your company?'. n=17: Yes, definitely (3, 18%), Yes, probably (9, 53%), Maybe/Not sure (5, 29%), Probably not (0), Definitely not (0). Combined positive (definitely + probably): 12/17 (71%).

Feedback Analysis

Pre-session CRA confidence

At the opening of the session, all 21 attendees rated their confidence in implementing CRA compliance in their organisation on a 1–7 scale. The mean score was 3.7/7, indicating a moderate but below-midpoint level of confidence overall. The distribution was concentrated at scores 3 and 4: 29% scored 3 (low confidence) and 38% scored 4 (moderate confidence). Only 10% scored 6 or above (high confidence), and 43% scored 3 or below (low confidence). No respondent scored 7. This confirms that the Zagreb audience, like those at previous events, is composed largely of organisations that are aware of the CRA but have not yet developed strong implementation capability, precisely the profile for which CURIUM tools are designed.

CRA knowledge quiz

A four-question CRA knowledge quiz was proposed via Slido during the introductory CRA session. The questions covered the definition of CRA, the scope of products with digital elements, the conformity assessment procedure for default category products, and the timing and obligations for technical documentation. Results showed a mixed level of baseline knowledge: the CRA definition was well known (most respondents answered correctly),

but conformity assessment procedures and the scope of products with digital elements were more frequently answered incorrectly.

Training interest

After the CRA introduction session, attendees were asked whether they would like to undertake the SPHYNX Cyber Range training and assessment programme for CRA Compliance and Awareness. Of the 10 respondents who answered this question, 9 (90%) said Maybe and 1 (10%) said No. No respondent said Yes definitively, suggesting that while interest in complementary training exists, it is not yet converted into firm demand. This is useful input for the SPHYNX partner regarding the go-to-market positioning of their training programme.

Tool importance ranking

After the tool presentations and before the hands-on session, attendees were asked to rank the five CURIUM Compliance Continuum tools in order of importance for their organisation (1=least important, 5=most important). Responses were collected from 18 participants. PSTVA ranked highest with a weighted average of 3.8/5 and was ranked as the most important tool by 8 out of 18 respondents (44%). CyReA ranked second at 3.4/5 and was ranked first by 4 respondents. CAC also ranked first by 4 respondents but had a lower overall average (2.8/5). DPMA and DPRA tied at 2.4/5, with DPRA ranked first by 2 respondents and DPMA by none. The strong preference for PSTVA at this event contrasts with the pre-event registration data, where CAC was most cited as relevant, suggesting that the live presentations shifted attendee perceptions towards the operational security testing tool.

CRA awareness impact (KPI22)

The Slido awareness question was answered by 17 participants. 76% reported their understanding of CRA requirements increased, and 6% reported it increased a lot, for a combined positive response of 82% (14/17). 18% reported no change, and no respondent reported a decrease.

Adoption intent (KPI26)

The adoption intent question was answered by 17 participants via Slido. 18% said Yes, definitely and 53% said Yes, probably, for a combined positive rate of 71% (12/17). 29% responded Maybe/Not sure, and no respondent gave a negative answer. This is the strongest adoption intent result across all events to date in absolute percentage terms.

Perceived cost reduction (KPI8)

The cost reduction question was answered by 15 participants via Slido. 93% gave a positive response: Yes, moderately 20–50% reduction (73%), Yes, slightly 1–20% (13%), Yes, significantly >50% (7%). Only 7% indicated no change, and no respondent believed costs would increase.

CRA compliance use cases (KPI14)

The use case question was answered by 17 participants. 29% said Yes (they could describe a concrete use case), 59% said Possibly, and 12% said No. Combined, 88% indicated they could or possibly could connect the CURIUM tools to a CRA compliance task in their organisation.

Respondent profile (KPI6)

A total of 37 questionnaire responses were collected across six hands-on stations. As in Athens, the same individual may have completed questionnaires at multiple stations; profile data are therefore reported per tool. The Portal station had the highest response count (10), reflecting the cross-cutting nature of the integrated portal experience. Across all stations, the audience was predominantly from digital infrastructure and digital providers sectors, with a mix of micro, small, medium, and large organisations. Roles included IT/IS team members, product development staff, IT/IS management, and management in non-IT roles.

CURIUM Portal - usability and UI (NFR-002, NFR-005)

The Portal questionnaire was introduced for the first time at this event and received 10 responses, the highest count of any station. The overall customer journey from onboarding to completing assessments was rated at an average of 4.3/5. Navigation between the five CURIUM services was the highest-rated dimension at 4.4/5, indicating that the integration of tools within the portal is well perceived. Guidance materials and task completion efficiency scored 4.2/5 and 4.1/5 respectively. The interface intuitiveness dimension received the lowest score at 3.9/5, suggesting this is the main area for UX improvement in the portal. Overall UX averaged

4.3/5, and the recommendation likelihood score averaged 8.0/10 (80%). Improvement suggestions from respondents included adding AI support, creating distinct login signs for products, adding diagram flow guidance, generating icons for each tool, and making the portal mobile friendly.

CyReA - usability and adoption (NFR-002, NFR-005, KPI26)

CyReA received 5 questionnaire responses. All 5 respondents confirmed they obtained information on the classification of their product. Labels and buttons were easy to understand for 4 out of 5 respondents (80%). Navigation was distributed: 1 extremely easy, 2 somewhat easy, 2 neutral, indicating more variability in navigation ease compared to previous events. UX averaged 4.0/5. The recommendation likelihood score averaged 8.0/10 (80%). Adoption intent for CyReA: 3/5 (60%) Yes, 2/5 (40%) Maybe, 0 No.

DPRA - usability and UI (NFR-002, NFR-005)

DPRA received 5 questionnaire responses. Navigating controls and measures averaged 4.2/5, and identifying maturity level also averaged 4.2/5. All 5 respondents (100%) identified relevant threats and mitigation controls (4 fully, 1 partially). Labels were easy for all 5 (100%). Navigation was predominantly somewhat easy (60%), with 1 extremely easy and 1 neutral. UX averaged 3.8/5. The recommendation likelihood score averaged 8.0/10 (80%).

DPMA - usability and UI (NFR-002, NFR-005)

DPMA received 5 questionnaire responses. Navigating controls and measures averaged 4.4/5 (88%) and identifying maturity level averaged 4.2/5 (84%). All 5 respondents gave a positive response on threat identification (3 fully, 2 partially). Labels were easy for 4 out of 5 (80%); one rated them as somewhat easy. Navigation was split: 2 somewhat easy, 2 neutral, 1 extremely easy, indicating moderate variability. UX averaged 4.0/5. The recommendation likelihood score averaged 8.0/10 (sum 40/50, 80%). Improvement suggestions included adding tooltips for columns, clearer guidance with practical examples, better UI, and LLM-guided flows through the process.

CAC - usability and UI (NFR-002, NFR-005)

CAC received 6 questionnaire responses. The average difficulty of adding a new product was 2.3/5 (1=very easy, 5=very difficult), indicating the task is generally perceived as easy to moderately easy. All 6 respondents agreed they could use the tool without hiring a cybersecurity expert (avg 4.5/5). UI cleanliness was rated positively by 4/6 (67% Yes, 33% Somewhat). All 6 respondents (100%) found labels, buttons, and instructions easy to understand. Navigation ease was mixed: 3 neutral, 1 somewhat easy, 1 extremely easy, 1 very easy. UX averaged 4.5/5. The recommendation likelihood score averaged 8.3/10 (83%). One respondent suggested UI improvements.

PSTVA - usability and UI (NFR-002, NFR-005)

PSTVA received 6 questionnaire responses. Scan instruction clarity, report helpfulness, and attack surface understanding all averaged 4.7/5, indicating strong functional clarity. Navigation intuitiveness for open-source tools averaged 4.0/5. Labels were easy for 5/6 (83%), with 1 somewhat easy. Dashboard navigation was evenly distributed: 2 neutral, 2 extremely easy, 2 somewhat easy. UX averaged 3.8/5. The recommendation likelihood score averaged 7.2/10 (sum 43/60, 72%), the lowest across all stations, driven by two lower scores (4 and 5). PSTVA UX and navigation continue to be the area requiring the most improvement across validation events.

Contact details for follow-up testing (KPI13)

13 unique email addresses were collected across all stations, with the Portal station having the highest contact capture rate (7/10). These contacts will be followed up to schedule dedicated testing sessions with their own products, contributing to the formal KPI13 count once sessions are conducted.

Recommendation likelihood across stations

Recommendation likelihood scores were collected at all six stations. CAC led with 8.3/10 (83%), followed by CyReA, DPMA, DPRA, and the Portal all at 8.0/10 (80%). PSTVA scored 7.2/10 (72%), below the 8.0 threshold seen in Athens.

Improvement suggestions

Recurring improvement themes across tools and the Portal include: mobile-friendly design (mentioned by multiple respondents across CyReA, DPRA, and the Portal); better UI and clearer guidance with practical

examples (DPMA and Portal); AI or LLM-guided flows through the compliance process (DPMA and Portal); tool-specific visual identity within the portal such as icons per tool (Portal); and navigation improvements to reduce neutral ratings across DPRA, DPMA, and PSTVA.

Conclusions

The Zagreb workshop confirmed the validation findings from Athens and extended them to the CURIUM Portal for the first time. The main conclusions are:

- The CURIUM Portal received its first public validation, with strong scores across navigation between services (4.4/5) and overall UX (4.3/5). Interface intuitiveness (3.9/5) is the main area for Portal UX improvement.
- All five tools demonstrated strong usability (NFR-002) with UX scores ranging from 3.8/5 (DPRA, PSTVA) to 4.5/5 (CAC). CAC showed the strongest improvement compared to Athens.
- UI quality (NFR-005) was positive across all tools. CAC labels (100%) and DPRA labels (100%) were particularly strong. Navigation neutrality (3 out of 5 options for neutral) was more prevalent at Zagreb than at Athens across DPRA, DPMA, PSTVA, and CAC, suggesting that dashboard navigation deserves focused attention in the next development cycle.
- Pre-session confidence was moderate (3.7/7), with 43% of attendees in the low-confidence range, confirming the relevance of CURIUM tools for this audience. CRA awareness impact (KPI22): 82% of Slido respondents reported increased understanding.
- Recommendation likelihood remained strong for CAC (8.3/10), CyReA, DPMA, DPRA, and Portal (all 8.0/10). PSTVA dropped to 7.2/10, driven by two low scores, reinforcing the need for UX iteration on that tool.
- Mobile friendliness is a recurring request across multiple tools and the Portal, so it should be evaluated as a development priority.

4.3.5. Cyprus Skills validation workshop

Event Overview

'Skills for Digital Autonomy: Empowering a Resilient Society', a high-level one-day conference, was held on 5 June 2026 at the EUC Cultural Centre in Nicosia, Cyprus. It was organised by the Cyprus Presidency of the Council of the European Union and the President of the Republic of Cyprus. The conference brought together policymakers, EU institutions, academia, industry, and civil society to discuss cybersecurity, artificial intelligence, digital literacy, and resilient governance.

The CURIUM project participated in the event with a dedicated stand. This was exhibition-based validation rather than a structured workshop, and participation was voluntary, with conference attendees choosing to test the CURIUM tools that interested them at the stand. Given the conference's focus on policy and skills, the audience was more inclined towards institutional and management stakeholders than the product-oriented SME audience seen at other events. This broadens the range of end-user types engaged across the validation campaign.

Validation Objectives

The questionnaires used at the stand were designed to capture:

- The usability of the tools by non-cybersecurity experts, in line with the project's focus on SME accessibility (NFR-002).
- The perceived quality of the user interface of each tool (NFR-005).
- The profile of the visitors in terms of role, sector, and organisation size (KPI6).
- Contact details from users interested in future testing with their own products (KPI13).

Validation Methodology

Validation was conducted through live, hands-on demonstrations at the stand. These were tailored to each visitor's interests and the tools they wanted to test. Visitors were then invited to complete the corresponding tool-specific questionnaire. Two questionnaires were completed on the day of the conference: CyReA (1) and DPMA (1). As this was an optional, stand-based survey conducted at a policy conference, the number of responses was limited. Therefore, the results below are indicative rather than statistically representative.

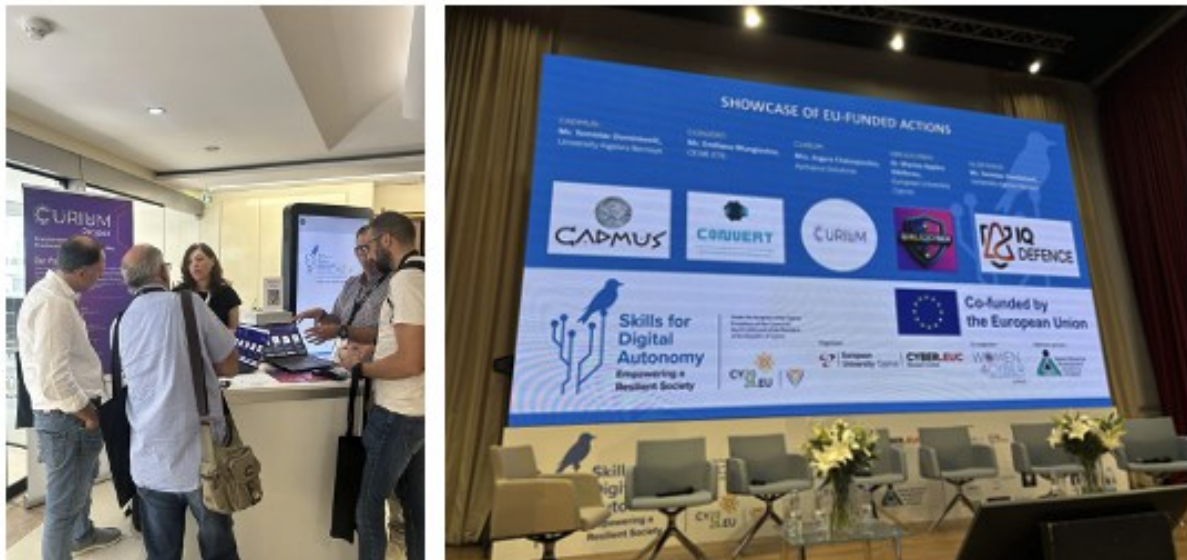


FIGURE 69: CYPRUS SKILLS EVENT ACTIVITIES

Requirements Validation results

The following table summarises the validation status of the requirements addressed at this event:

TABLE 16: CYPRUS SKILLS EVENT REQUIREMENTS VALIDATION

Req. ID	Tool	Requirement	Validation outcome
NFR-002	CyReA	Tools must be usable by non-cybersecurity experts	1 respondent. Would adopt the tool: Yes. Obtained product classification: No (lack of time). Navigation: 1 Extremely easy.
NFR-002	DPMA	Tools must be usable by non-cybersecurity experts	1 respondent. Navigating controls/measures: 5/5. Identifying maturity level: 5/5. Threats identified: Yes (1/1). Navigation: 1 Extremely easy.
NFR-005	CyReA	Dashboard will have clean, simple UI	1 respondent. Labels and buttons easy to understand: Yes (1/1). UX: 4/5.
NFR-005	DPMA	Dashboard will have clean, simple UI	1 respondent. Labels and buttons easy to understand: Yes (1/1). UX: 5/5.

KPIs Validation results

The following table summarises the contributions of the 'Skills for Digital Autonomy: Empowering a Resilient Society' conference activity to the CURIUM project KPIs:

TABLE 17: CYPRUS SKILLS EVENT KPIs VALIDATION

KPI ID	KPI Description	Result at this event
KPI5	Number of prospective products and end-users benefiting from the tools	2 people tested the tools and completed the hands-on questionnaires.
KPI6	Number of diverse instances of Continuum supporting different types of end-users	By role: 2 Management (Non-IT/IS). By sector: 1 Digital infrastructure, 1 Other. By size: 2 Micro-enterprises.
KPI13	Number of tools and services evaluated during validation phase	1 respondent (CyReA) left contact details for future testing.
KPI21	Percentage of end-users providing feedback	Total questionnaires received: 2 (CyReA 1, DPMA 1). All participants who tested a tool completed the corresponding questionnaire, so the feedback rate for this event is 100%.

Feedback analysis

Respondent profile

The two respondents were both Management (Non-IT/IS) representatives of micro-enterprises, one from the digital-infrastructure sector and one from another sector — consistent with the institutional, policy-oriented profile of the conference audience.

CyReA — usability and adoption (NFR-002, NFR-005)

CyReA received 1 response. The respondent indicated they would adopt the tool, but he did not have enough time during the session to complete the classification process for his product, as it contrasts with the strong classification success rate observed at other events and may reflect the short, informal nature of a stand interaction. Labels and buttons were rated easy to understand, navigation was extremely easy, UX was rated 4/5, and recommendation likelihood was 8/10. The respondent left contact details for future testing.

DPMA — usability and UI (NFR-002, NFR-005)

DPMA received 1 response. Navigating through controls and measures and identifying the organisation's maturity level were both rated 5/5, and the respondent identified relevant threats occurring in their organisation. Labels and buttons were rated easy to understand, navigation was extremely easy, UX was rated 5/5, and recommendation likelihood was 10/10.

Conclusions

The 'Skills for Digital Autonomy: Empowering a Resilient Society' conference offered an additional opportunity for external validation through a CURIUM stand at a high-level, policy-oriented European event. The main conclusions are as follows:

- The activity broadened the scope of the validation audience to include institutional and management stakeholders, in addition to the SME- and product-oriented audiences reached at other events (KPI6).

- Both the CyReA and DPMA tools were highly rated for usability and UI by non-cybersecurity experts, with UX scores of 4/5 and 5/5 respectively, and a high likelihood of recommendation (8/10 and 10/10).
- A CyReA respondent expressed intent to adopt the tool but did not complete a product classification during the session (lack of time).

4.3.6. BEYOND validation workshop

Event Overview

BEYOND Expo is the leading international exhibition and forum for digital technology and innovation in Southeast Europe. The sixth edition took place from 17-19 June 2026, at the Metropolitan Expo in Athens. It hosted more than 230 exhibitors from 11 countries and brought together companies, investors, public institutions, and research organizations to explore emerging technologies, such as artificial intelligence, cybersecurity, and digital governance.

The CURIUM project was showcased within this setting at the APIROPLUS SERVICES stand. Unlike the structured validation workshops, this was an exhibition-based activity, with visitors self-selecting to test the CURIUM tools that were most relevant to them. This explains the uneven distribution of responses across tools and the absence of PSTVA testers. Visitors had the opportunity to explore the CURIUM tools through live, hands-on demonstrations and learn how the project helps organizations prepare for and address the requirements of the Cyber Resilience Act (CRA). The demonstrations generated substantive discussions on cybersecurity, regulatory compliance and digital resilience, and produced valuable direct feedback from potential end users, in particular SMEs and product-oriented organisations facing the forthcoming CRA obligations.

Validation Objectives

The validation objectives were the following:

- Validate the functional completeness of the Compliance Continuum tools through live demonstration and/or hands-on testing with a diverse audience of stakeholders.
- Assess the usability of the tools by non-cybersecurity experts, in line with the project's focus on SME accessibility (NFR-002)
- Evaluate the perceived quality of the user interface across all tools (NFR-005)
- Characterise the profile of the visitors in terms of role, sector, and cybersecurity expertise level (KPI6)
- Collect contact details from users interested in future testing with their own products (KPI13).

Validation Methodology

In line with the approach taken at the other workshops, the validation was conducted through live, hands-on demonstrations tailored to each visitor's product and the specific tool they wished to test. Afterwards, visitors were invited to complete the corresponding questionnaire for the tool they had just tested.

The number of completed questionnaires per tool was: CyReA 6, DPRA 1, DPMA 1, CAC 3, PSTVA 0.



FIGURE 70: BEYOND EVENT ACTIVITIES

Requirements Validation results

The following table summarises the validation status of the requirements addressed at this event:

TABLE 18: BEYOND EVENT REQUIREMENTS VALIDATION

Req. ID	Tool	Requirement	Validation outcome
NFR-002	CyReA	Tools must be usable by non-cybersecurity experts	All 6 respondents reported that using the CyReA tool they managed to obtain information on the classification of their product (100%). Navigating: 4 Extremely High, 2 Somewhat easy.
NFR-002	DPRA	Tools must be usable by non-cybersecurity experts	Navigating controls/measures: avg 5/5 Identifying maturity level: avg 4/5 Threats identified: YES (1/1) Navigation ease: 1 Somewhat easy.
NFR-002	DPMA	Tools must be usable by non-cybersecurity experts	Navigating controls/measures: avg 5/5 Identifying maturity level: avg 5/5 Threats identified: YES (1/1) Navigation ease: 1 Extremely easy.
NFR-002	CAC	Tools must be usable by non-cybersecurity experts	Add new product difficulty: avg 1.3/5 (Very Easy) Use without expert: avg 5/5 (strongly agree). Navigation ease: 1 Extremely easy, 2 Very Easy.
NFR-005	CyReA	Dashboard will have clean, simple UI	Labels and buttons easy to understand: 6/6 Navigating: 4 Extremely High, 2 Somewhat easy. UX avg: 4.4/5.

NFR-005	DPRA	Dashboard will have clean, simple UI	Labels easy: 1/1 (100%). Navigation ease: 1 Somewhat easy. Overall user experience: 4/5
NFR-005	DPMA	Dashboard will have clean, simple UI	Labels easy: 1/1 (100%). Navigation: 1 Extremely easy (100%). UX avg: 5/5.
NFR-005	CAC	Dashboard will have clean, simple UI	UI clean: 3/3 (100%). Labels easy: 3/3 (100%). Navigation: 1 Extremely easy, 2 Very Easy Overall user experience: 5/5

KPIs Validation results

The following table summarises the contributions of the BEYOND 2026 expo activity to the CURIUM project KPIs:

TABLE 19: BEYOND EVENT KPIs VALIDATION

KPI ID	KPI Description	Result at this event
KPI5	Number of prospective products and end-users benefiting from the tools	9 people tested the tools and completed the hands-on questionnaires.
KPI6	Number of diverse instances of Continuum supporting different types of end-users	Digital Providers: 5 Research: 2 Other: 2
KPI13	Number of tools and services evaluated during validation phase	Respondents who left contact details: CyReA: 3/6 DPRA: 1/1 (same responder with CyReA and DPMA) DPMA: 1/1 (same responder with CyReA and DPRA) CAC: 0/3 In total, 3 different people expressed their interest in being contacted for further testing.
KPI21	Percentage of end-users providing feedback	Total questionnaires received: 11 (CyReA: 6, DPRA: 1, DPMA: 1, CAC: 3) All participants who tested a specific tool or the Portal completed the corresponding questionnaire, so the feedback rate for this event is 100%.

Feedback analysis

Respondent profile

The 11 questionnaires (9 responders) completed by visitors represented a diverse cross-section of stakeholders. By role (KPI6): 1 Management (Non-IT/ IS), 2 Management (IT/IS), 1 Member of the IT / IS team, 1 Member of an Academic Institution, 1 Academic Institution, 3 Other. By industry sector: 5 Digital providers, 2 Research, 2 Other.

Tools tested during the hands-on session

Visitors were able to select multiple tools. The most tested tool was CyReA (6/11), followed by CAC (3/11), DPRA (1/11) and DPMA (1/11).

CyReA - usability and adoption (NFR-002, NFR-005)

CyReA received 6 questionnaire responses. All 6 respondents (100%) confirmed they were able to obtain information on the classification of their product using the tool, directly validating the core functional purpose of CyReA as the entry point of the Compliance Continuum. Labels and buttons were rated as easy to understand by all respondents (100%). Navigation was extremely easy for 4 (60%) respondents and somewhat easy for 2 (40%). The overall UX was rated at an average of 4.4/5 (88%). The recommendation likelihood scores averaged 9.1/10 (91%). No improvements or recommendations defined.

DPRA - usability and UI (NFR-002, NFR-005)

DPRA received 1 questionnaire response. Navigating through controls and measures was rated 5/5 and identifying the organisation's maturity level at 4/5. Labels and buttons were rated as easy to understand (100%). Navigation was somewhat easy. The respondent identified relevant threats occurring in their organisation and the corresponding mitigation controls (100%). Overall user experience 4/5 (80%). Tool recommendation 8/10 (80%). No improvements or recommendations defined.

DPMA - usability and UI (NFR-002, NFR-005)

DPMA received 1 questionnaire response. Navigating through controls and measures was rated 5/5 and identifying the organisation's maturity level at 5/5. Labels and buttons were rated as easy to understand (100%). Navigation was extremely easy. The respondent identified relevant threats occurring in their organisation and the corresponding mitigation controls (100%). UX rating 5/5 (100%). Tool recommendation 10/10 (100%). No improvements or recommendations defined.

CAC -usability and UI (NFR-002, NFR-005)

CAC received 3 questionnaire responses. All three respondents strongly agreed they could use the tool without hiring a cybersecurity expert (avg 5.0/5). The difficulty of adding a new product was rated at an average of 1.3/5 (1=very easy, 5=very difficult). Clean and simple UI: yes 3/3 (100%). Labels and buttons were rated as easy to understand (100%). Navigation was very easy for 2 respondents and extremely easy for 1 respondent. Overall user experience 5/5 (100%). Tool recommendation 29/30 (96%). No improvements or recommendations defined.

Conclusions

The BEYOND 2026 Expo confirmed the usability findings of the earlier workshops and, in several respects, exceeded them. The main conclusions are as follows:

- The activity produced the strongest usability and recommendation scores of any external validation event: CyReA achieved 4.4/5 for UX and 9.1/10 for recommendation; CAC achieved 5/5 for UX and 96% for recommendation; and DPMA achieved 5/5 for UX.
- CyReA was validated as the entry point of the Compliance Continuum, with all six respondents confirming that they had obtained their product's classification using the tool.
- The usability of the tools for non-cybersecurity experts (NFR-002) and the quality of the user interface (NFR-005) were confirmed as positive.
- We consider the results for DPRA and DPMA as indicative rather than statistically representative because they are based on one respondent each.
- Consistent with the maturity of the tools at this stage of the project, no improvement requests were recorded.

4.3.7. Dedicated product testing

This section describes the activities carried out to engage SMEs in dedicated testing sessions using the CURIUM Compliance Continuum with their own digital products. These activities are directly linked to two project KPIs: KPI13 (number of tools and services evaluated during the validation phase, target >10) and KPI14 (number of CRA compliance use cases and best practices, target >5).

Building the pipeline

Throughout the project's validation and dissemination activities, a systematic effort was made to identify SMEs and organisations interested in testing the CURIUM tools with their own products. This was done through three complementary approaches:

- In validation events with a hands-on component (described in the previous sections) participants were invited through the specific questionnaires to leave their contact details if they wished to be contacted for further testing activities. This captured interest from participants who had already interacted directly with the tools and had a concrete sense of what they could offer.
- In dissemination and capacity building events (described in D5.2) where the focus was on presenting the portal and providing guidance on CRA compliance rather than hands-on testing, participants were invited to scan a QR code and register their interest in staying informed and participating in future activities. Follow-up emails sent after these events included all relevant resources and reiterated the invitation to get involved.
- In addition, partners made direct outreach efforts to SMEs in their own networks who had not necessarily participated in any CURIUM event. These were personalised communications, tailored to the specific profile and compliance needs of each contact, leveraging the trust and existing relationships that partners had built within their ecosystems.

All contacts collected through these channels were compiled into a centralized list, which served as the basis for the individual outreach campaign described below.

Making the tools accessible: the CURIUM Portal

In parallel with the outreach campaign, the consortium made a deliberate effort to lower the barrier to entry for any SME wishing to explore the tools independently. A dedicated section on the project website was created to explain what the Compliance Continuum is, provide access to tool manuals, link to an explanatory video, and offer a direct way to contact the team. From this page, users can access the CURIUM Portal, which opens with an awareness-raising introduction covering the key questions any manufacturer needs to address what the CRA is, which products are impacted, and what the essential security requirements entail. Once familiar with the basics, users can proceed to the compliance portal, register freely, and access all five tools directly. Inside the portal, users can test the tools, download manuals, submit feedback, request support, and book a free one-to-one expert session, all from a single interface.

The portal and its resources were actively promoted through multiple channels: the project website, LinkedIn, follow-up emails to contacts from all validation and dissemination events, and direct outreach by partners to their networks. Despite these efforts, self-registration through the portal did not generate significant inbound interest from unknown SMEs. The participants ultimately engaged in dedicated testing sessions were contacts established through direct personal interaction at events or through partners' existing networks, confirming that in this domain, trust and personal relationship remain the primary drivers of engagement, particularly when organisations are asked to share information about their own products.

Outreach campaign

Once the portal was live and a set of available testing slots had been confirmed with the tool owners, a targeted outreach campaign was launched. The contacts on the list were distributed among partners following a logic of proximity and relevance. In some cases, the allocation was based on who had organised the event (for example, CYS led the Zagreb workshop and is therefore the most recognisable contact for participants from that event). In others, it was based on who had driven the invitations (DSA, for instance, had mobilised most of the participants for the Cyprus event), making a follow-up from them more natural and effective. In the case of the Athens workshop, the Greek-speaking partners were best placed to maintain the relationship with local participants due to the language connection. This personalised approach was chosen deliberately to maximise response rates, as a message from a familiar contact is significantly more likely to generate engagement than an impersonal communication.

The outreach was conducted in two rounds. A first email introduced the opportunity and invited recipients to express their interest and provide basic information about their product and role in the supply chain. A follow-up email was sent to those who had not responded, this time including the confirmed available slots to create a concrete call to action and a sense of urgency.

Organising the sessions

To ensure the testing sessions would be productive and generate the documentation needed for KPI14, a structured preparation process was put in place:

- **Tool owner availability:** An internal coordination round was conducted to identify the dates and times when the tool owners could be available to lead or support the sessions. This resulted in a set of confirmed slots offered to the SMEs.
- **Centralised tracking:** A shared document was created to centralise all relevant information (confirmed participants, selected slots, product information received, and session outcomes) ensuring visibility across the consortium.
- **Pre-session preparation:** SMEs confirming their participation were asked to provide information about their product and intended use case before the session, using a structured template. This allowed the tool owners to tailor the session to the SME's specific context and ensured that the information needed to complete the use case documentation was collected systematically.
- **Use case documentation:** A dedicated Use Case Documentation Template was developed, structured around five sections: Overview and Objectives, Use Case Description, Experiment Setup and Methodology, Results, and Conclusions. This template serves both as a preparation tool for the SME and as the formal evidence for KPI14. The template is provided in **Annex 1 – Use case template for Dedicated Product testing activities**.
- **Post-session follow-up:** After the guided session, SMEs are given access to the portal to continue exploring the tools independently. A follow-up session is planned to collect final feedback and complete the use case documentation.

External validation outcomes and Compliance Gap Analysis

Strategic Overview of External Validation Activities (August–September 2026)

This validation cycle, executed between August and September 2026, represents a critical strategic milestone in fulfilling KPI14 of the CURIUM project. It served as a rigorous stress-test of the CURIUM Compliance Continuum against a diverse portfolio of Products with Digital Elements (PDEs) active in the European market. By subjecting real-world hardware-linked software and AI-driven platforms to the "CURIUM Journey," we have simulated the end-to-end regulatory lifecycle mandated by the EU Cyber Resilience Act (CRA). This process is vital for identifying the friction points SMEs face when transitioning from informal engineering workflows to a formal "Secure-by-Design" mandate.

To ensure data privacy, the **Pseudonymized Entity Identification Key (PEIK)** was implemented to facilitate public disclosure while masking proprietary companies and their respective products names. This is achieved via a structured composite key formatted as: [Country Code]- [SME Code]- [SME ID]- [PDE Code]- [PDE ID].

The following table summarizes the primary validation participants and the technological diversity of the stress-test:

TABLE 20: VALIDATION PARTICIPANTS

Product Name	Product Type / Technology	Organization Role	Assessment Methodology
HR-A-1	Multimedia AR Platform (Cloud/Mobile)	Manufacturer	Guided
HR-B-5	AI-powered Fintech/Banking SDK	Manufacturer	Guided
HR-C-6	Gamified VR Application (Meta Quest/Unity)	Manufacturer	Guided
GR-F-1	Drone flight simulator (desktop software)	Manufacturer	Self-paced

The implementation of the CURIUM Journey, spanning **CyReA** (Scope), **DPRA** (Risk), **DPMA** (Maturity), **PSTVA** (Testing), and **CAC** (Compliance), demonstrated that a logical flow from initial scoping to conformity is the only viable path for SMEs to meet looming CRA deadlines. This structured approach prevents "compliance contagion" where unaddressed risks in early development phases to derail final certification. However, initial assessments immediately surfaced with significant regulatory hurdles regarding the interpretation of "remote data processing" and its impact on classification.

The Comparison Table shows technical documentation gaps & outcomes of guided sessions:

TABLE 21: COMPARISON TABLE AND OUTCOMES OF THE GUIDED SESSIONS

Feature / Metric	HR-A-1	HR-B-5	HR-C-6	GR-F-1
Product Type & Architecture	AR multimedia platform (Azure cloud SaaS & mobile app)	AI data extraction SDK for mobile/web banking apps	VR gamified real estate platform (Unity / OpenXR.apk)	Desktop drone flight simulator running autopilot software used on real drones
CRA Classification	Cloud SaaS not in scope of the CRA (assumed on-prem for testing)	Default (Standard) category	Default (Standard) category	Default (Standard) category
Conformity Assessment Route	Module A (Internal Control / Self-Assessment)	Module A (Internal Control / Self-Assessment)	Module A (Internal Control / Self-Assessment)	Module A (Internal Control / Self-Assessment)
Technical Documentation Uploaded	Draft technical docs & SBOM (parsing timed out)	Internal policies, ISO 27001 SOA, SBOM, public docs	Annex VII draft PDF (v0.9) & SPDX 2.3 JSON SBOM	SBOM and pen testing results uploaded
Identified Documentation & Compliance Gaps	- Missing Annex VII required chapters - Architectural ambiguity (SaaS vs. component) - Questionnaire	- Internal documentation needed restructuring for CRA - Missing "N/A" options for	- Formal Art. 13 risk assessment record missing - Coordinated vulnerability disclosure policy & security.txt missing	- High administrative documentation burden identified - Guidance needed on document

	items left unanswered without warnings	irrelevant self-assessment items External third-party DoC alignment needed	- Defined support period & update policy missing - Art. 14 CSIRT/ENISA reporting workflow missing	ordering and completeness No concrete error messages when assessment failed
SBOM & Vulnerability Findings	SBOM file parsing did not complete within session window	Critical and high-severity library vulnerability findings identified	SPDX 2.3 JSON parsed successfully; minor app defects logged	One vulnerability identified; majority of software components not identified by the platform
CAC Evaluation Outcome	Failed (incomplete questionnaire & parsing delay)	Completed (findings flagged for remediation)	Passed (EVAL_2026_09_15) after initial setup failures	Completed (Declaration of Conformity generated)
Declaration of Conformity (DoC)	Not generated	Issued (EU DoC for HR-B-5 v9.2.1)]	Draft prepared; final DoC pending gap closure	Generated

CRA Scope Assessment and Product Classification Matrix

Determining the correct CRA classification is the foundational pivot of the entire regulatory process. It dictates the mandatory conformity assessment route, specifically whether a manufacturer can utilize a self-assessment (Module A) or must engage in a third-party Notified Body (NB). For SMEs, this distinction is critical; avoiding the months-long bottleneck and high fiscal overhead of an NB audit is a primary driver for product design choices.

The validation activities yielded the following classification outcomes:

- **HR-B-5 (v9.2.1):** This AI-powered SDK was classified under the **"Default" (Standard)** product category. The manufacturer's existing alignment with **ISO/IEC 27001:2022** and **ISO/IEC 27701:2025** provides a robust "Presumption of Conformity" baseline, streamlining the path to meeting the CRA's Essential Requirements.
- **HR-C-6:** Utilizing Meta Quest and OpenXR technology, this VR product was placed in the **"Default"** category. Under **Article 32(1)**, this allows the manufacturer to pursue **Module A (Internal Control)**, enabling a faster time-to-market by keeping the conformity assessment entirely in-house.
- **HR-A-1:** This case highlighted the "SaaS Exclusion" debate. While the mobile client is clearly a PDE, the Azure-hosted backend sparked a debate over **Article 3(1)** regarding "remote data processing solutions." If classified as standalone SaaS, it falls under NIS2; if deemed integral to the PDE, it falls under CRA. For this validation, an **on-premises hosting assumption** was adopted to allow testing to proceed, though the ambiguity remains a strategic risk for the manufacturer.
- **GR-F-1:** Their product was classified as a product with digital elements in scope of the CRA under the Default category, allowing the manufacturer to pursue Module A (Internal Control) self-assessment. The product's in-scope classification was confirmed through CyReA, and a Declaration of Conformity was successfully generated through CAC after completing the full compliance journey.

The "So What?" Layer: These classifications prove that while SMEs can often leverage Module A, any misclassification into "Important" (Class I/II) tiers would introduce a resource-intensive third-party auditing requirement that most small firms are currently unequipped to manage.

Detailed Product Assessment: Vulnerabilities, SBOM, and CAC Outcomes

Technical rigor was applied through the **Cyber Resilience Assessment (CyReA)**, **Digital Product Risk Assessment (DPRA)**, **Digital Product Maturity Assessment (DPMA)**, **Conformity Assessment Companion (CAC)**, and **Product Security Testing and Vulnerability Assessment (PSTVA)** phases. These sessions moved beyond documentation to evaluate the actual "Security of the Build."

HR-B-5

The SBOM analysis for version 9.2.1 identified several **high-severity vulnerabilities** within the dependency set. Given the product's role in "Critical Infrastructure Interactivity"—specifically within the banking and fintech sectors—these findings necessitate a remediation plan prior to issuing a Declaration of Conformity (DoC). Under the CRA, these vulnerabilities must be acknowledged and resolved to prevent supply-chain risks for the thousands of downstream applications integrating the SDK.

HR-C-6

The DPRA identified several exposures inherent to the VR deployment model:

- **Unsigned .apk sideloads** creating update channel vulnerabilities.
- **Man-in-the-Middle (MITM)** risks due to potentially weak certificate validation in outbound HTTPS calls to the content server.
- **Third-party deep-link surfaces** that could be exploited to compromise the headset environment.

HR-A-1

The technical evaluation faced significant hurdles during SBOM parsing. The CAC system encountered processing hangs due to the extreme **dependency tree complexity** of the broader **HR-A** platform. The evaluation initially failed because of incomplete questionnaire responses and the platform's inability to resolve these deep dependencies within the allotted session time.

Across all products, the use of DPRA demonstrated that matching version-specific data against vulnerability databases allows manufacturers to prioritize security patches based on objective risk, rather than subjective internal intuition.

Comparative Synthesis of Technical Documentation Gaps (Annex VII)

Annex VII documentation constitutes the "evidentiary backbone" of CRA compliance. Validation revealed a stark gap between informal "best practices" and the formal evidentiary requirements of the regulation.

The most frequent gaps identified across all participants included:

- **Formal Risk Assessment Records:** A lack of structured records mapping specifically to **Article 13** requirements for identifying "all potential risks."
- **Coordinated Vulnerability Disclosure (CVD):** Absence of public policies, specifically the lack of a "security.txt" file to provide a clear contact point for researchers.
- **Article 14 Reporting Procedures:** Manufacturers lack defined workflows for the **24-hour prescribed reporting window** to CSIRT/ENISA regarding actively exploited vulnerabilities.
- **Lifecycle Management:** Missing definitions for support periods and formal security update policies, which are now legally mandated.

These deficiencies reflect the difficult transition SMEs must make from flexible engineering to a world where "if it isn't documented according to Annex VII, it isn't compliant."

Portal Usability, Privacy, and Technical Integrity Feedback

To ensure tool adoption, the CURIUM portal must minimize "Barriers to SME Onboarding." Feedback from the participants identified three critical technical and UX areas for improvement:

- **Navigation and Workflow:** Users found the separation between "Dashboard" and "Products" confusing. The absence of **validation warnings** for unanswered mandatory fields allowed users to proceed to the evaluation stage only to have it fail without a clear reason.
- **Data Privacy (Critical Finding):** A major "Portal Visibility Concern" was identified where users could see assets belonging to other organizations. This is an **artifact of the free project version's** shared visibility configuration. Future iterations require dedicated restricted sessions to protect confidential technical documentation.
- **Technical Integrity:** Significant "perceived system hangs" occurred during SBOM parsing. This was identified as a UX failure due to a **lack of progress indicators** for long-running parsing tasks. Users also reported UI locks that prevented editing or deleting records while a background evaluation was in progress.

Note on HR-A Self-Paced Testing and Unfinalized Feedback

Beyond the three primary PDEs, HR-A has initiated self-paced testing for three additional products: **HR-A-2**, **HR-A-3**, and **HR-A-4**.

Due to the self-paced nature of these assessments and the timing of the cycle, these results are not yet finalized. However, the next steps are clearly defined:

1. **HR-A-4 requires** a rigorous check for "Important Class" categorization, given its deployment in **Critical Infrastructure** (energy and transport).
2. All three products must prepare granular **SPDX 2.3 JSON SBOMs** to prevent the parsing failures encountered in the **HR-A-1** session.
3. Follow-up sessions will focus on generating draft Declarations of Conformity and refining the "secure-by-design" maturity profiles.

4.3.8. External Validation Summary

This section presents the aggregated assessment of the requirements and KPIs that were identified as externally evaluable, those whose validation depends on the response of real end-users interacting with the tools. For each requirement and KPI, the evidence collected across all events is synthesised to provide a final verdict on whether the target has been met, drawing on the progressive improvement observed throughout the project lifetime.

NFR-002: The tools must be usable by non-cybersecurity experts/non-technical people (SMEs)

To enable a consistent cross-event comparison, overall UX score has been used as the common metric across all events and tools. UX score, as rated by non-specialist users, captures the same dimension: whether a user who is not a cybersecurity expert found the tool sufficiently intuitive and accessible to use.

At Riga (M10), with only CAC and PSTVA available and both tools at an early development stage, the weighted mean UX score was 3.65/5. In Cyprus (M12), the score was 3.70/5, indicating moderate but not yet strong perceived accessibility across the full Continuum. A significant improvement was recorded at Athens (M15), where the weighted mean UX score across five tools reached 4.44/5, reflecting both tool maturation and the richer per-tool feedback enabled by the new questionnaire format. At Zagreb (M16), the weighted mean was 4.10/5 across five tools and the newly introduced CURIUM Portal, a slight decrease compared to Athens that is largely explained by the addition of the Portal at its first validation round and by higher rates of neutral navigation responses across several tools, rather than by a regression in the tools themselves. At Cyprus Skills (M18), both tools evaluated received strong scores (CyReA 4/5 and DPMA 5/5), with navigation rated as extremely easy in both cases. At BEYOND (M18), UX scores across the four tools evaluated averaged 4.6/5, with DPMA and CAC both reaching 5/5 and CyReA averaging 4.4/5.

Taken together, these results confirm that NFR-002 has been met: the Compliance Continuum tools are broadly perceived as usable by non-cybersecurity experts, with all tools scoring above 3.5/5 across all events and the majority scoring above 4.0/5 from Athens onwards. The consistently high scores at BEYOND and Cyprus Skills confirm that this level of usability has been sustained through to the final validation events. The tools most consistently requiring further UX attention are PSTVA and DPRA, which scored 3.8/5 at Zagreb, and Portal interface intuitiveness, which scored 3.9/5 at its first evaluation. These areas were flagged as development priorities for the remaining project period.

NFR-005: The dashboard will have clean, simple UI

Given that NFR-005 specifically requires that the dashboard has a clean, simple UI, the primary indicator used for cross-event comparison is label and button comprehension (the percentage of respondents who found labels, buttons, and instructions easy to understand. In Cyprus, where the label question was not included in the post-event questionnaire, the direct question "Do the applications/tools have a clean, simple UI?" is used instead, as it maps directly onto the NFR-005 definition.

At Riga (M10), label comprehension was low: only 25% of responses rated labels as clearly easy to understand. In Cyprus (M12), 68% of respondents rated the UI as clean and simple (score 4 or 5 on a 1–5 scale), indicating a meaningful improvement. At Athens (M15), label comprehension reached 91% positive (21/23 responses rating labels as clearly easy to understand), with 100% of responses giving at least a somewhat positive rating. At Zagreb (M16), label comprehension remained strong at 89% positive (24/27 responses), with 100% giving at least a somewhat positive rating across all five tools. At Cyprus Skills (M18), label comprehension was also 100%

across both tools evaluated. At BEYOND (M18), label comprehension was 100% across all four tools evaluated (CyReA: 6/6, DPRA: 1/1, DPMA: 1/1, CAC: 3/3).

Taken together, these results confirm that NFR-005 has been met. The improvement from 25% at Riga to 100% at the final validation events is the clearest indicator of UI progress across the project's development cycles, confirming that the UI improvements introduced between Riga and Athens have been fully sustained.

KPI5: Number of prospective products and end-users benefiting from the tools

KPI5 tracks the number of prospective end-users who have directly benefited from the CURIUM Compliance Continuum tools through hands-on testing. Across all six validation activities, a total of 47 unique individuals tested at least one CURIUM tool: 4 at Riga (M10), 6 at Cyprus (M12), 10 at Athens (M15), 16 at Zagreb (M16), 2 at Cyprus Skills (M18) and 9 at BEYOND (M18). No audience overlap between events has been identified, as each event took place in a different country or distinct setting with a local audience. The cumulative count of 47 unique testers across the six validation events, complemented by 1 additional SME recruited through direct partner outreach for the dedicated product testing activities, significantly exceeds the target of more than 20, confirming that KPI5 has been met with considerable margin.

KPI6: Number of diverse instances of Continuum supporting different types of end-users

KPI6 tracks the diversity of end-user profiles that have engaged with the CURIUM Compliance Continuum across validation activities. Profile data were collected through questionnaires at all six events, covering respondent role, industry sector, and organisation size.

Across all six events, at least 8 distinct roles were represented, including team members, management, product development staff, compliance officers, manufacturers, end users, consultants, and academics. At least 10 distinct industry sectors were covered, including IT, banking, telecommunications, financial services, research, public administration, education, healthcare, energy and defence. The addition of BEYOND and Cyprus Skills further diversified the audience by including policy-oriented stakeholders and institutional representatives not prominently present in the earlier structured workshops. All four organisation size categories (micro, small, medium, and large) were represented across the events where this dimension was collected.

Taken together, these results confirm that KPI6 has been met with considerable margin: the Compliance Continuum has been tested by a diverse range of stakeholder profiles across multiple EU Member States, sectors, and organisational contexts.

KPI8: End-users testing and reporting reduction of costs via the use of CURIUM Compliance Continuum

KPI8 tracks the percentage of end-users who, after testing the CURIUM Compliance Continuum, believe it could reduce their overall CRA compliance costs compared to their current approach. The question was proposed at Cyprus and Zagreb; it was not included at Riga, Athens, Cyprus Skills or BEYOND, due to format constraints at those events. In Cyprus, 24 out of 25 questionnaire respondents (96%) selected one of the three affirmative options: Yes, significantly (20%); Yes, moderately (40%); or Yes, slightly (36%). Only 4% indicated no change and no respondent believed costs would increase. At Zagreb, 14 out of 15 respondents to the question (93%) gave a positive response, with the majority expecting a moderate reduction (73%). Combined across both events, 38 out of 40 respondents (95%) reported a positive cost reduction perception, well above the 85% target. These results confirm that KPI8 has been met.

KPI13: Number of tools and services to evaluate during validation phase

KPI13 tracks the number of external products and services evaluated using the CURIUM Compliance Continuum tools through dedicated testing sessions in which SMEs test their own products rather than pre-prepared use-case scenarios. The pipeline for these sessions was built throughout the project's validation activities, with a total of 34 unique contacts collected from respondents who expressed interest in participating: 1 at Riga, 6 at Cyprus, 10 at Athens, 13 at Zagreb, 1 at Cyprus Skills and 3 at BEYOND. Additional SMEs were recruited through direct outreach by consortium partners to their own networks, independently of the event-based pipeline. From both sources, four SMEs confirmed their participation and completed dedicated testing sessions between August and September 2026. Each SME tested one or more of their digital products using multiple CURIUM tools, resulting in a total of 17 product-tool combinations evaluated across the four organisations.

KPI14: Number of CRA compliance use-cases and best-practices

KPI14 tracks the number of documented CRA compliance use cases produced by SMEs using the CURIUM tools, following a structured template covering objectives, methodology, results, and conclusions. At Zagreb (M16), the Slido closing question "During your use of the CURIUM tools, can you describe a use-case where the tool helped your SME complete a CRA compliance task?" was answered by 17 participants: 29% said Yes, 59% said Possibly, and 12% said No. While this indicates that 88% of respondents could at least potentially describe a relevant use case, a verbal indication of possibility does not constitute a documented use case for the purposes of this KPI. The collection of completed use-case templates has been done as part of the dedicated SME testing activities (Section 4.3.7) in conjunction with the KPI13 follow-up sessions (7 use cases).

KPI18: Number of business cases elaborated

KPI18 tracks the number of business cases elaborated by the CURIUM consortium, distinct from the SME-produced use cases of KPI14. Business cases in this context refer to the structured use-case scenarios developed and demonstrated by consortium partners during validation events, each illustrating how a specific CURIUM tool addresses a concrete CRA compliance need. Across all six validation activities, six distinct business cases have been elaborated and demonstrated: CyReA for CRA product scope and classification; DPRA for ICT product risk assessment, illustrated with a CCTV system scenario; DPMA for risk treatment planning and maturity assessment; CAC for technical documentation creation and automated EU Declaration of Conformity generation; PSTVA for web service vulnerability assessment; and the CURIUM Portal for end-to-end Compliance Continuum workflow navigation, introduced at Zagreb. The target of more than 5 business cases has been met.

KPI21: Percentage of end-users providing feedback

KPI21 tracks the percentage of end-users who participated in hands-on testing and subsequently provided structured feedback through a questionnaire. The feedback rate was 100% at all six validation events.

KPI22: Increase of levels of awareness of participating SMEs on the scope and requirements of the CRA

KPI22 tracks the percentage of participants who report an increase in their understanding of CRA requirements following a CURIUM validation session. The question "After today's session, my understanding of the CRA requirements has..." (Increased a lot / Increased / Stayed the same / Decreased) was administered in Cyprus (M12) and Zagreb (M16); it was not included at Riga, Athens, Cyprus Skills or BEYOND, due to the format of those events. In Cyprus, 84% of respondents reported a positive change in awareness (60% Increased, 24% Increased a lot), out of 25 responses. At Zagreb, 82% of Slido respondents reported a positive change (76% Increased, 6% Increased a lot), out of 17 responses. Combined across both events, 35 out of 42 respondents (83%) reported increased awareness, above the 80% target. These results confirm that KPI22 has been met.

KPI26: Acceptance of the available tools and services from the end-users / SMEs that are using CURIUM

KPI26 tracks the acceptance of CURIUM tools and services among end-users and SMEs, with a target of more than 75% positive responses. The adoption intent question ("After using/testing the CURIUM tools, would you consider adopting them in your company?") was collected in Cyprus, Athens, and Zagreb; not at Riga, Cyprus Skills or BEYOND.

Across the three events where the question was administered, 31 out of 49 respondents gave a positive answer (Yes, definitely or Yes, probably), for a combined rate of 63%. While this represents a positive and improving trend (from 56% at Cyprus to 71% at Athens and 71% at Zagreb), the primary adoption indicator does not reach the 75% target.

A complementary indicator is available through the recommendation likelihood question (0–10 scale, threshold of 7 or above as positive), which was included in the per-tool questionnaires at Riga, Athens, Zagreb, and BEYOND. At Riga, Athens, and Zagreb 80% of the testers gave a positive recommendation score. At BEYOND, all 11 testers gave scores above 7, with averages ranging from 8/10 (DPRA) to 10/10 (DPMA) across all tools tested, and CyReA averaging 9.1/10. Cyprus is excluded from this calculation as the recommendation question was not included in the Cyprus post-event questionnaire, and Cyprus Skills is excluded as the event format did not include this question.

Taken together, these two indicators point in the same direction but at different levels: adoption intent, which reflects a more demanding form of acceptance requiring a concrete commitment to use, falls just below the target at 63%, while recommendation intent, which reflects a broader form of endorsement, reaches 80% across the structured workshops and is further reinforced by the exceptionally high scores at BEYOND. The gap

between the two is consistent with what is typically observed at an early adoption stage, where users find a product valuable enough to recommend to others before committing to adopting it themselves.

Dedicated product testing

The dedicated product testing sessions described in Section 4.3.7 provide an additional and qualitatively distinct layer of evidence that complements the workshop-based validation results. Unlike the structured events, which used pre-prepared use-case scenarios, these sessions involved SMEs testing the CURIUM tools with their own real digital products under guided expert support. Four SMEs participated, testing a total of eight product-tool combinations across CyReA, DPRA, CAC, and PSTVA. The sessions confirmed the functional validity of the tools in real-world conditions, identified specific technical issues, including SBOM parsing limitations in CAC and data visibility concerns in the portal, that have been communicated to the development team, and generated concrete CRA compliance findings for each product, including vulnerability prioritisation reports, technical documentation gap analyses against Annex VII, and preliminary product classifications.

5. Final Assessment

5.1. Requirements

All 57 requirements defined in D2.2, 25 functional (FR), 16 technical (TR), and 16 non-functional (NFR), have been confirmed as met through the validation activities documented in Sections 4.2 and 4.3. The requirements were evaluated across five aspects defined in D2.2: Functionality, Reliability and Functional Stability, Usability and ease of access, Knowledge capacity, and Financial factors. The following analysis consolidates the results by evaluation aspect, covering both internal and external validation.

Functionality

The majority of requirements address functional aspects, all 25 functional requirements and a subset of technical requirements (TR-001, TR-006, TR-007, TR-009, TR-010, TR-012, TR-013, TR-016, TR-017) fall under this aspect. All were validated internally through demonstration, inspection, or testing by the responsible tool owners.

The validation confirmed that the Compliance Continuum covers the full CRA compliance workflow: CyReA guides users through product scoping and classification (FR-021 to FR-025); DPRA supports asset decomposition, vulnerability identification, and risk assessment publication (FR-014 to FR-020); DPMA enables assessment of cybersecurity control performance, maturity road-mapping, and extraction of mitigating measures (FR-008 to FR-013); PSTVA supports scan execution, report generation, and report management (FR-005 to FR-007); and CAC generates Technical Documentation, the EU Declaration of Conformity, and manages digital product metadata (FR-001 to FR-004).

A noteworthy case within this aspect is the evolution of DPMA's technical requirements. TR-016 and TR-017 were originally specified in terms of Microsoft Excel functions and sheet-level protection mechanisms, reflecting the tool's initial spreadsheet-based implementation. Following APIRO's decision to migrate DPMA to a web application, these requirements were re-evaluated against the new implementation: the filtering and search capabilities of the web application replace the Excel functions, and server-side data integrity enforcement replaces sheet-level protection. The requirements are confirmed as met in their intent, with the means of verification updated accordingly.

Reliability and Functional Stability

Requirements under this aspect address system availability, fault tolerance, security, and operational robustness. They include TR-003 (containerization), TR-004 (encrypted and immutable data storage), TR-005 (user action logging), and NFR-004 (GDPR compliance), NFR-006 (easy updates and patches), NFR-008 (least privilege execution), NFR-011 (strong authentication and authorization), and NFR-014 (real-time interoperability with open intelligence sources). All were validated internally through inspection or demonstration.

A notable finding within this aspect is NFR-008 (least privilege execution), where the validation confirmed that privileged container execution has been avoided across all services with one documented and justified exception: the worker service requires Docker API access for scanner orchestration. This exception is network-isolated and localhost-bound, and remaining hardening actions have been identified and scheduled for a further release.

Usability and Ease of Access

This aspect covers how intuitive and accessible the tools are for SMEs with limited resources. It includes TR-002 (SSO), TR-008 (output formats in PDF, Word, XML), TR-011 (browser-based UI), TR-014 (cross-platform operability), NFR-001 (browser accessibility), NFR-002 (usability by non-experts), NFR-003 (error handling and guided help messages), NFR-005 (clean, simple UI), NFR-012 (intuitive DPRA dashboard), NFR-013 (browser access and secure storage of risk assessment outcomes), NFR-015 (questionnaire access for legitimate users), and NFR-016 (wizard-based interactive questionnaire). Evaluation methods include test, inspection, and demonstration depending on the requirement.

This is the aspect where the most significant evolution was observed across the project lifetime, as it includes the two externally validated requirements. NFR-002 (usability by non-cybersecurity experts) showed a clear improvement trajectory across all validation events: from a weighted mean UX score of 3.65/5 at Riga (M10) to 4.4–5.0/5 per tool at BEYOND (M18). NFR-005 (clean, simple UI) showed the clearest progression: label and

button comprehension rose from 25% positive at Riga to 100% at BEYOND and Cyprus Skills, directly reflecting the impact of the iterative UI refinements carried out between validation rounds.

TR-014 deserves specific mention: originally specified for Microsoft Excel 2016 on Windows and macOS, the migration of DPMA to a web application means the portability objective is now met more broadly, as the tool is accessible through any modern browser on any operating system.

Knowledge Capacity

Two requirements address this aspect: NFR-009 (user manuals for CLI and Web UI) and NFR-010 (detailed technical documentation including architecture). Both were validated internally through demonstration, confirming that step-by-step user guides are accessible directly from the portal for each tool, and that technical documentation including architecture is maintained in the tool repositories. These resources were referenced by participants across multiple validation events as a key enabler for independent tool exploration.

Financial Factors

NFR-007 (resource efficiency) is the only requirement under this aspect. It was validated through testing and direct measurement of container resource consumption via docker stats, captured at three operational states: idle (total memory ≤ 2 GiB, CPU $\leq 10\%$), under load (total memory ≤ 4 GiB during concurrent scanning), and post-load (memory returns to within 10% of idle baseline). This confirms that the tools operate within cost-effective hardware limits without requiring expensive high-performance infrastructure, a critical factor for SME adoption.

5.2. KPIs

The following table presents the consolidated status of the 20 KPIs tracked in this deliverable. These correspond to the KPIs related to technical validation and the validation process itself, as indicated in the project's Performance Monitoring excel file document. KPIs related to knowledge and capacity building (Objective 3) and communication and dissemination are reported in D3.2 and D5.2 respectively. Detailed evidence and analysis for each KPI are provided in Section 4.2 (for the KPIs validated internally) and Section 4.3 (for the KPIs validated externally).

TABLE 22: KPIs RELATED TO TOOL DEVELOPMENT AND TECHNICAL IMPLEMENTATION

#	KPI	Target	Status	Result
1	Number of tools to facilitate and automate CRA compliance	>10	Met=20	The total is 6 third-party engines and 14 in-house modules, across all five CURIUM tools
4	Number of tools to simplify and automate CRA documentation	>=2	Met=2	CAC and PSTVA provide documentation
7	Number of open-source tools used	>8	Met=15	CVE, CPE, CAPEC, Nmap, Nikto, Horusec, ADENUM, Kerbrute, Keycloak, Grype, Spring Boot, SPDX 2.3, Apache Maven, Ollama, Qwen3-4B
13	Number of tools and services to evaluate during validation phase	>10	Met=17	Number of tools/services evaluated with SME own products has been 17. At the moment of submitting this deliverable, another two SMEs are testing the continuum, this will be included in the final review report.
16	Number of open-source components made available	>5	Partially Met=5	IAM, Frontend, Backend, Scanning environment, SmartGraph

23	Open-source tools examined for integration	>10	Met=14	CVE, CPE, CAPEC, Nmap, Netdiscover, Nikto, OpenVAS Scanner, Secret Scanner (GitHub), Bandit, Gripe, Vault, TheHive, Fuff, Metasploit Framework
----	--	-----	--------	--

TABLE 23: KPIS FOR CRA COMPLIANCE AND REQUIREMENTS COVERAGE

#	KPI	Target	Status	Result
2	CRA essential requirements fully covered by tools	>12	Partially Met=12	SR1, SR2, SR3a, SR3b, SR3c, SR3f, SR3g, SR3h, SR3i, VR1, VR2, VR3
3	CRA essential requirements partially covered by tools	>6	Met=9	SR3d, SR3e, SR3j, SR3k, VR4, VR5, VR6, VR7, VR8
14	Number of CRA compliance use-cases and best-practices	>5	Met=7	External testers have created their use-cases with the help of the CURIUM partners using the use case template (see Annex 1 – Use case template for Dedicated Product testing activities). At the moment of submitting this deliverable, another two SMEs are testing the continuum and will fill in the template with the results obtained.
25	Alignment of tools with CRA essential requirements	>90%	Partially Met=84%	SR1, SR2, SR3a, SR3b, SR3c, SR3d
28	Completion of all mandated documentation needed by an SME using CURIUM to comply with CRA	>80%	Met=100%	CAC tool provides guidelines to the requirements for the technical documentation and gives comments and feedback in accordance with Annex VII to the uploaded documentation and SBOM. PSTVA generates structured report about vulnerabilities, etc.
29	Maintain a compliance documentation accuracy rate through regular internal reviews and validation processes	>=98%	Met=99,2%	Successfully maps all CRA Essential Requirements, including those related to product properties, vulnerability handling, and Annex V-VIII mandates, to the system's functional architecture

TABLE 24: KPIS FOR USER ADOPTION AND FEEDBACK

#	KPI	Target	Status	Result
---	-----	--------	--------	--------

5	Number of prospective products and end-users benefiting from the tools	>20	Met=47+1=48	47 unique testers were recorded across the six validation events. Of these, 5 SMEs that had participated in the Zagreb workshop went on to join the dedicated product testing activities, with 3 of them producing concrete results by the time of submitting this deliverable. An additional SME, which had not previously participated in any validation event, also joined the dedicated product testing activities through direct partner outreach.
6	Number of diverse instances of Continuum supporting different types of end-users	>5	Met	8+ roles, 10+ sectors, 4 organisation sizes across 6 events and dedicated product testing.
8	End-users reporting cost reduction	>85%	Met=95%	95% positive across Cyprus and Zagreb events
21	Percentage of end-users providing feedback	>90%	Met=100%	100% across all 6 validation events and dedicated product testing.
22	Increase in SME awareness of CRA	>80%	Met=83%	83% combined (Cyprus 84%, Zagreb 82%)
26	Acceptance of tools by end-users / SMEs that are using CURIUM	>75%	Partially Met	Adoption intent 63%; recommendation intent 80%

TABLE 25: KPIs FOR PROJECT MANAGEMENT AND OPERATIONS

#	KPI	Target	Status	Result
18	Number of business cases elaborated	>5	Met=6	6 distinct business cases demonstrated across validation events
19	Number of release rounds	>=2	Met=3	3 rounds completed (M8-M12 progressive, M16, M18)

6. Conclusions and next steps

The validation process, covering the period from M8 to M21 of the project, encompassed six external validation events across five EU countries, dedicated SME testing sessions, and internal assessment of 57 requirements and 20 KPIs. Together, these activities provide sufficient evidence to evaluate the CURIUM Compliance Continuum not only as a collection of five individual tools but as an integrated system designed to guide organisations through the full CRA compliance journey.

The tools work best when used in sequence. CyReA establishes whether action is needed and of what kind; DPRA identifies the specific vulnerabilities and risks associated with the product's components; DPMA maps those risks to concrete mitigation measures at the appropriate maturity level; PSTVA provides the technical evidence of security testing; and CAC assembles the final documentation package including the EU Declaration of Conformity. The introduction of the CURIUM Portal formalised this sequence into a single unified access point, making the compliance journey navigable for organisations without dedicated cybersecurity expertise. The dedicated SME testing sessions confirmed this in practice: across the four SMEs that participated, the tools collectively enabled product classification, vulnerability identification, maturity assessment, security testing, and structured gap analysis against CRA Annex VII, addressing precisely the documentation gaps most frequently identified in real products.

All 57 requirements are confirmed as met. Of the 20 KPIs tracked, 16 are confirmed as met and 4 are partially met. The most significant results include: 47 unique testers across 6 events, plus 1 additional SME recruited through direct partner outreach for the dedicated product testing activities. 5 SMEs from Zagreb event also joined these activities but are not counted again, as they are already included in the 47 unique testers (KPI5, target >20); 95% of interviewed respondents indicating cost reduction potential (KPI8, target >85%); 83% reporting increased CRA awareness (KPI22, target >80%); and 100% feedback rate across all events (KPI21, target >90%). KPI26 (tool acceptance) presents the most nuanced picture: adoption intent reached 63% (below the 75% target) while recommendation intent reached 80%, reflecting the gap between finding a tool valuable and committing to integrate it into organisational practice. This gap is expected to narrow as the tools mature and as regulatory deadlines create concrete urgency.

The validation also confirmed a clear improvement trajectory across the project lifetime. UX scores rose from 3.65/5 at Riga (M10) to 4.6/5 at BEYOND (M18), and label comprehension from 25% to 100%, directly reflecting the impact of the iterative feedback and refinement cycles between validation rounds. The remaining technical gaps (SBOM parsing limitations, a portal data visibility issue, and UI workflow gaps) are known, documented, and being addressed in the final development cycle.

Beyond the project's formal conclusion, the CURIUM Compliance Continuum will remain publicly accessible through the portal until the end of 2027, aligned with the full entry into force of the Cyber Resilience Act in December of that year. During this period, SMEs will be able to access all five tools, download training materials and user manuals, and book free expert-guided sessions to test the tools with their own products. This extended availability ensures that the Continuum can accompany organisations throughout the entire transition period, from initial CRA awareness to full compliance readiness, providing practical, free, and expert-supported guidance at every stage of the journey.

7. Annexes

7.1. Annex 1 – Use case template for Dedicated Product testing activities

CURIUM Compliance Continuum — Use Case Documentation Template

This document is intended to capture a concrete use case of the CURIUM tools applied to a real digital product, demonstrating how the Compliance Continuum supports CRA compliance in practice (KPI14).

1. Overview and Objectives

Organisation name	
Role in supply chain	☐ Manufacturer / ☐ Importer / ☐ Distributor:
Product selected for this use case	
Brief product description	
CRA scope	Is the product in scope of the CRA? (☐ Yes / ☐ No / ☐ Uncertain):
Current compliance status	What CRA-related activities has the organisation already undertaken, if any?
Objective of this use case	What does the organisation aim to achieve by using the CURIUM tools? For example: • "We need to assess whether our product falls under CRA scope and which conformity assessment procedure applies" • "We want to perform a risk assessment for our product and identify the key cybersecurity risks" • "We need to generate technical documentation aligned with CRA Annex VII" • "We want to run a vulnerability scan on our product and get a report"

2. Testing Setup / Methodology

Format	☐ Online session / ☐ self-paced:
Date	
Duration	
Participants	Role and number of people involved from the organisation:

Tools accessed	Which tools were used: ☐ CyReA ☐ DPRA ☐ DPMA ☐ PSTVA ☐ CAC ☐ TAC ☐ CURIUM COMPLIANCE CONTINUUM
Support provided	☐ Guided by CURIUM technical experts / ☐ Self-guided with manual / ☐ Both:
Product information used	What information about the product was shared or input into the tools (no sensitive data required):

3. Results

CyReA	What did the tool reveal about the product's CRA classification and scope?
DPRA	What cybersecurity risks were identified for the product?
DPMA	What maturity level was assessed for the product's security controls?
PSTVA	What vulnerabilities were identified? What did the scan report show?
CAC	What gaps were identified in the technical documentation? Was a Declaration of Conformity generated?
Overall outcome	Did the tools help complete the intended CRA compliance task? (☐ Yes / ☐ Partially / ☐ No)
Key findings	Summary of the most relevant findings for the organisation
Feedback on the tools	Usability, clarity, usefulness...any comments from the participants

4. Conclusions

Value delivered	How did the CURIUM tools help this organisation with CRA compliance?
------------------------	--

Best identified practices	Any recommendations or lessons learned that could be useful for other SMEs in a similar situation
Next steps	What will the organisation do next as a result of this session?
Interest in continued use	Would the organisation consider using the CURIUM tools beyond this session?

7.2. Annex 2 – Compliance Coverage Matrix

Req	Topic	Tool feature that addresses it	Coverage
SR1	Risk-based security	DPRA automated multi-order risk assessment; Protection Profile	Full
SR2	No known exploitable vulnerabilities	CAC SBOM vulnerability analysis; PSTVA scans; DPRA CTI feed	Full
SR3a	Secure by default configuration	PSTVA misconfiguration findings; DPRA configuration controls	Full
SR3b	Protection from unauthorised access	DPRA objectives, requirements and NIST controls; PSTVA Kerbrute	Full
SR3c	Confidentiality of data	DPRA objectives and controls; PSTVA transport and web checks	Full
SR3d	Integrity of data, commands and configuration	DPRA control assignment; CAC questionnaire and evidence upload	Partial
SR3e	Data minimisation	CAC questionnaire and documentation; DPMA measures	Partial
SR3f	Availability and DoS resilience	DPRA cascading-effect and propagated-risk estimation	Full
SR3g	Minimise impact on other services	DPRA interdependent-asset cascading analysis	Full
SR3h	Limit attack surfaces	PSTVA Nmap service discovery; Ffuf fuzzing; Nikto	Full

SR3i	Exploitation mitigation	PSTVA exploitability checks; DPRA attack potential and controls	Full
SR3j	Logging and monitoring	DPMA logging measures; DPRA audit controls; CAC questionnaire	Partial
SR3k	Security updates	CAC questionnaire and documentation upload	Partial
VR1	SBOM and component identification	CAC SPDX import, component tree, highlighted vulnerabilities	Full
VR2	Remediate without delay	CAC Recommendations with action tracking; PSTVA prioritised remediations	Full
VR3	Regular tests and reviews	PSTVA automated scans; repeatable CAC self-assessment	Full
VR4	Public disclosure of fixed vulnerabilities	Advisory content from CAC and PSTVA findings; publication is manual	Partial
VR5	Coordinated vulnerability disclosure policy	CAC documentation upload (vulnerability management plan)	Partial
VR6	Information sharing and contact address	CAC user-instructions document; DPRA CTI repository	Partial
VR7	Secure distribution of updates	CAC questionnaire and documentation	Partial
VR8	Free, timely patches with advisories	CAC questionnaire and documentation	Partial