



Cra sUppoRt contInuUM

D5.2 - Final report on Dissemination, Exploitation, Standardisation & Sustainability

Document Summary Information

Grant Agreement No	101190372	Acronym	CURIUM
Full Title	Cra sUppoRt contInuUM		
Start Date	01.01.2025	Duration	18 months
Project URL	www.curium-project.eu		
Deliverable	D5.2 - Final report on Dissemination, Exploitation, Standardisation & Sustainability.		
Work Package	WP5		
Contractual due date	30.09.2026	Actual submission date	30.09.2026
Nature	R — Document, report	Dissemination Level	PU - Public
Lead Beneficiary	APIROPLUS SERVICES LTD.		
Responsible Author	Argyro Chatzopoulou		
Contributions from	All partners		

Revision history (including peer reviewing & quality control)

Version	Date	Author	Notes
0.1	11/05/2025	APIRO	ToC
0.2	06/07/2026	P-NET, APIRO	Input from P-NET and APIRO
0.3	20/07/2026	APIRO, P-NET, NCSA	Input from partners P-NET, APIRO and NCSA
04	28/08/2026	APIRO, P-NET, NCSA	Input from partners P-NET, APIRO and NCSA
0.5	11/09/2026	APIRO, P-NET, NCSA	Input from partners P-NET, APIRO and NCSA
0.6	17/09/2026	P-NET	KPIs updates
0.7	18/09/2026	AEGIS, DSA	Internal review
0.8	25/09/2026	APIRO, P-NET, NCSA	Address comments from Internal review
1.0	29/09/2026	APIRO	Final Version

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 This Deliverable contains original unpublished work except where clearly indicated otherwise.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	8
2. Introduction	10
3. Dissemination & Communication Activities	11
3.1 Introduction & Scope	11
3.2 Dissemination and Communication Approach During the Reporting Period	12
3.3 Dissemination Activities.....	12
3.3.1 Collaboration with European Projects and Initiatives	12
3.3.2 Participation in the CRA Cluster and CRA Standards Unlocked EU Tour	16
3.3.3 Participation in the CyberHubs European Network.....	17
3.3.4 Conference & Scientific Events	18
3.3.5 Awareness-Raising & Stakeholder Engagement	20
3.3.6 Training and Capacity Building	27
3.3.7 Validation Activities and Stakeholder Engagement	28
3.3.8 Scientific Publications and Magazine Articles	28
3.3.9 Policy and Regulatory Stakeholder Engagement	30
3.4 Communication Activities	31
3.4.1 Project Website	31
3.4.2 Social Media	33
3.4.3 Newsletters	35
3.4.4 Videos	36
3.4.5 Promotional Material and Outreach	37
3.5 Assessment of Dissemination and Communication KPIs	38
3.5.1 KPI Achievement Overview	38
3.5.2 Dissemination & Communication KPI Achievement	38
3.5.3 Overall Assessment	41
4. Exploitation Activities / Plans	43
4.1. Introduction & Scope.....	43
4.2. Methodology for Exploitation Planning.....	44
4.2.1. Exploitation and Market Analysis Strategy	44
4.2.2. Identification and Classification of Exploitable Results	45
4.3. Overview of the 7 KERs	48
4.3.1. Overview of the CURIUM KER Ecosystem	48
4.3.2. Business and Value Creation Logic.....	50
4.3.3. Value Proposition Canvas Approach	51
4.3.4. Exploitation Intentions Overview	54
4.3.5. Market Context and Stakeholder Ecosystem	55
4.3.6. Competitive Positioning of CURIUM's Compliance Continuum	58

4.3.7. IPR & Exploitation Governance	59
4.3.8. Sustainability and Future Evolution	61
4.4. Exploitation Plans per Key Exploitable Result	63
4.4.1. KER1 – CURIUM Continuum – Responsible Partner: Consortium	63
4.4.2. KER2 – Penetration Self-Testing and Vulnerability Assessment Services and tools (PSTVA) - Responsible Partner: AEGIS	67
4.4.3. KER3 – CRA Scoping and Product Classification Service (CyReA) - Responsible Partner: NLG	72
4.4.4. KER4 – Digital Product Risk Management (DPRA) - Responsible Partner: NLG	77
4.4.5. KER5 – Conformity Assessment and Compliance Service (CAC) - Responsible Partner: CYS	83
4.4.6. KER6 – Digital Product Maturity Assessment (DPMA) - Responsible Partner: APIRO	89
4.4.7. KER7 – CURIUM Capacity Building Plan and Services	94
5. Standardization Activities	103
5.1. Introduction & Scope	103
5.2 Provision of feedback	104
5.2.1 Feedback on draft standards	104
5.2.2 Participation in standardisation related working groups	105
5.2.3 Feedback on draft regulatory (related) activities	106
5.3 Clustering	107
5.4 Other activities	110
6. Collaboration Activities	111
6.1. Introduction & Scope	111
6.2. Collaboration Activities Performed	113
6.3 Section Summary	121
7. Conclusion	123
7.1. General remarks	123
7.2. Sustainability Outlook	124

List of Figures

FIGURE 1: EU CYBER RESILIENCE WORKSHOP – “CYBERPROOFING YOUR COMPANY: TOOLS & TIPS”	13
FIGURE 2: OPEN VALIDATION WITH SMES, PARIS	14
FIGURE 3: COCYBER CONCERTATION WORKSHOP, BRUSSELS	15
FIGURE 4: CRA STANDARDS UNLOCKED – EU TOUR	17
FIGURE 5: IEEE CSR WORKSHOP ON INFORMATION & OPERATIONAL TECHNOLOGY SECURITY (IOSEC), LISBON	18
FIGURE 6: LIFESEC WORKSHOP / IEEE SMARTCOMP 2026	19
FIGURE 7: INTERNATIONAL CONFERENCE ON ENGINEERING, TECHNOLOGY AND INNOVATION (ICE IEEE/ITMC 2026), PORTO	20
FIGURE 8: BEYOND EXPO 2026, ATHENS	21
FIGURE 9: SKILLS FOR DIGITAL AUTONOMY: EMPOWERING A RESILIENT SOCIETY, CYPRUS.....	22
FIGURE 10: SOUTH SUMMIT MADRID 2026.....	23
FIGURE 11: PATRAS IQ 2026.....	24
FIGURE 12: AI ENABLES CYBERSECURITY EVENT, ATHENS	24
FIGURE 13: ISACA ATHENS CHAPTER CONFERENCE 2025	25
FIGURE 14: CYBERSECURITY CAREER FAIR, NICOSIA.....	26
FIGURE 15: CYBER RESILIENCE ACT (CRA): OBLIGATIONS IN THE SUPPLY CHAIN EVENT, CYPRUS	27
FIGURE 16: CURIUM GA4 ANALYTICS – WEBSITE VISITS 2025.....	32
FIGURE 17: CURIUMGA4 ANALYTICS – WEBSITE VISITS 2026.....	32
FIGURE 18: LINKEDIN ANALYTICS – FOLLOWER GROWTH	33
FIGURE 19: LINKEDIN ANALYTICS – IMPRESSIONS.....	34
FIGURE 21: CURIUM PROJECT NEWSLETTERS	35
FIGURE 22: NEWSLETTER SUBSCRIBERS OVERVIEW (BREVO)	36
FIGURE 23: VIDEO VIEWS OVERVIEW (YOUTUBE)	37
FIGURE 24: VALUE PROPOSITION CANVAS USED FOR THE ANALYSIS OF STAKEHOLDER NEEDS, PAINS, GAINS, AND VALUE PROPOSITIONS ASSOCIATED WITH THE CURIUM KEY EXPLOITABLE RESULTS (ADAPTED FROM STRATEGYZER).	52
FIGURE 25 THE CURIUM PROJECT STANDARDIZATION STRATEGY STEPS.....	103
FIGURE 26 THE CRA CLUSTER MIRO BOARD WITH THE CURIUM PROJECT CONTRIBUTION	108
FIGURE 27: CURIUM CLUSTERING AND COLLABORATION FRAMEWORK	112

List of Tables

TABLE 1: PUBLICATIONS PRODUCED	29
TABLE 2: WHITE PAPER	30
TABLE 3: MAGAZINE ARTICLES	30
TABLE 4: ASSESSMENT OF RAISING AWARENESS OF CURIUM	39
TABLE 5: ASSESSMENT OF ENABLING KNOWLEDGE EXCHANGE	40
TABLE 6: ASSESSMENT OF MAXIMISING IMPACT OF CURIUM'S OUTPUTS AND EXPLOITATION	41
TABLE 7: ASSESSMENT OF BUSINESS GROWTH THROUGH PROJECT'S BENEFITS	41
TABLE 8: OVERVIEW OF THE CURIUM KEY EXPLOITABLE RESULTS (KERS) AND THEIR POSITIONING WITHIN THE CRA-ORIENTED COMPLIANCE LIFECYCLE.	49
TABLE 9: PSTVA (KER2) – INDICATIVE POST-PROJECT MILESTONES AND KPIS	71
TABLE 10: CYREA (KER3) – INDICATIVE POST-PROJECT MILESTONES AND KPIS	77
TABLE 11: DPRA (KER4) – INDICATIVE POST-PROJECT MILESTONES AND KPIS	82
TABLE 12: CAC (KER5) – INDICATIVE POST-PROJECT MILESTONES AND KPIS	88
TABLE 13: DPMA (KER6) – INDICATIVE POST-PROJECT MILESTONES AND KPIS	94
TABLE 14: OVERVIEW OF THE CURIUM CAPACITY BUILDING MATERIALS AND SERVICES PORTFOLIO ..	99
TABLE 15: OWNERSHIP OF THE CURIUM CAPACITY BUILDING MATERIALS AND SERVICES PORTFOLIO	101
TABLE 16: OVERVIEW OF CURIUM COLLABORATION AND NETWORKING INTERACTIONS	120
TABLE 17 SUMMARY OF KER RESPONSIBILITY AND POSSIBLE PATHWAYS.....	126

List of Abbreviations

Abbreviation	Description
AI	Artificial Intelligence
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
DIH	Digital Innovation Hub
DPMA	Digital Product Maturity Assessment
DPRA	Digital Product Risk Management
DSA	Digital Security Authority
ENISA	European Union Agency for Cybersecurity
ER	Exploitable Result
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCC	EU Cybersecurity Certification scheme
GA	Grant Agreement
GRC	Governance, Risk and Compliance
IEC	International Electrotechnical Commission
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
JTC	Joint Technical Committee
KER	Key Exploitable Result
KPI	Key Performance Indicator
NCSA	National Cybersecurity Authority
PSTVA	Penetration Self-Testing and Vulnerability Assessment (Services and Tools)
PU	Public (dissemination level)
SBOM	Software Bill of Materials
SDO	Standards Developing Organisation

1. Executive Summary

This deliverable, D5.2 – Final Report on Dissemination, Exploitation, Standardisation & Sustainability, presents the consolidated results of the CURIUM project's dissemination, communication, exploitation, standardisation and collaboration activities carried out throughout the project's lifetime, with particular focus on the second reporting period (July 2025 to September 2026). It builds upon and reports the implementation of the strategy and initial activities presented in Deliverable D5.1, monitors their performance against the Key Performance Indicators (KPIs) defined in the Grant Agreement, and presents the exploitation, standardisation and collaboration plans that will support the uptake and sustainability of CURIUM's results beyond the project's duration.

[Section 3](#) reports on the dissemination and communication activities implemented to raise awareness of the Cyber Resilience Act (CRA) and of the CURIUM Compliance Continuum among SMEs, industry, researchers, public authorities and standardisation bodies. These activities combined direct stakeholder engagement, through conferences, workshops, demonstrations and collaboration with other EU projects, with digital communication channels such as the project website, social media, newsletters and videos. The cumulative KPI assessment shows that the large majority of dissemination and communication targets were met or exceeded, including website visits, social media growth, newsletter production, publications and event participation.

[Section 4](#) presents CURIUM's exploitation strategy and the individual exploitation plans developed for the project's seven Key Exploitable Results (KERs): the CURIUM Compliance Continuum (KER1), the Penetration Self-Testing and Vulnerability Assessment tool (PSTVA, KER2), the CRA Scoping and Product Classification Service (CyReA, KER3), the Digital Product Risk Management service (DPRA, KER4), the Conformity Assessment and Compliance service (CAC, KER5), the Digital Product Maturity Assessment service (DPMA, KER6) and the CURIUM Capacity Building Plan and Services (KER7). For each KER, the deliverable defines target stakeholders, value propositions, exploitation approaches, ownership and IPR arrangements, cost and revenue considerations, and sustainability pathways beyond the project's duration, following a methodology based on the Value Proposition Canvas and aligned with the project's Grant and Consortium Agreements.

[Section 5](#) reports on the standardisation activities implemented under the project's step-wise standardisation strategy, including the identification of relevant standards and Standards Developing Organisations (SDOs), the provision of feedback on draft

CEN/CENELEC and ETSI standards related to the CRA, participation in standardisation working groups, and contribution to regulatory consultations.

[Section 6](#) presents CURIUM's collaboration and clustering activities, including its active participation in the CRA Cluster and its structured engagement with complementary EU-funded projects, national authorities and standardisation bodies, aimed at maximising the relevance, uptake and long-term impact of the project's results.

Overall, this deliverable demonstrates that CURIUM has successfully implemented a comprehensive and well-monitored strategy for disseminating its results, planning their exploitation, contributing to relevant standardisation efforts and building lasting collaborations across the European cybersecurity and CRA compliance ecosystem, thereby establishing solid foundations for the sustainability of the project's results beyond its lifetime.

2. Introduction

This document constitutes Deliverable D5.2 – Final Report on Dissemination, Exploitation, Standardisation & Sustainability of the CURIUM project (Grant Agreement No. 101190372), submitted under Work Package 5 (WP5) and led by APIROPLUS SERVICES LTD. (APIRO). It reports on the activities carried out under Task T5.1 (Dissemination and Communication), Task T5.2 (Impact Creation, Exploitation & Standardisation Activities) and Task T5.3 (Networking, Clustering and Collaboration), covering the full duration of the project and focusing in particular on the second reporting period, from July 2025 to September 2026.

This deliverable builds directly upon Deliverable D5.1 – Plan and Early Activities on Dissemination, Exploitation, Standardisation & Sustainability, which established the project's dissemination and communication strategy, the initial set of Exploitable Results (ERs), the Value Proposition Canvas methodology, and the standardisation and collaboration/clustering strategies. Rather than repeating that strategic groundwork, D5.2 focuses on reporting the implementation and results of these activities, and on consolidating them into concrete, forward-looking plans for the exploitation, standardisation and continued collaboration of CURIUM's results after the project's completion.

The remainder of this document is structured as follows. [Section 3](#) reports on the dissemination and communication activities implemented during the project and assesses their performance against the KPIs defined in the Grant Agreement. [Section 4](#) presents the methodology and individual exploitation plans developed for the project's seven Key Exploitable Results. [Section 5](#) reports on the standardisation-related activities performed under the project's step-wise standardisation strategy. [Section 6](#) presents the collaboration, networking and clustering activities undertaken with complementary EU projects, national authorities and standardisation organisations. [Section 7](#) concludes the deliverable with a synthesis of the results achieved across all four areas and an outlook on the sustainability of CURIUM's results beyond the project's lifetime.

3. Dissemination & Communication Activities

3.1 Introduction & Scope

Deliverable D5.2 reports on the dissemination and communication activities implemented during the second reporting period of the CURIUM project, covering **July 2025 to September 2026**. While the content up to Section 3.3.5 focuses primarily on activities undertaken during this reporting period, the achievements and KPI results presented from Section 3.3.6 onwards are **cumulative**, reflecting the overall implementation and performance of dissemination and communication activities throughout the entire project duration.

The activities reported in this section build on the Dissemination and Communication (D&C) strategy established in Deliverable D5.1 – *Plan and early activities on Dissemination, Exploitation, Standardisation & Sustainability*. D5.1 established the project's D&C objectives, target stakeholder groups, communication and dissemination channels, procedures and Key Performance Indicators (KPIs), and reported the initial activities undertaken during the first reporting period.

The present section therefore focuses on the implementation and results of dissemination and communication activities undertaken during the second reporting period, rather than reproducing the detailed strategy already presented in D5.1. The activities aimed to increase awareness of CURIUM and the Cyber Resilience Act (CRA), disseminate project results, promote the CURIUM Compliance Continuum and its tools and services, engage relevant stakeholder communities, and support the future uptake and exploitation of the project's results.

The activities addressed the stakeholder groups identified in D5.1, with particular emphasis on SMEs, industry and cybersecurity professionals, researchers, public authorities and policymakers, certification and standardisation actors, and relevant European cybersecurity initiatives.

Activities implemented under WP3 and WP4 also contributed to the project's dissemination, stakeholder-engagement and knowledge-transfer objectives. Training and capacity-building activities implemented under WP3, and validation activities implemented under WP4, are therefore briefly referenced where relevant. Their detailed implementation and results remain reported in **D3.2** and **D4.1** respectively. This approach avoids duplication while ensuring that their contribution to the overall dissemination and communication objectives is appropriately reflected.

The dissemination and communication activities were implemented in line with the Grant Agreement's objectives for raising awareness of CURIUM and its value to end-users and European SMEs, establishing mechanisms for knowledge transfer and exchange, promoting the project's tools and results through targeted events, and engaging policy and regulatory stakeholders.

3.2 Dissemination and Communication Approach During the Reporting Period

The implementation focused on four complementary objectives, reflecting the objectives established in D5.1:

- raising awareness of CURIUM, its objectives, activities and results, as well as the Cyber Resilience Act (CRA) and related cybersecurity compliance challenges;
- disseminating knowledge and project results, including tools and services developed by CURIUM, best practices, insights and methodologies;
- promoting stakeholder interaction and collaboration, through networking, knowledge-sharing and engagement with relevant European, national, scientific and industrial communities; and
- creating lasting impact and supporting the uptake of CURIUM results, including their future exploitation and contribution to a more secure and resilient digital environment.

The dissemination approach combined targeted activities for specific stakeholder groups with broader communication activities intended to increase project visibility. Conferences, exhibitions, workshops and demonstrations provided opportunities for direct interaction, while scientific publications and international magazine articles extended the reach of project knowledge. The project website, social media, newsletters, videos and promotional materials provided complementary channels for continuous communication.

3.3 Dissemination Activities

3.3.1 Collaboration with European Projects and Initiatives

Collaboration with other European projects and initiatives was an integral part of CURIUM's dissemination approach. Through participation in collaborative activities, CURIUM exchanged knowledge and good practices, identified synergies and common priorities, and extended the reach of its results to stakeholder communities beyond the project consortium. These activities also supported the positioning of the CURIUM Compliance Continuum and its tools within the wider European cybersecurity ecosystem, while creating opportunities for continued engagement, uptake and exploitation of the project results.

3.3.1.1 CYNERGY Event at Bucharest Tech Week

As part of Bucharest Tech Week 2026, held in Bucharest on 16 June 2026, CURIUM in collaboration with the CUSTODES Project engaged with stakeholders from research, industry, policymaking and innovation communities to discuss cybersecurity, digital resilience and the evolving European regulatory landscape.

The session “*Cyberproofing your Company: Tools & Tips*” (Figure 1) provided practical insights into the Cyber Resilience Act (CRA) and Cybersecurity Act (CSA), while

presenting the CURIUM Compliance Continuum and highlighting the complementary contribution of the CURIUM and CUSTODES projects in supporting organisations with practical approaches to cybersecurity compliance and resilience.

Through presentations and networking, the activity enabled CURIUM to present its objectives, tools and results to a wider stakeholder audience while raising awareness of the project's tools and results. With more than 50 participants, the event contributed to the project's exploitation activities.

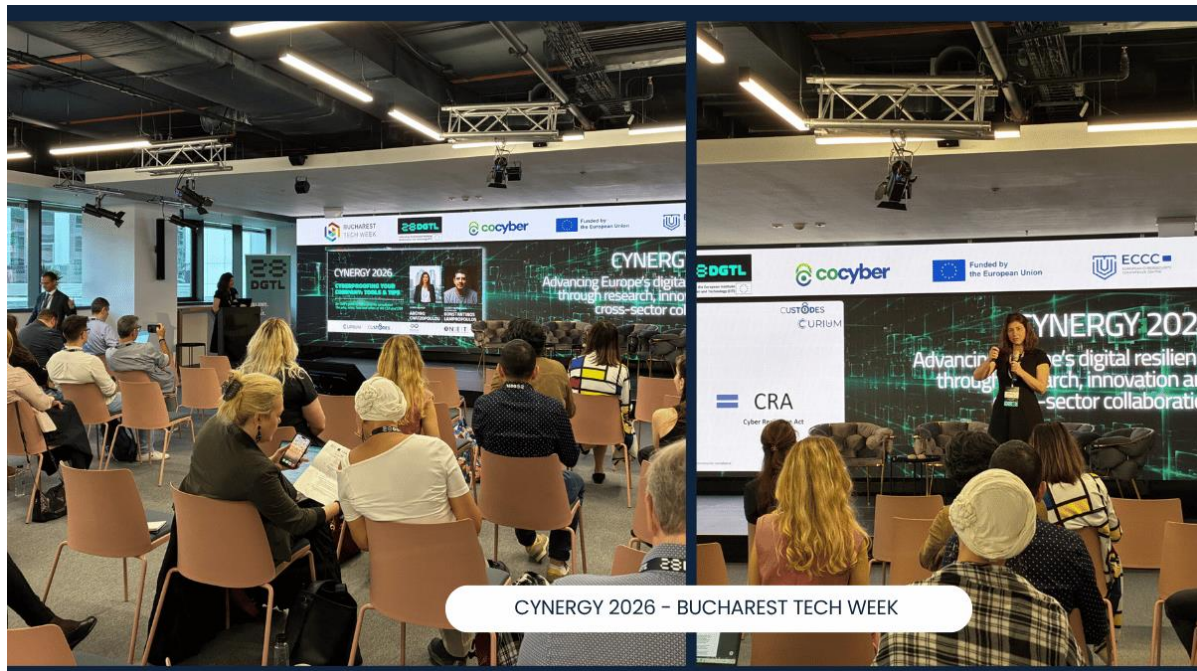


Figure 1: EU Cyber Resilience Workshop – “Cyberproofing your Company: Tools & Tips”

Link to CURIUM Website: [Strengthening Cyber Resilience at Bucharest Tech Week 2026 – Curium Project](#)

3.3.1.2 Open Validation with SMEs

On 28 January 2026, CURIUM in collaboration with the CUSTODES Project organised an Open Validation with SMEs in Paris (Figure 2). The activity brought CURIUM directly into contact with potential end-users and provided an opportunity to present and discuss the project's results in the context of cybersecurity and CRA compliance.

The activity combined dissemination with direct stakeholder engagement, allowing CURIUM to communicate its results while gaining insights into the needs and perspectives of SMEs and other potential users. It therefore supported both the visibility of the project results and their validation in a relevant stakeholder environment.



Figure 2: Open Validation with SMEs, Paris

Link to CURIUM website: [Validation Workshop with SMEs in Paris – Curium Project](#)

3.3.1.3 COcyber Concertation Workshop

The COcyber Concertation Workshop (Figure 3), held on 19 November 2025 at DIGITALEUROPE in Brussels and organised by AMETIC, brought together representatives of ten European cybersecurity projects, including CURIUM, with the objective of strengthening collaboration across Europe's cybersecurity and digital-trust ecosystem.

The workshop addressed common priorities and opportunities for cooperation in areas including networking and communication, policy alignment, knowledge and technology transfer, research and innovation, and skills and training. CURIUM's participation provided an opportunity to exchange knowledge and experience with complementary European initiatives, strengthen links with other projects and identify opportunities for further cooperation.



Figure 3: COcyber Concertation Workshop, Brussels

Link to CURIUM website: [COcyber Concertation Workshop at DIGITALEUROPE – Curium Project](#)

3.3.1.4 Participation in the “Building Cyber Resilience in the Digital Era” Event

CURIUM will be represented at the “Building Cyber Resilience in the Digital Era” event, taking place on Friday, 2 October 2026, at Electra Palace Athens, Greece. The event will bring together EU-funded cybersecurity projects and stakeholders to exchange knowledge and practical approaches to the evolving European cybersecurity regulatory landscape.

As part of the program, Leonidas Kallipolitis (AEGIS) will present the CURIUM CRA Support Continuum. The presentation will introduce the CURIUM project and its support approach for organisations seeking to understand and address the requirements of the Cyber Resilience Act (CRA).

The event will provide an opportunity to raise awareness of CURIUM among relevant cybersecurity stakeholders and facilitate exchange with other EU-funded projects addressing cybersecurity compliance, resilience and regulatory requirements.

3.3.1.5 Additional Collaboration with European Projects

CURIUM's engagement with the wider European cybersecurity ecosystem was further supported through a series of collaborative workshops, webinars and events undertaken as part of the project's training and capacity-building activities and reported in detail in **D3.2**.

These included the:

- Prepare Your SME for EU Cyber Rules webinar
- Cyber Resilience & Security Workshop at Techritory 2025
- Risk Assessment and Incident Response Workshop
- CRA & CSA: Mandatory Cybersecurity Requirements for Digital Products in the EU – The Deadline Is Approaching workshop at Patras IQ 2026
- EU AI Act and EU-Funded Research Projects webinar
- Cybersecurity through the Lens of EU Policies & Regulations webinar

Together, these activities enabled CURIUM to engage with complementary European initiatives and stakeholder communities while disseminating knowledge on the CRA, cybersecurity compliance and the project's results. At the same time, they provided opportunities for knowledge exchange and strengthened CURIUM's links with the wider European cybersecurity community.

3.3.2 Participation in the CRA Cluster and CRA Standards Unlocked EU Tour

As part of this broader engagement with the European cybersecurity community, CURIUM actively participated in the [CRA Cluster](#), an initiative bringing together EU-funded projects working on Cyber Resilience Act (CRA) compliance, tooling, guidance and standardisation.

Through representatives in Cluster's three core groups - Technical Interoperability, Standardization, and Training and Outreach - CURIUM contributed to discussions on CRA coverage and gaps, standardisation activities, and training and outreach approaches aimed at supporting SMEs and other organisations preparing for CRA implementation. The CURIUM Compliance Continuum and its tool owners also contributed their expertise to Cluster's technical activities.

CURIUM participated in the CRA Standards Unlocked – EU Tour (Figure 4), with its results presented at events in Zagreb (20 January 2026), Barcelona (26 March 2026), Malta (21 May 2026), Bucharest (24 June 2026) and Lisbon (17 September 2026). The tour brought together SMEs, industry representatives, standardisation experts, policymakers and European cybersecurity initiatives, providing a targeted setting for CURIUM to present its Compliance Continuum, project portal and supporting tools and engage with stakeholders on practical approaches to CRA compliance.

Across these activities, CURIUM strengthened the visibility of its results within the European CRA community and provided a consistent platform for communicating how its solutions can support organisations, particularly SMEs, in understanding and addressing CRA compliance requirements. The participation also enabled CURIUM to engage directly with stakeholders working on the practical implementation of the CRA and to raise awareness of the potential application of its results.

As part of the collaboration and dissemination activities with CYBERSTAND.eu, a direct link to the CURIUM Portal was added to the CURIUM project page on the [CYBERSTAND.eu website](https://cyberstand.eu) in September 2026, providing visitors with direct access to the CURIUM Portal and its available resources and tools.

This action further increased the visibility and accessibility of CURIUM results beyond the project's own communication channels, supporting wider outreach to stakeholders interested in the Cyber Resilience Act (CRA) and cybersecurity.

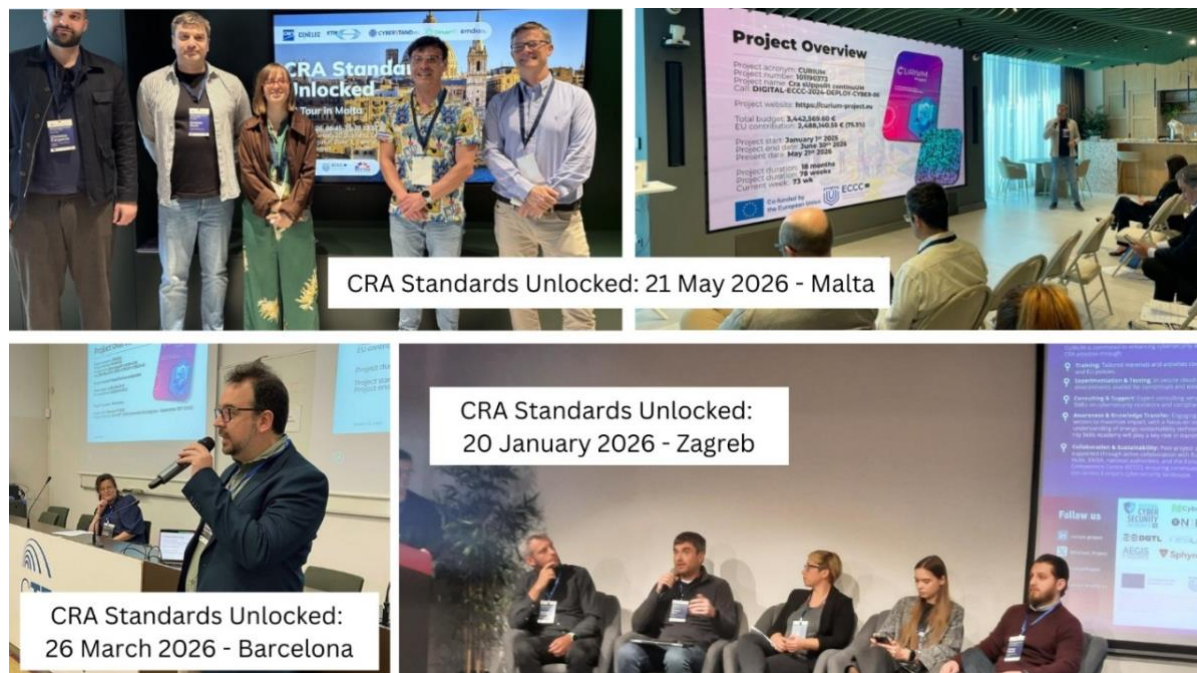


Figure 4: CRA Standards Unlocked – EU Tour

Links to CURIUM website:

- [CURIUM Presented at the CRA Standards Unlocked EU Tour in Bucharest – Curium Project](#)
- [CURIUM Presents Compliance Continuum at CRA Standards Unlocked Event in Malta – Curium Project](#)
- [CURIUM Participates in CRA Standards Unlocked – EU Tour in Barcelona – Curium Project](#)
- [CRA Standards Unlocked Event in Zagreb – Curium Project](#)
- [CURIUM at CRA Standards Unlocked – EU Tour in Lisbon – Curium Project](#)

3.3.3 Participation in the CyberHubs European Network

CURIUM's engagement with European initiatives extended beyond the CRA-focused activities described above through its participation in the [CyberHubs – the European Network of Cybersecurity Skills Hubs](#) as an Associated Project. The network brings together industry, academia, policymakers and training providers across seven European countries, with a focus on strengthening cybersecurity skills and knowledge sharing. Through its association with CyberHubs, CURIUM expanded its opportunities

to exchange expertise, promote skills development initiatives and further disseminate its project results, contributing to a stronger European cybersecurity ecosystem.

3.3.4 Conference & Scientific Events

CURIUM participated in international conferences and scientific workshops to disseminate its research and technical results and engage with the wider European cybersecurity and research community. These activities provided opportunities to present CURIUM's work, share emerging approaches to cybersecurity compliance and resilience, and connect with researchers and practitioners working on related technical and regulatory challenges.

3.3.4.1 IEEE CSR Workshop on Information & Operational Technology Security (IOSEC)

The 2026 IEEE CSR Workshop on Information & Operational Technology Security (IOSEC) took place in Lisbon (Figure 5), Portugal, from 3 to 5 August 2026, in conjunction with the IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2026). The workshop brought together researchers and practitioners addressing emerging challenges and solutions in Information Technology (IT) and Operational Technology (OT) security, including security architectures, vulnerability and risk management, cybersecurity certification, threat intelligence, intrusion detection and secure software development.

CURIUM was among the EU-funded projects supporting the workshop, alongside other cybersecurity research initiatives. Participation increased the project's visibility within the European cybersecurity research community and strengthened connections with researchers and practitioners working on cybersecurity, resilience and compliance.



Figure 5: IEEE CSR Workshop on Information & Operational Technology Security (IOSEC), Lisbon

Link to CURIUM website: [CURIUM at IOSEC 2026: Strengthening Cyber Resilience and CRA Awareness – Curium Project](#)

3.3.4.2 LIFESEC Workshop / IEEE SmartComp 2026

The LIFESEC Workshop, held in conjunction with IEEE SmartComp 2026 (Figure 6), provided an additional opportunity to communicate CURIUM results within the European research and cybersecurity community. The workshop addressed themes relevant to CURIUM, including whole-lifecycle security, automated compliance and European cybersecurity regulations.

The activity complemented the project's wider awareness-raising and stakeholder-engagement efforts by connecting CURIUM's work with broader discussions on cybersecurity and regulatory compliance.



Figure 6: LIFESEC Workshop / IEEE SmartComp 2026

Link to CURIUM website: [International Conference on Engineering, Technology and Innovation \(ICE IEEE/ITMC\)](#)

CURIUM participated in the International Conference on Engineering, Technology and Innovation (ICE IEEE/ITMC) (Figure 7), held in Porto, Portugal, from 22 to 25 June 2026. Kristian Ravic presented the paper “Ontology-driven Compliance Reasoning for the EU Cyber Resilience Act: A Proof-of-Concept”, which explored how automated pre-market conformity triage can be facilitated by bridging unstructured technical documentation with the formal symbolic logic required for regulatory satisfiability.

The presented work introduced the OntoCRA-NS concept, developed through collaboration between the CURIUM and CUSTODES projects. The activity demonstrated CURIUM's contribution to research on innovative approaches to cybersecurity

compliance and regulatory readiness, while also highlighting the value of cross-project collaboration in advancing technical solutions to emerging regulatory requirements.

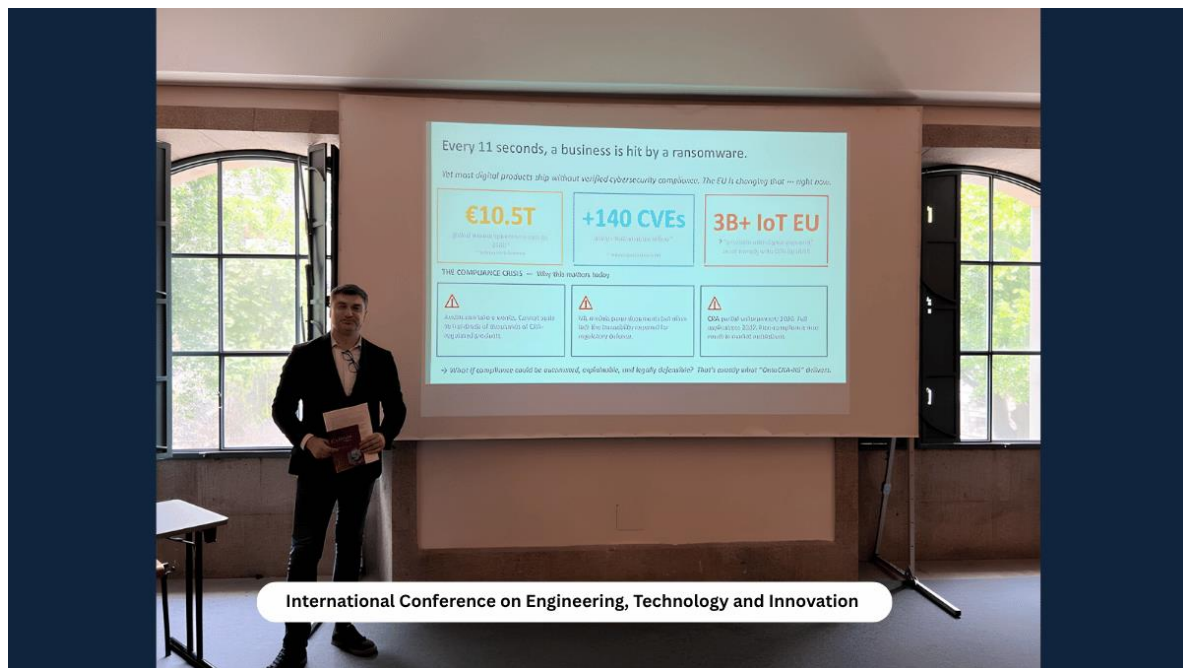


Figure 7: International Conference on Engineering, Technology and Innovation (ICE IEEE/ITMC 2026), Porto

Link to CURIUM website: [CURIUM participates in the International Conference on Engineering, Technology and Innovation \(ICE IEEE/ITMC\) – Curium Project](#)

3.3.5 Awareness-Raising & Stakeholder Engagement

Building on its participation in international conferences and scientific workshops, CURIUM also undertook a broader range of awareness-raising and outreach activities through exhibitions, workshops and other relevant events. These activities provided opportunities to extend the dissemination of CURIUM's work beyond the scientific community, raise awareness of the Cyber Resilience Act (CRA) and its implications, present the project's results and solutions, and engage directly with stakeholders across the cybersecurity, research, innovation, industry and public sectors.

3.3.5.1 BEYOND Expo 2026

At BEYOND Expo 2026 (Figure 8), held in Athens from 17 to 19 June 2026, CURIUM was showcased through practical demonstrations that enabled visitors to interact with the project's tools and discuss their relevance to cybersecurity and regulatory compliance.

A dedicated demonstration delivered by APIROPLUS SERVICES introduced visitors to the CURIUM tools through live demonstrations and provided information on how the project supports organisations in preparing for and addressing Cyber Resilience Act (CRA) requirements. The activity provided a direct means of demonstrating the practical application of the CURIUM tools to an external audience and further communicating the

relevance of the project's results. The validation dimension of this activity is described in D4.1.

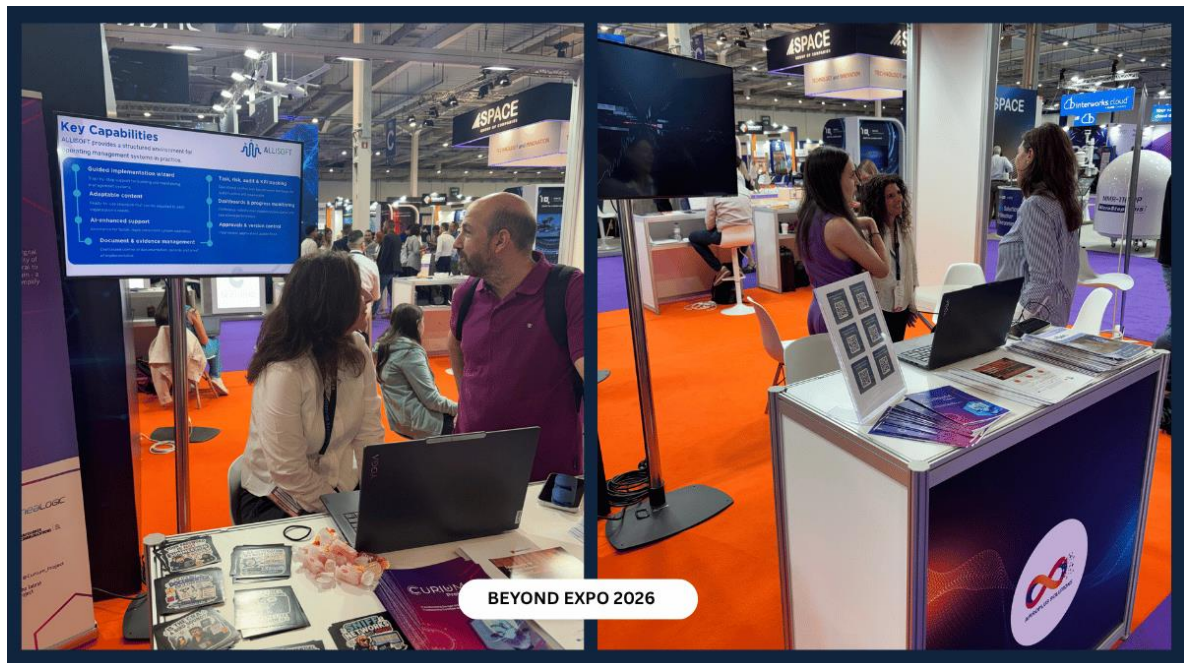


Figure 8: BEYOND Expo 2026, Athens

Link to CURIUM website: [BEYOND Expo 2026 – Curium Project](#)

3.3.5.2 Skills for Digital Autonomy: Empowering a Resilient Society

At Skills for Digital Autonomy: Empowering a Resilient Society (Figure 9), held in Cyprus on 5 June 2026, CURIUM was presented through a dedicated booth offering information and hands-on testing opportunities. The activity enabled direct engagement with policymakers, academics, industry representatives and cybersecurity experts.

The event provided an opportunity to communicate the project's objectives and practical solutions to a diverse stakeholder audience, while allowing participants to explore the CURIUM approach to cybersecurity resilience and CRA compliance. The validation dimension of this activity is described in D4.1.

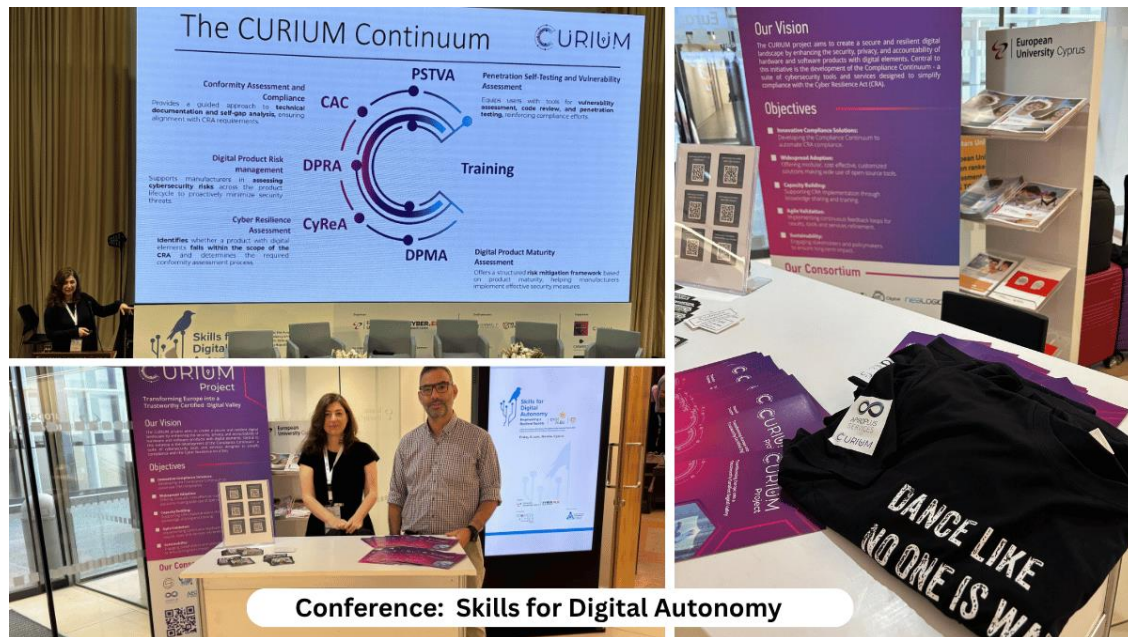


Figure 9: Skills for Digital Autonomy: Empowering a Resilient Society, Cyprus

Link to CURIUM website: [CURIUM participates in Conference “Skills for Digital Autonomy” in Nicosia – Curium Project](#)

3.3.5.3 South Summit Madrid 2026

In June 2026, 28DIGITAL represented CURIUM at South Summit Madrid 2026 (Figure 10), engaging with startups, SMEs, investors and technology leaders from across Europe.

Through a dedicated CURIUM booth, the project presented its approach to strengthening cybersecurity resilience and supporting organisations in preparing for the requirements of the Cyber Resilience Act (CRA). Direct discussions with visitors provided an opportunity to present CURIUM’s approach and engage with stakeholders from the innovation and technology communities on cybersecurity, compliance and digital trust.



Figure 10: South Summit Madrid 2026

Link to CURIUM website: [South Summit Madrid 2026 – Curium Project](#)

3.3.5.4 Patras IQ 2026

CURIUM had a visible presence at Patras IQ 2026 (Figure 11), held in Patras from 27 February to 1 March 2026. p-NET hosted a dedicated CURIUM booth, where project materials and the promotional banner were displayed and consortium representatives engaged directly with visitors, including students, researchers, industry representatives, regional authorities and members of the wider innovation ecosystem.

In addition, p-NET organised the workshop “CRA & CSA: Mandatory Cybersecurity Requirements for Digital Products in the EU – The Deadline Is Approaching” on 28 February 2026. As described in D3.2, the workshop raised awareness of forthcoming regulatory requirements and demonstrated the relevance of CURIUM's results to organisations preparing for the implementation of the CRA.



Patras IQ 2026 [Exhibition booth]: 27 February - 1 March 2026 - Patras

Figure 11: Patras IQ 2026

Link to CURIUM website: [Patras IQ 2026, CRA & CSA: Mandatory Cybersecurity Requirements for Digital Products in the EU – The Deadline Is Approaching – Curium Project](#)

3.3.5.5 AI Enables Cybersecurity Event

On 14 January 2026, CURIUM was presented at the AI Enables Cybersecurity (Figure 12) event held at OTE headquarters in Athens, in the context of the Vigilance and CyberAid kick-off meetings. Participants were introduced to CURIUM's solutions and to the CURIUM Compliance Continuum, including its role in supporting organisations and SMEs in navigating CRA compliance requirements.



Figure 12: AI Enables Cybersecurity Event, Athens

Link to CURIUM website: [CURIUM participates in AI Enables Cybersecurity Event – Curium Project](#)

3.3.5.6 ISACA Athens Chapter Conference

On 4 December 2025, CURIUM participated in the ISACA Athens Chapter Conference 2025 – Decoding Digital Trust (Figure 13), held at the OTE Academy in Athens. The event provided an opportunity to present CURIUM and demonstrate its tools and services supporting CRA compliance.

A dedicated booth enabled direct interaction with stakeholders interested in strengthening cybersecurity resilience and regulatory preparedness, extending awareness of the project's results among the professional cybersecurity community.

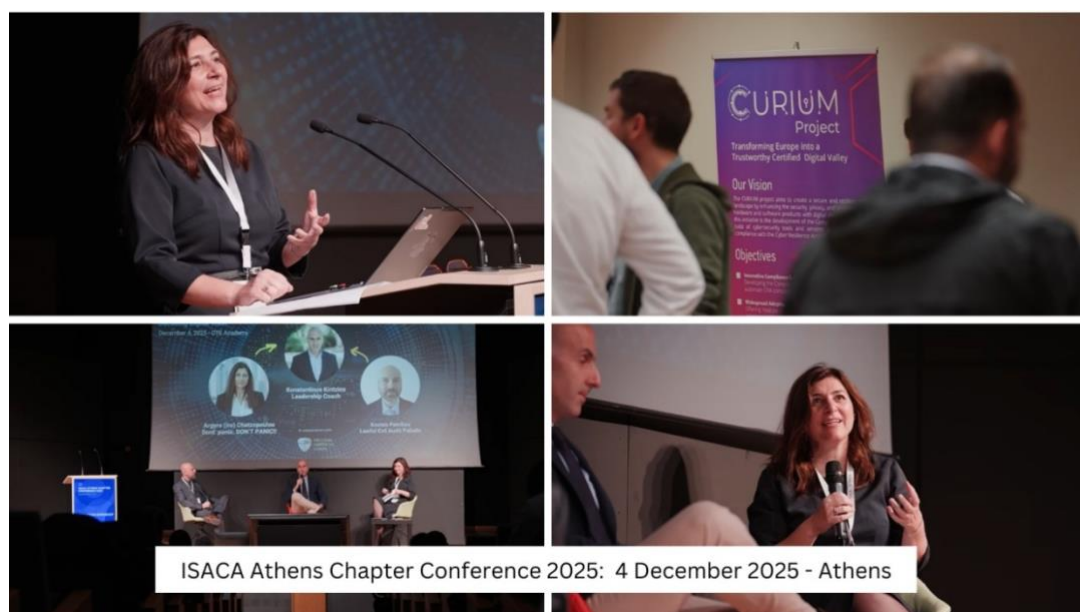


Figure 13: ISACA Athens Chapter Conference 2025

Link to CURIUM website: [CURIUM at ISACA Athens Chapter Conference 2025 – Curium Project](#)

3.3.5.7 Cybersecurity Career Fair

The Cybersecurity Career Fair (Figure 14) was held in Nicosia, Cyprus, on 25 - 26 November 2025 as part of the European Cybersecurity Month initiative and aimed to bring high school students, as well as the wider public into direct contact with the academic and professional world of Cybersecurity, highlighting study pathways and career opportunities in a field of growing importance. Organisations, companies and institutions active in the Cybersecurity sector in Cyprus participated in the Career Fair, offering information on job openings, internships, training opportunities and the skills required in today's labour market.

CURIUM participated through a dedicated information booth, introducing visitors to the project's objectives, activities and tools supporting cyber resilience, capacity building and cybersecurity awareness.

The event provided an additional channel for engaging with the cybersecurity community and communicating the practical relevance of CURIUM's results to individuals and organisations interested in cybersecurity.



Figure 14: Cybersecurity Career Fair, Nicosia

Link to CURIUM website: [Cybersecurity Fair in Nicosia, Cyprus – Curium Project](#)

3.3.5.8 Cyber Resilience Act: Obligations in the Supply Chain

On 17 October 2025, the Digital Security Authority of Cyprus organised the event “Cyber Resilience Act (CRA): Obligations in the Supply Chain” (Figure 15). The event examined the obligations introduced by the CRA and their implications for manufacturers, importers, distributors and other stakeholders involved in the supply chain of products with digital elements.

CURIUM was presented as an initiative supporting awareness, training and capacity building related to CRA implementation, helping stakeholders understand the relevance of the new regulatory requirements and the resources available to support compliance.



CRA Act: Obligations in the Supply Chain event: 17 October 2025 - Nicosia

Figure 15: Cyber Resilience Act (CRA): Obligations in the Supply Chain event, Cyprus

Link to CURIUM website: [CRA: Obligations in the Supply Chain – Curium Project](#)

3.3.6 Training and Capacity Building

Building on the awareness-raising and outreach activities described above, CURIUM also implemented a range of training and capacity-building activities aimed at strengthening stakeholders' practical understanding of the Cyber Resilience Act (CRA), cybersecurity risk assessment, incident response, SME preparedness and related European regulatory developments. These activities complemented the project's dissemination efforts by providing opportunities for stakeholders to develop practical knowledge and engage more directly with the topics addressed by CURIUM.

A dedicated CRA Compliance and Awareness training program was developed and delivered through the Sphynx Cyber Range. To support continued access to the training material, a shortened version of the program was also integrated into the CURIUM Compliance Continuum Portal.

Training and knowledge transfer were also supported through three internal training sessions delivered to project partners and relevant staff. These sessions familiarised participants with the CURIUM tools and supported knowledge transfer within the consortium, helping partners to communicate and demonstrate the project's results consistently.

The training and capacity-building activities were complemented by a series of workshops and webinars addressing specific aspects of cybersecurity compliance and the evolving European regulatory landscape. Further details on these activities, including their implementation and results, are provided in **D3.2**.

Together, these activities supported CURIUM's objective of building practical knowledge and capacity among SMEs, cybersecurity professionals and other relevant stakeholders.

3.3.7 Validation Activities and Stakeholder Engagement

Validation activities provided an additional channel for stakeholder engagement by enabling potential users and other relevant stakeholders to interact directly with the CURIUM Compliance Continuum and its tools. Beyond supporting the technical and user-oriented validation of the project results, these activities provided opportunities to gather user feedback, assess the practical relevance of the solutions and identify areas for further refinement.

Validation was carried out through a range of workshops and stakeholder engagement activities, involving direct interaction with the CURIUM tools in different contexts. This provided valuable feedback on the usability and relevance of the solutions and helped assess their potential application by different types of users.

The validation process complemented the project's dissemination and communication activities by creating direct engagement between the project results and potential users. It also generated practical input to support the further refinement and future uptake of the CURIUM tools and services.

The validation methodology, stakeholder participation, user feedback and assessment of the results are reported in detail in **D4.1**.

3.3.8 Scientific Publications and Magazine Articles

Scientific publications provided an important channel for disseminating the technical knowledge and research results generated by CURIUM and for reaching the wider cybersecurity and research community.

During the project, the consortium produced five scientific publications (Table 1). The publications addressed key areas relevant to CURIUM, including explainable and auditable cybersecurity compliance, dynamic cybersecurity risk assessment, cyber-insurability and automated certification frameworks. To support continued access to the project's scientific outputs, all five publications were made publicly available through Zenodo. This ensures that the research results remain accessible to the scientific and professional communities beyond the lifetime of the project.

Authors	Title	Journal / Conference
Jasmin Cosic, Miroslav Baca	Ontology-driven Compliance Reasoning for the EU Cyber Resilience Act: A Proof-of-Concept (Manuscript)	ICE IEEE/ITMC Conference (ICE2026)
Jasmin Cosic, Admir Jukan, and Miroslav Baca	OntoCRA-NS: A Neuro-Symbolic Framework for Explainable and Auditable Cybersecurity Compliance Aligned with EU Regulatory Frameworks	IEEE CAI 2026
Shareeful Islam, Bilal Sardar, Eleni Maria Kalogeraki, Kostas Lampropoulos, Spyridon Papastergiou	Hybrid AI-Based dynamic risk assessment framework with explainable AI practices for composite product cybersecurity certification	International Journal of Information Security
Spyridon Papastergiou, Nihala Basheer, Kostas Lampropoulos, Panayiotis Verrios, Shareeful Islam	Explainable AI based dynamic cybersecurity risk management for cyber insurability	International Journal of Information Security
Jasmin Cosic et.al.	Towards Automated Certification Framework of Composite Systems: A SWRL-Based Approach	2025 IEEE International Conference on Engineering, Technology and Innovation

Table 1: Publications produced

The project also produced a White Paper on the “Comparative Analysis of the Cybersecurity Incident Responder Role Across Frameworks” (Table 2), developed in collaboration with CyberSecPro. In addition, CURIUM partners contributed to four international magazine articles (Table 3) addressing cybersecurity compliance, the Cyber Resilience Act, explainable and auditable AI for cyber resilience, and cybersecurity-related activities undertaken by project partners.

White Paper produced by	Title
CURIUM & CyberSecPro	Comparative Analysis of the Cybersecurity Incident Responder Role Across Frameworks

Table 2: White Paper

Authors	Title	Magazine
Federico Guerrini	Securing Europe's Digital Future: 28DIGITAL's Work in Cybersecurity	28 DIGITAL / News
Miroslav Baca, Jasmin Cosic	When Compliance Meets Intelligence: Why Europe Needs Explainable and Auditable AI for Cyber Resilience	28 DIGITAL / News
Bilal Sardar, Shareeful Islam, Argyro Chatzopoulou	Trustworthy AI: Navigating Conformity with the EU Cyber Resilience Act	Cyber Security Magazine
Athanasios Staveris-Polykalas	Turning the EU Cyber Resilience Act into Operational Cyber Defence	Cyber Defense Magazine [pages 288 – 291]

Table 3: Magazine articles

3.3.9 Policy and Regulatory Stakeholder Engagement

Engagement with policy and regulatory stakeholders formed an important part of CURIUM's dissemination activities, supporting the project's objective of increasing awareness and understanding of the Cyber Resilience Act (CRA) and its implications for organisations.

The National Cybersecurity Authority (NCSA) and the Digital Security Authority (DSA) played an important role in supporting this engagement by bringing their expertise and established links with relevant policy and regulatory communities into the project. Their involvement provided CURIUM with opportunities to communicate the project's objectives, tools and results to policymakers, national and regional authorities, regulatory agencies and other relevant European stakeholders, while also facilitating knowledge exchange on cybersecurity resilience, regulatory compliance and CRA implementation.

Through their involvement in CURIUM, NCSA and DSA contributed to strengthening the project's connections with the policy and regulatory environment surrounding the CRA. This engagement supported the wider dissemination of CURIUM's results and their potential uptake, particularly among stakeholders involved in understanding and implementing the evolving European cybersecurity regulatory framework. In addition, with the interaction and collaboration with the projects, of AKADIMOS and secure4sme, the two projects which are represented by national authorities, NCCs, EDIHs, standardization organizations, the technical partners had the opportunity to present the CURIUM platform and the solutions on CRA to relevant partners. The videos for the use of the tools were presented to the projects' representatives and creative feedback was collected on the use of the tools. All related material was provided to the secure4sme project, for use within the scope of the project and for outreach purposes of the tools.

3.4 Communication Activities

3.4.1 Project Website

The CURIUM website served as the project's central digital communication and dissemination hub throughout the project. It provided information on the project, its objectives and activities and offered access to project results, publications, events, newsletters, videos and other dissemination materials.

Figure 16 Figure 17 In 2025, the CURIUM website recorded 2,352 sessions (website visits) from 1,494 users. Users viewed an average of 1.85 pages per session, with an average session duration of 3 minutes and 10 seconds.

While from 1 January to 25 September 2026, the website recorded 4,018 sessions (website visits) from 2,401 users. The average number of views per session was 1.70, while the average session duration was 3 minutes and 11 seconds.

The 2026 figures show a substantial increase in website traffic, with the number of visits already approximately 71% higher than the total recorded for the full 2025 calendar year, despite the 2026 reporting period covering only the first nine months of the year. This demonstrates growing visibility of and engagement with the CURIUM website during the project's final year.

In addition, the website generated **236 brochure downloads** and **492 downloads of dissemination materials**, demonstrating continued interest in the project's activities and results.

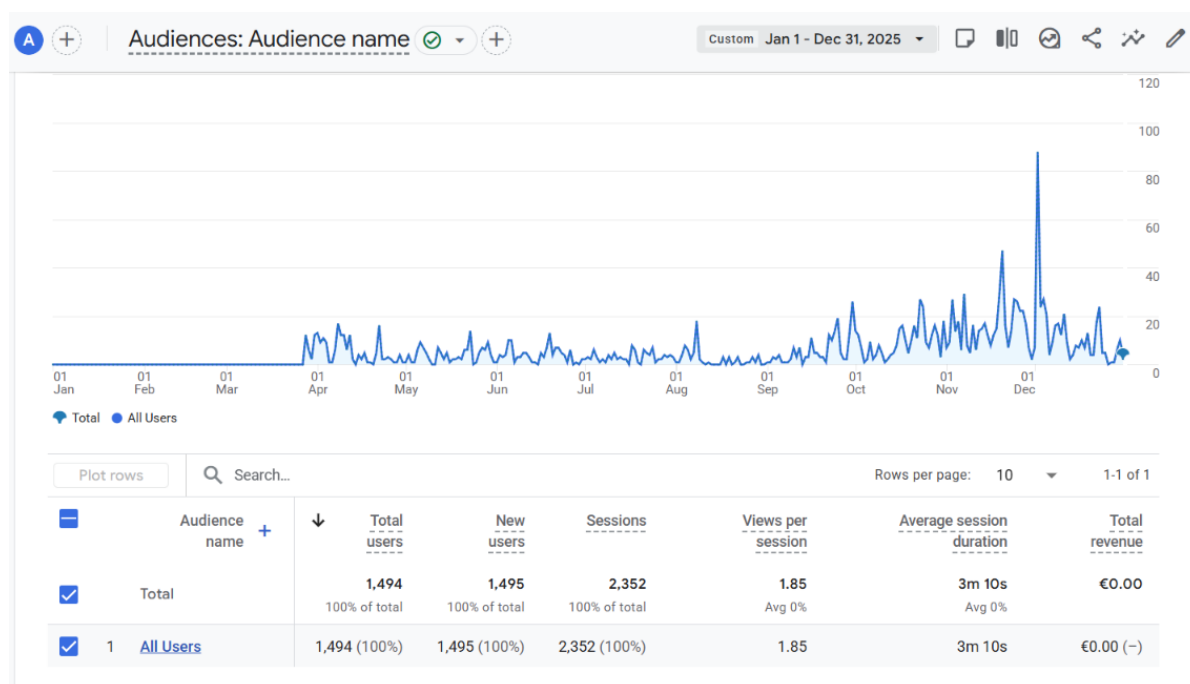


Figure 16: CURIUM GA4 Analytics – Website Visits 2025

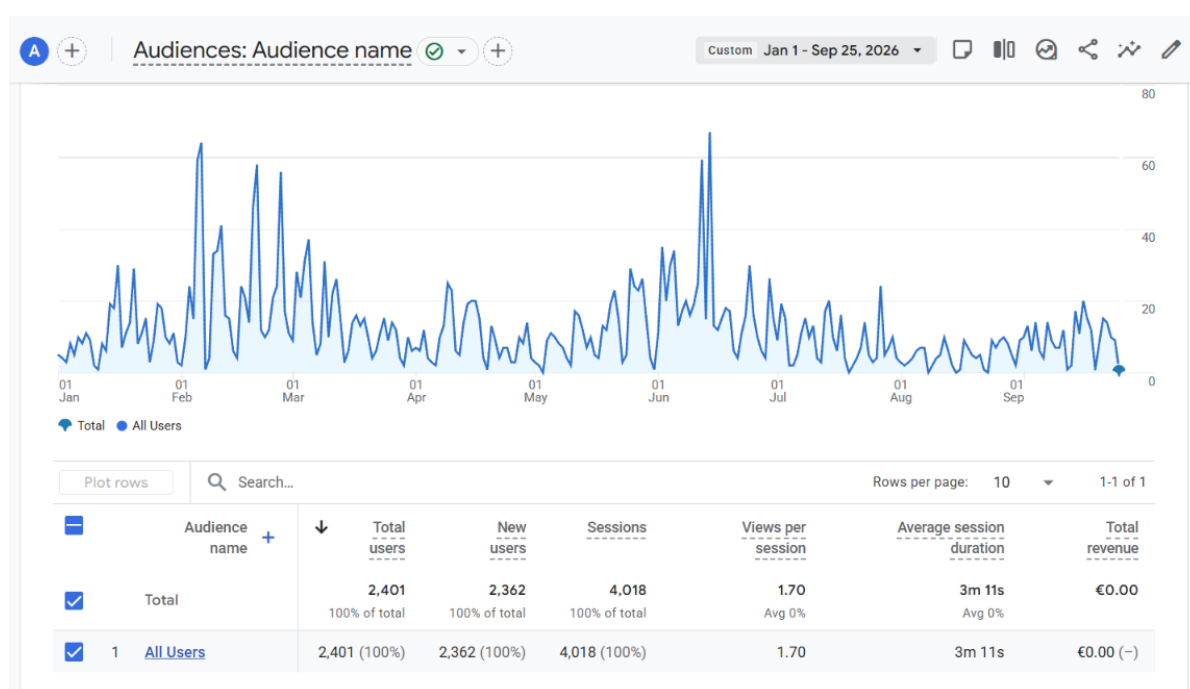


Figure 17: CuriumGA4 Analytics – Website Visits 2026

The website will remain available beyond the project's lifetime, supporting continued access to CURIUM results, publications and dissemination materials.

3.4.2 Social Media

Social media supported the project's visibility, event promotion, dissemination of results and stakeholder engagement, where the project maintained an active presence through **LinkedIn** and **YouTube**.

Content included project news, event announcements, , workshops, demonstrations, videos and partner activities. LinkedIn polls were also used to stimulate discussion and obtain stakeholder perspectives on cybersecurity, regulatory compliance and emerging digital-policy issues.

LinkedIn analytics provide follower growth data for the most recent 365 days. The available export covers 27 September 2025 to 26 September 2026, during which the CURIUM LinkedIn page gained 257 followers. This represents an average of approximately 22 followers per month, exceeding the KPI target of more than 5 per month. The page has 395 followers in total.

The audience data indicate that CURIUM is reaching professional communities relevant to the project. Followers work in sectors including IT services and consulting, software development, higher education, telecommunications, and computer and network security. The data also show reach into smaller organisations: 199 followers are associated with companies employing 2–200 people.

Figure 18

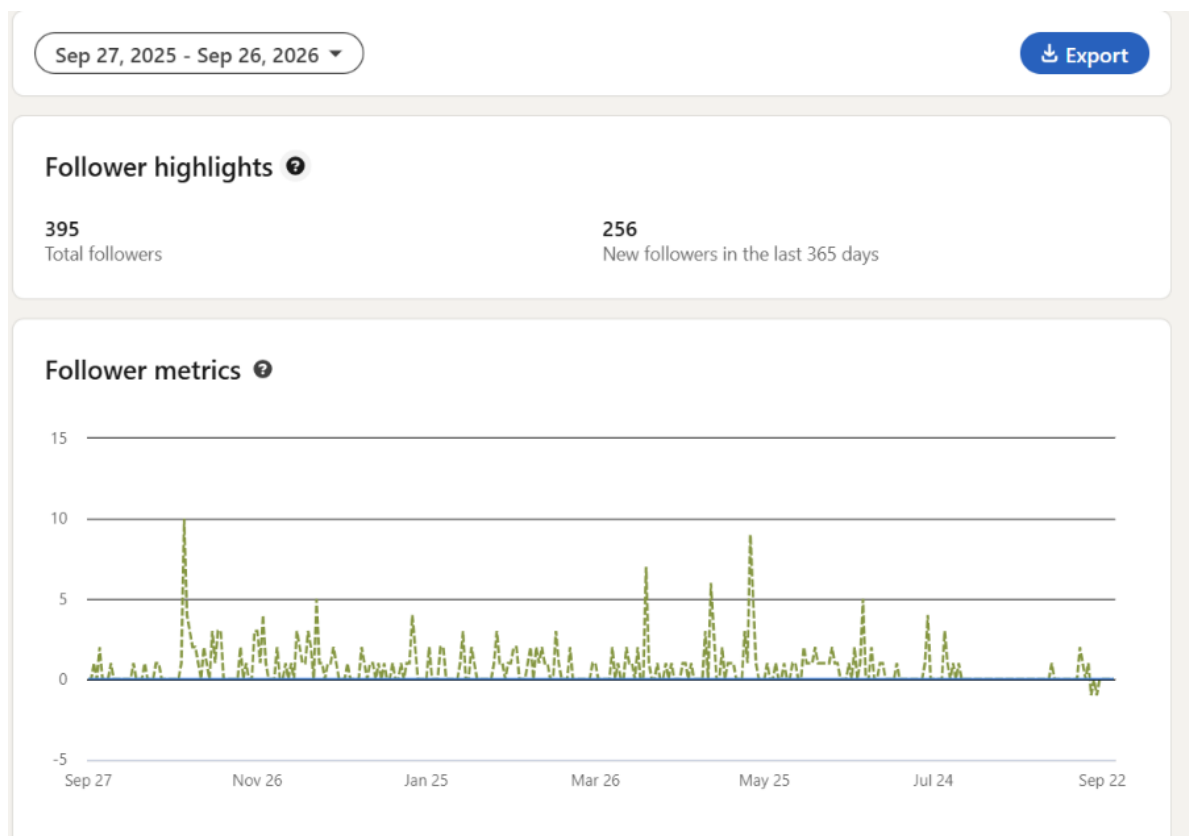


Figure 18: LinkedIn Analytics – Follower Growth

During the same period, the page generated **52,138 impressions, 2,642 reactions, and 58 comments**. These figures demonstrate continued growth of the project's audience and engagement with the content disseminated through the channel.

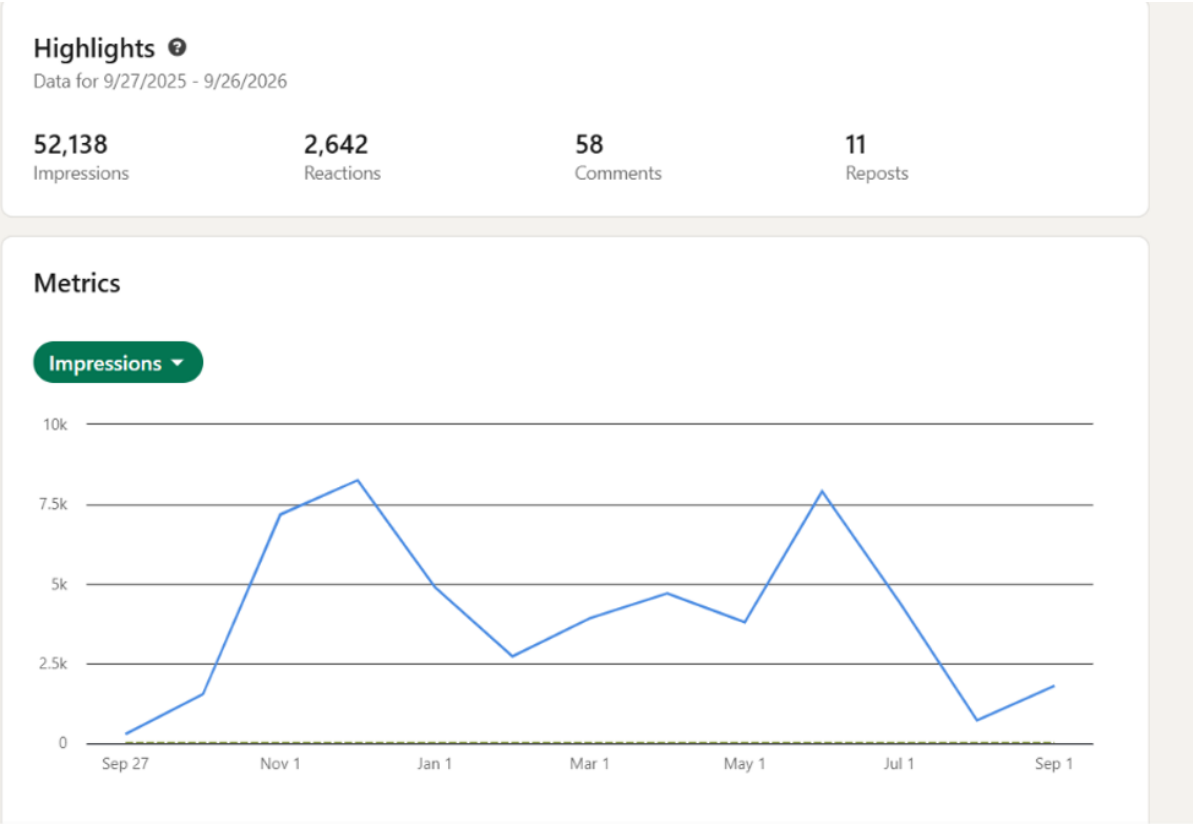


Figure 19: LinkedIn Analytics – Impressions

38 posts were posted on LinkedIn during 2025, whereas from January 2026 to 25 September 2026, a total of **61 posts** were published. **Error! Reference source not found.**

The KPI of ≥ 20 new LinkedIn discussions initiated to stimulate two-way knowledge exchange has been achieved. For the purpose of measuring this KPI, discussions were generated through CURIUM’s LinkedIn activities, including dedicated poll/question-based posts specifically designed to encourage audience participation and knowledge exchange around CRA-related topics, as well as interactions and discussions arising from other project posts. Through these activities, CURIUM encouraged interaction and two-way engagement with its audience. This KPI is also discussed in **D3.2 (Section 7.2.6)**, which provides further details on the related communication and engagement activities.

3.4.3 Newsletters

Electronic newsletters distributed through the **Brevo** platform provided a direct communication channel for maintaining contact with the CURIUM stakeholder community and disseminating project developments, activities and results.

During the project period, **four project newsletters** were produced:

- **August 2025:** introduced the project and the CURIUM Compliance Continuum, including the tools and services being developed to support organisations in addressing CRA requirements;
- **December 2025:** provided an overview of project activities and achievements, including workshops, webinars, stakeholder engagement and developments related to CRA implementation; and
- **June 2026:** focused on the CURIUM Portal and the availability and practical relevance of the project's tools and services.
- **September 2026:** focused on the final phase of the project, highlighting validation activities and real-world testing of the CURIUM Portal, scientific workshops, collaboration with the wider CRA community, and the continued availability of CURIUM's tools and resources beyond the project's conclusion.

The newsletters provided a direct communication channel to stakeholders who had expressed an interest in the project and helped maintain awareness of CURIUM activities and results. (Figure 20)



Figure 20: CURIUM Project Newsletters

Link to CURIUM website: [Newsletters – Curium Project](#)

The number of subscribers on Brevo amounts to 514 against the KPI target of at least 500 recipients. (Figure 21)

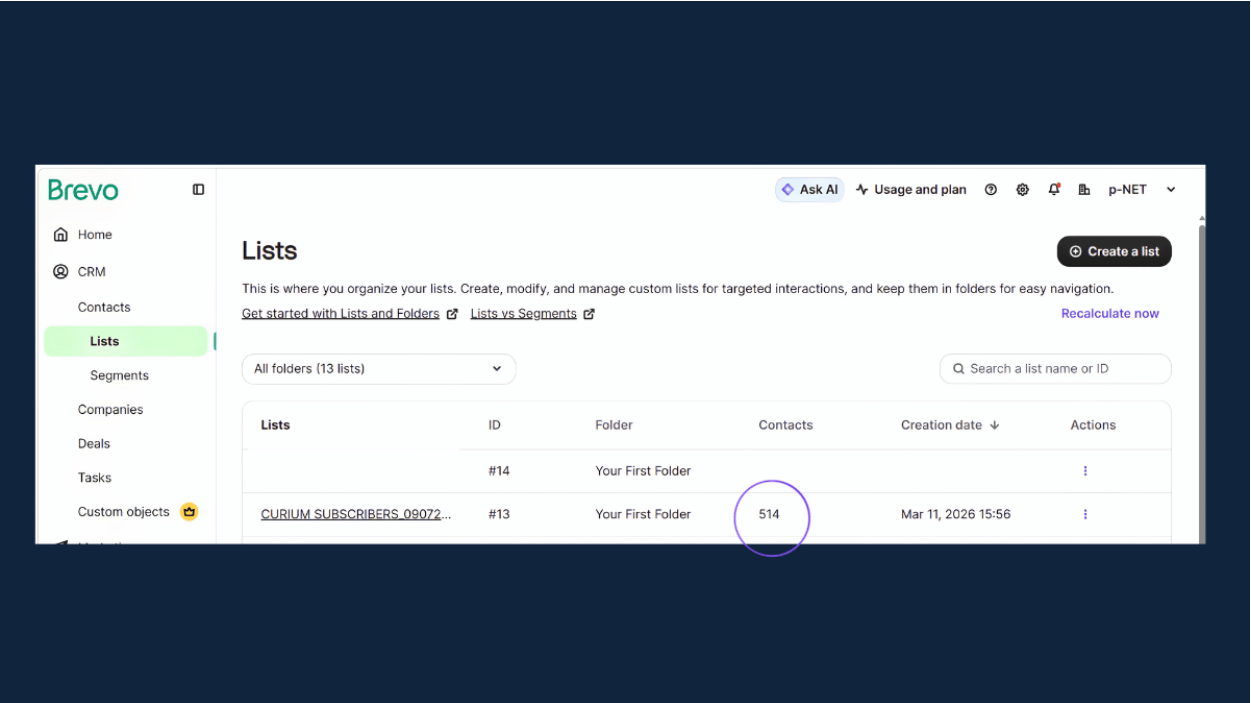


Figure 21: Newsletter Subscribers Overview (Brevo)

3.4.4 Videos

Video-based communication supported the dissemination of CURIUM's objectives, tools and results through an accessible and reusable format.

During the project, the CURIUM YouTube channel was used to publish and promote webinar recordings, event presentations, awareness-raising content, demonstrations and other multimedia material. (Figure 22)

The consortium developed **five video demonstrators**, exceeding the Grant Agreement target of at least four.

The demonstrator material was subsequently consolidated into a comprehensive video presenting the end-to-end journey towards CRA compliance. The comprehensive video illustrates key stages of the CURIUM Compliance Continuum, including determining CRA applicability, assessing cybersecurity risks, improving cybersecurity maturity, validating security measures and generating evidence required for conformity assessment and CE marking.

The available project records report 1048 views for the video material. The videos constitute reusable dissemination assets that remain available for continued viewing and promotion beyond the project period.

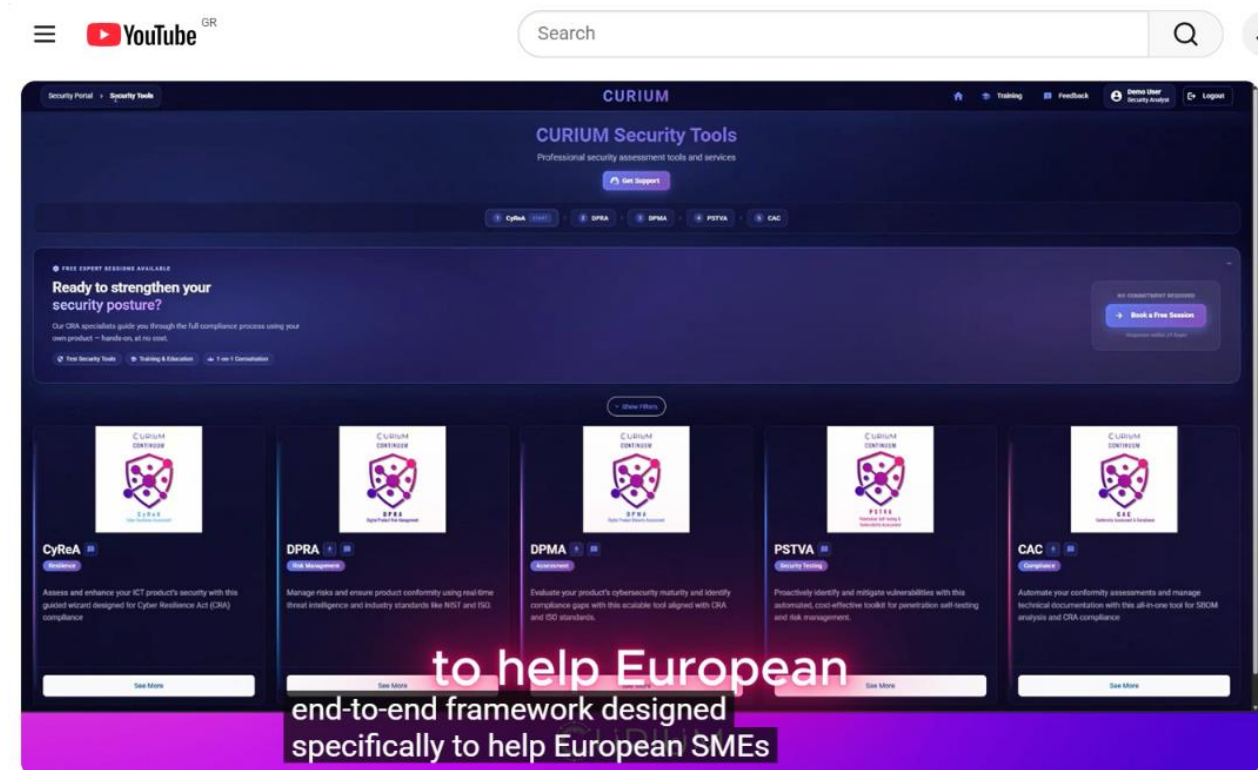


Figure 22: Video Views Overview (YouTube)

Link to CURIMUM's YouTube channel: [Curium Project - YouTube](#)

Link to CURIMUM's website: [Videos – Curium Project](#)

3.4.5 Promotional Material and Outreach

Promotional material supported the project's communication and awareness-raising objectives.

Project brochures, banners and other dissemination materials were used at conferences, workshops, exhibitions and stakeholder events, while electronic versions were made available through the project's digital channels.

A total of **236 brochure downloads** were recorded, while **354 hard-copy brochures** were distributed during project events and stakeholder-engagement activities. Project banners were also displayed at conferences, exhibitions and dissemination events, contributing to project visibility and recognition among stakeholders.

These materials provided stakeholders with concise information about the project, its objectives, the CURIMUM Compliance Continuum and the tools and services developed within the project.

3.5 Assessment of Dissemination and Communication KPIs

3.5.1 KPI Achievement Overview

The KPI assessment provides a cumulative overview of the project's performance over the full project period, up to 25 September 2026.

The activity descriptions in Sections up to 3.3.5 focus primarily on activities implemented during the second reporting period, from July 2025 onwards. Activities undertaken during the first reporting period and already reported in D5.1 remain part of the cumulative KPI assessment.

Activities implemented under WP3 and WP4 that contributed to dissemination, communication, stakeholder engagement or capacity-building objectives are included in the cumulative KPI assessment where the relevant KPI definition permits their contribution to be counted. Their detailed implementation is reported separately in D3.2 and D4.1.

3.5.2 Dissemination & Communication KPI Achievement

The following tables present the cumulative achievement of the Dissemination and Communication KPIs against their respective targets, based on the approach outlined above.

KPI	Description	Target	Cumulative
Website visits	Annual visits to the CURIUM website measuring awareness among SMEs, industry, academia and the general public.	≥500 / year	2025: 2,352 2026: 4,018
Downloads of materials	Number of downloads of public deliverables, results and dissemination materials.	≥100	492
Social media announcements	Push announcements on social media (Twitter/LinkedIn) promoting project activities and results.	≥10 / month	-
New followers	Growth of followers on CURIUM social media channels as an indicator of increased visibility.	>5 / month	+ 22 / month Total: 395
Re-tweets	Number of re-tweets amplifying CURIUM-related messages.	≥20 / year	-
Social media posts	Number of posts published annually across social media channels.	≥30 / year	2025: 38 2026: 61
Project Accounts	Project Accounts (ResearchGate & LinkedIn)	2	2: LinkedIn & Zenodo

E-newsletters produced	Number of technical e-newsletters disseminated to share project progress, achievements and next steps.	≥3	4
Newsletter receivers	Number of recipients reached through CURIUM e-newsletters.	≥500	514
Dissemination & Exploitation Plan versions	Number of updated versions of the Dissemination, Communication and Exploitation Plan produced during the project.	2	2
Synergies with similar projects	Number of similarly themed EU projects and initiatives identified for collaboration.	>5	8 EU-funded projects
Jointly organised workshops	Number of workshops jointly organised with other EU projects or initiatives.	>2	10
Peer-reviewed publications	Publications in international peer-reviewed scientific journals.	≥3	4 & 1 Manuscript & 1 White Paper
International magazine publications	Publications in international professional or technical magazines.	≥3	4
Conference / industrial presentations	Presentations of CURIUM results in conferences, scientific or industrial events.	≥5	15

Table 4: Assessment of raising awareness of CURIUM

KPI	Description	Target	Cumulative
Brochure downloads	Downloads of high-quality electronic brochures describing CURIUM's technical approach and activities.	≥200	236
LinkedIn discussions	Number of new LinkedIn discussions initiated to stimulate two-way knowledge exchange.	≥20	22
Monthly website downloads	Average monthly downloads of reports, videos, infographics and other content hosted on the CURIUM website.	≥20 / month	±23 / month Total: 492
Video demonstrators	Number of video demonstrators produced to showcase CURIUM tools and services.	≥4	5

YouTube views	Total views of 5-minute CURIUM videos on YouTube by the end of the project.	≥1000	1048
Events organised	Number of workshops, demonstrations or webinars organised to promote CURIUM tools and results (25 - 100 participants); 40% of the participants in each event attracted and registered as contacts.	≥3	3
Hard copies distributed	Number of hard copies distributed during ≥3 public and policy-related events.	≥120	354 during 9 events
Policy-making bodies engaged	Number of policy-making bodies engaged through consultations or networking events.	≥3	4 [NCSA, DSA partners of the project, ACN and Centre for Cybersecurity Belgium from Secure4smes project and Slovenian Authority]
More than 5 raise awareness activities organized	Targeting SMEs, SMEs associations and general public	>5	7
Number of trainings provided by CURIUM	External, from consortium members or developed inside the project	>10	11

Table 5: Assessment of Enabling Knowledge Exchange

KPI	Description	Target	Cumulative
Participation in events	Participation in small or large-scale events promoting exploitation of project outputs - presenting results to engage stakeholders for exploitation of outputs (education, industrial open days, organization of workshops, participation in EU	≥3 events	6

	annual meetings, conferences & exhibitions)		
Events organised (≥50 attendees)	One event organised with at least 50 attendees; 20% of participants engaged for further exploitation.	≥1	1
Impact KPI reports	Reports published with impact KPIs that are continuously updated.	3 reports	3

Table 6: Assessment of maximising impact of CURIUM's outputs and exploitation

KPI	Description	Target	Cumulative
Internal trainees	Number of internal trainees trained within partner organisations to become familiar with the CURIUM training tools.	≥10	30
Business partnerships formed	Number of partnerships formed with key business / open-source communities to support market uptake of CURIUM results.	≥3	3 strategic relationships formally established through signed MoUs with AKADIMOS, COcyber and CyberHubs and 1 CRA Cluster Community and 8 EU-funded projects

Table 7: Assessment of business growth through project's benefits

3.5.3 Overall Assessment

Overall, the implementation of the CURIUM dissemination and communication strategy resulted in broad and sustained engagement with scientific, industrial, SME, policy, regulatory and cybersecurity communities. During the second reporting period, the project combined direct stakeholder engagement through conferences, exhibitions, workshops, demonstrations and awareness-raising activities with digital communication through the website, social media, newsletters, videos, publications and promotional materials.

The cumulative KPI assessment demonstrates strong performance across the majority of the project's dissemination and communication objectives, with particularly strong results in social-media activity and follower growth, dissemination-material and brochure downloads, video production, scientific and magazine publications, awareness-raising activities and participation in events promoting project outputs. The project also strengthened its presence within the wider European cybersecurity ecosystem through collaboration with other projects and initiatives, enabling knowledge exchange, identification of synergies and wider dissemination of CURIUM results in the areas of cybersecurity, standards and CRA implementation.

Dissemination and communication activities also complemented the training, capacity-building and validation activities undertaken under WP3 and WP4. While these activities are reported in detail in D3.2 and D4.1, they provided additional opportunities to communicate project results, engage stakeholders and gather feedback relevant to the future uptake of the CURIUM tools and services.

Overall, the results demonstrate that the dissemination and communication approach established in D5.1 was effectively implemented and further developed as the project's results and tools became available. The combination of stakeholder engagement, awareness raising, scientific dissemination, demonstrations, collaborative activities and digital communication contributed to increasing awareness of the Cyber Resilience Act and promoting the CURIUM Compliance Continuum as a practical approach to supporting cybersecurity and compliance. The communication assets and resources developed during the project also provide a basis for maintaining visibility and access to CURIUM results beyond the project's completion.

4. Exploitation Activities / Plans

4.1. Introduction & Scope

This deliverable builds upon the work initiated in Deliverable D5.1 – Plan and early activities on Dissemination, Exploitation, Standardisation & Sustainability, where the initial dissemination, exploitation, sustainability, and standardisation strategy of the CURIUM project was defined. During the first reporting period, the project partners identified and analysed the Exploitable Results (ERs) emerging from the project activities, while also initiating stakeholder analysis, market assessment activities, and Value Proposition Canvas exercises for the identified results.

The work presented in this deliverable further develops and operationalises the exploitation-related activities foreseen under Task T5.2 – Impact creation, Exploitation & Standardization activities. The objective of this task is to support the transition of CURIUM results from research and innovation outcomes towards exploitable, sustainable, and market-oriented solutions capable of supporting the cybersecurity and compliance needs of organisations affected by the Cyber Resilience Act (CRA).

More specifically, Task T5.2 focuses on:

- the refinement and consolidation of the project's exploitation strategy;
- the identification and prioritisation of Key Exploitable Results (KERs);
- the definition of exploitation pathways and business approaches;
- the analysis of market needs and stakeholder expectations;
- the consideration of Intellectual Property Rights (IPR), ownership, and sustainability aspects;
- the exploration of adoption, service delivery, and pricing approaches;
- the support of future uptake and post-project continuation of CURIUM results.

Building on the analysis performed in D5.1, the consortium initially identified thirteen Exploitable Results (ERs), covering technological outputs, methodologies, platform components, capacity-building activities, and supporting project outcomes. Through further assessment and classification activities conducted during the second reporting period, these ERs were consolidated into seven Key Exploitable Results (KERs), representing the core exploitable assets of the project and the main focus of the exploitation activities presented in this deliverable.

The identified KERs collectively contribute to the implementation of the CURIUM Compliance Continuum, a modular and scalable ecosystem of cybersecurity tools and services designed to support organisations, particularly SMEs and micro-enterprises, in addressing CRA-related cybersecurity and compliance requirements.

The identified KERs build upon a combination of project-generated outcomes and partner-owned background assets, services, and cybersecurity capabilities integrated within the CURIUM ecosystem in accordance with the project's exploitation and access-rights framework.

The exploitation planning activities presented in this deliverable were developed through a structured and iterative process, combining:

- stakeholder and market analysis;
- Value Proposition Canvas exercises;
- identification of customer needs, pains, and expected gains;
- analysis of exploitation intentions and ownership structures;
- assessment of business and service delivery models;
- consideration of sustainability and post-project operational aspects.

Emphasis was placed on ensuring that the identified exploitation pathways remain aligned with:

- the modular architecture of the CURIUM ecosystem;
- the different maturity levels and needs of target stakeholders;
- the project's validation activities and pilot feedback;
- evolving CRA-related market and regulatory developments.

In this context, the present deliverable does not approach exploitation as a single standalone commercialisation activity, but rather as a combination of:

- standalone exploitation opportunities for individual KERs;
- coordinated exploitation through the CURIUM Continuum;
- service-oriented and ecosystem-based exploitation approaches;
- capacity-building and adoption-support activities.

The following sections present:

- the methodology followed for the development of the exploitation plans;
- the business and value creation logic of the identified KERs;
- the market context and target stakeholder ecosystem;
- and the individual exploitation plans developed for each Key Exploitable Result of the CURIUM project.

4.2. Methodology for Exploitation Planning

4.2.1. Exploitation and Market Analysis Strategy

The exploitation planning activities of the CURIUM project build upon the work initiated in Deliverable D5.1 – *Plan and early activities on Dissemination, Exploitation,*

Standardisation & Sustainability, where the initial exploitation, dissemination, sustainability, and standardisation approach of the project was established.

According to the European Commission's Research and Innovation framework, exploitation refers to the use of project results in further research and innovation activities, in the development and improvement of products, processes, and services, as well as in standardisation activities and policy support. In this context, exploitation is not limited to direct commercialisation activities but also includes broader societal, operational, and ecosystem-oriented uptake of project outcomes.

Within the CURIUM project, exploitation focuses on supporting the transition of research and innovation outputs into usable, sustainable, and market-oriented cybersecurity solutions capable of addressing the needs created by the Cyber Resilience Act (CRA) and the broader cybersecurity ecosystem.

The methodology followed within the project was based on a structured process combining exploitation planning, ownership analysis, and sustainability considerations.

The main methodological steps followed are presented below.

4.2.2. Identification and Classification of Exploitable Results

During the first reporting period, a structured analysis of the project outcomes was conducted to identify the Exploitable Results (ERs) generated by the project activities. This analysis resulted in the identification of thirteen (13) ERs covering:

- technological outputs and platform components;
- cybersecurity assessment and compliance services;
- capacity-building and awareness activities;
- methodologies and supporting project outcomes.

The identified ERs included both standalone outputs and integrated components related to the broader CURIUM Compliance Continuum.

Building upon the work performed in D5.1, further assessment and classification activities were conducted during the second reporting period in order to prioritise the most mature, strategically important, and exploitable results of the project. Through this process, the consortium consolidated the identified ERs into seven (7) Key Exploitable Results (KERs), which form the basis of the exploitation planning activities presented in this deliverable.

4.2.2.1. Identification of IPR and Ownership Aspects

As part of the exploitation planning activities, the consortium analysed Intellectual Property Rights (IPR), ownership structures, and exploitation responsibilities related to the identified ERs and KERs.

Each partner identified:

- background knowledge introduced into the project;
- ownership of newly generated results;
- potential exploitation interests and constraints;
- possible joint exploitation scenarios.

The ownership status of the identified ERs and KERs was initially documented in D5.1 and remains aligned with the provisions of the Grant Agreement and the Consortium Agreement of the project.

Particular attention was given to jointly owned results and coordinated exploitation scenarios, especially in relation to the CURIUM Continuum and the interoperability between individual KERs.

The exploitation planning activities were additionally coordinated in alignment with the project's Innovation Manager in order to ensure consistency between technical development, market orientation, sustainability objectives, and exploitation pathways.

The exploitation planning activities additionally considered the background assets, access rights conditions, and ownership restrictions defined within the Consortium Agreement, particularly in relation to partner-owned cybersecurity services, assessment tools, and platform components integrated within the CURIUM ecosystem.

4.2.2.2. Stakeholder Analysis and Market Assessment

The exploitation methodology additionally included stakeholder identification and market analysis activities aiming to better understand:

- the needs and expectations of target users;
- potential market opportunities;
- barriers to adoption;
- possible exploitation pathways and service models.

Special focus was placed on SMEs and micro-enterprises, which represent the primary target group of the CURIUM project and are expected to face increasing cybersecurity and compliance obligations due to the introduction of the Cyber Resilience Act. The analysis additionally considered:

- cybersecurity providers and consultants;
- certification and standardisation actors;
- public authorities and policy stakeholders;
- research and innovation ecosystems.

4.2.2.3. Value Proposition Canvas Activities

To support the identification of stakeholder needs and the development of exploitation pathways, the consortium utilised the Value Proposition Canvas methodology developed by Dr. Alexander Osterwalder.

The Value Proposition Canvas activities were initiated during the first reporting period and further refined during the second reporting period. For each identified KER, the methodology supported the analysis of:

- customer segments and target stakeholders;
- customer jobs and operational objectives;
- stakeholder pains and barriers;
- expected gains and value drivers;
- value propositions and exploitation opportunities.

The results of these activities contributed directly to:

- the structuring of the individual exploitation plans;
- the identification of adoption pathways;
- the definition of business and service models;
- the positioning of the KERs within the CURIUM Compliance Continuum.

4.2.2.4. Development of Exploitation Plans

Based on the outcomes of the previous methodological steps, the consortium developed individual exploitation plans for the identified KERs.

The exploitation plans take into consideration:

- the exploitation interests of the project partners;
- ownership and IPR considerations;
- possible exploitation and deployment routes;
- market needs and stakeholder expectations;
- sustainability and post-project continuation aspects;
- business, adoption, and pricing approaches.

Given the limited duration of the project, particular emphasis was placed on post-project exploitation and sustainability activities rather than only short-term project-period exploitation.

The developed exploitation plans additionally consider:

- standalone exploitation opportunities for individual KERs;
- coordinated exploitation through the CURIUM Continuum;
- service-oriented and ecosystem-based exploitation models;
- support for future scalability and market uptake.

4.2.2.5. Iterative Market Monitoring and Validation

The exploitation methodology followed an iterative and validation-driven approach throughout the project lifecycle.

Feedback collected through:

- pilot activities;
- stakeholder engagement;
- validation exercises;
- dissemination and communication activities;
- interactions with the broader cybersecurity ecosystem,

was continuously considered in order to refine exploitation assumptions, identify emerging market needs, and align the project outcomes with evolving CRA-related requirements and market expectations.

This iterative approach supports the progressive adaptation of the exploitation pathways and contributes to the long-term relevance and sustainability of the project results.

4.2.2.6. Standardisation and Regulatory Alignment

The exploitation planning activities additionally considered alignment with relevant cybersecurity, certification, and standardisation ecosystems.

Particular attention was given to:

- alignment with CRA-related regulatory developments;
- interoperability and compatibility considerations;
- future integration with conformity assessment and certification processes;
- potential engagement with standardisation and regulatory fora relevant to cybersecurity and compliance activities.

These activities support the positioning of CURIUM results within the broader European cybersecurity and regulatory ecosystem and contribute to the long-term sustainability and usability of the project outcomes.

4.3. Overview of the 7 KERs

4.3.1. Overview of the CURIUM KER Ecosystem

The CURIUM project delivers a set of interrelated Key Exploitable Results (KERs), forming the foundation of the proposed CURIUM Compliance Continuum. The Continuum represents a modular and scalable ecosystem of cybersecurity tools and services designed to support organisations, primarily European SMEs and micro-enterprises, in achieving and maintaining compliance with the Cyber Resilience Act (CRA), while enhancing the cybersecurity posture of products with digital elements throughout their lifecycle.

Building upon the analysis conducted in Deliverable D5.1, the identified KERs are structured around a combination of core cybersecurity services, supporting tools, and capacity-building activities that collectively address different stages of the cybersecurity compliance lifecycle. These stages include CRA scoping and

classification, risk management, security validation and testing, compliance verification, and continuous improvement activities.

The identified KERs are designed to operate both as standalone exploitable components and as integrated elements of the CURIUM Compliance Continuum, enabling flexible adoption depending on the needs, maturity level, and operational capabilities of the target stakeholders. (Table 8)

KER	Description	CRA Compliance Lifecycle Position
CyReA	CRA scoping and product classification service supporting organisations in identifying applicability and regulatory obligations.	Scope & Classification
DPRA	Risk analysis and risk management service supporting identification and evaluation of cybersecurity risks.	Risk Management
PSTVA	Vulnerability assessment and penetration self-testing service supporting security validation activities.	Security Validation & Testing
CAC	Compliance assessment and conformity support service enabling audit-readiness and compliance verification.	Compliance Verification
DPMA	Cybersecurity maturity assessment service supporting continuous improvement and security enhancement activities.	Continuous Improvement
Capacity Building Services	Training, awareness, and knowledge transfer activities supporting adoption and capability development.	Horizontal Support
CURIUM Continuum	Integrated orchestration environment enabling coordinated use of CURIUM services across the compliance lifecycle.	Full Lifecycle Integration

Table 8: Overview of the CURIUM Key Exploitable Results (KERs) and their positioning within the CRA-oriented compliance lifecycle.

Within this context, the CURIUM Continuum acts as the orchestration and integration layer enabling the coordinated use of the individual KERs across the CRA-oriented cybersecurity compliance lifecycle.

The identified KERs are additionally supported by complementary methodologies, consulting activities, awareness actions, and capacity-building mechanisms that

facilitate usability, adoption, interoperability, and long-term sustainability of the project outcomes.

A key characteristic of the CURIUM KER ecosystem is its modular architecture. Each KER can be exploited independently as a standalone component or service addressing specific cybersecurity and compliance needs. At the same time, the integration of these KERs within the CURIUM Compliance Continuum enables a coordinated and interoperable cybersecurity compliance ecosystem supporting different stages of the CRA-oriented compliance lifecycle.

This modular approach supports:

- flexible adoption depending on organisational maturity and needs;
- gradual integration of additional services and functionalities;
- interoperability between cybersecurity assessment, testing, risk management, and compliance activities;
- scalability across different organisational environments and stakeholder groups.

4.3.2. Business and Value Creation Logic

The exploitation and value creation approach of the CURIUM project is designed to support the sustainable uptake and long-term usability of its Key Exploitable Results (KERs), while maintaining flexibility and accessibility for the targeted stakeholder groups, particularly SMEs and micro-enterprises.

Rather than relying on a single commercialisation pathway, CURIUM adopts a hybrid and adaptable exploitation approach, enabling different deployment, integration, and service delivery models depending on the maturity level, operational needs, and technical capabilities of the adopting organisations.

The value creation logic of the CURIUM ecosystem is based on two complementary dimensions:

- standalone exploitation of individual KERs addressing specific cybersecurity and compliance needs;
- coordinated and interoperable exploitation through the CURIUM Compliance Continuum, enabling coordinated support across different stages of the CRA-oriented cybersecurity compliance lifecycle.

Within this context, different exploitation and deployment models may be adopted, including:

- Software-as-a-Service (SaaS) approaches for cloud-based access to cybersecurity and compliance services;
- service-oriented models combining consulting, assessment, and compliance support activities;

- integration of partner-owned services, tools, and CURIUM components into existing operational environments, platforms, or service portfolios;
- training and capacity-building services supporting knowledge transfer and ecosystem adoption.

This multi-model approach enables different partners and stakeholders to exploit the project outcomes according to their role within the ecosystem, while additionally supporting scalability, interoperability, and gradual adoption.

The sustainability of the CURIUM ecosystem is expected to be supported through a combination of:

- subscription-based services;
- consulting and support activities;
- integration and licensing agreements;
- training and awareness services;
- reuse of project outcomes in future initiatives and operational environments.

At the same time, the exploitation approach takes into consideration the importance of accessibility, modularity, and the use of low-cost or open-source-based elements, aiming to minimise adoption barriers, particularly for organisations with limited cybersecurity expertise or financial resources.

The exploitation approach additionally reflects the distributed ownership model of the CURIUM ecosystem, where individual KERs may be independently exploited by the respective partners while also contributing to coordinated ecosystem-oriented service offerings through the CURIUM Continuum.

4.3.3. Value Proposition Canvas Approach

4.3.3.1. Value Proposition Canvas Methodology

To support the identification of stakeholder needs, market expectations, and exploitation opportunities, the consortium utilised the Value Proposition Canvas methodology developed by Dr. Alexander Osterwalder (Figure 23).

The Value Proposition Canvas activities were initiated during the first reporting period and further refined during the second reporting period in alignment with the development of the Key Exploitable Results (KERs).

The methodology supported the analysis of:

- target stakeholder groups and customer segments;
- operational objectives and customer jobs;
- stakeholder pains, barriers, and adoption challenges;
- expected gains and value drivers;
- value propositions and exploitation opportunities associated with each KER.

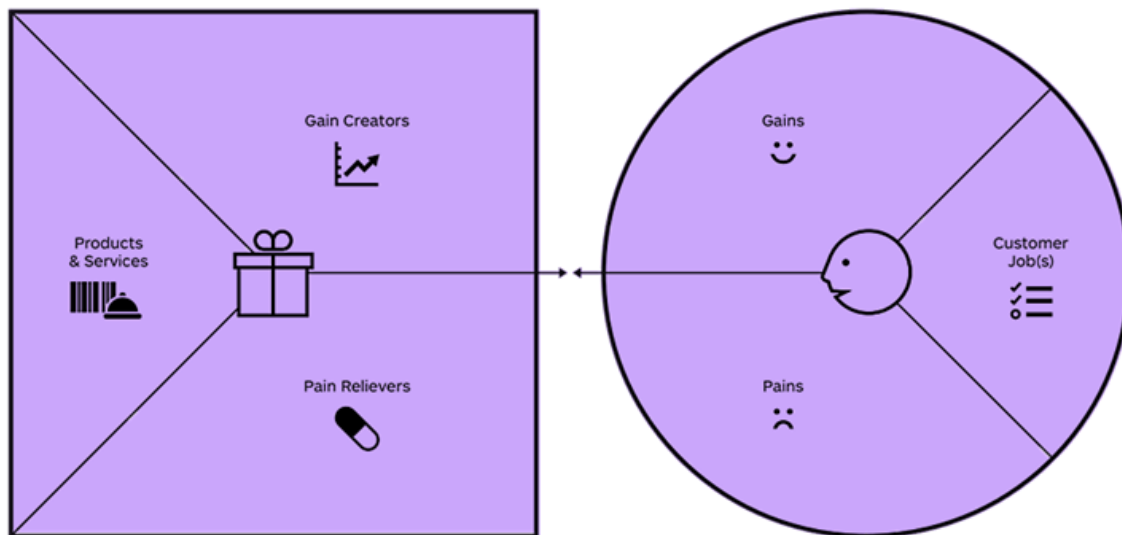


Figure 23: Value Proposition Canvas used for the analysis of stakeholder needs, pains, gains, and value propositions associated with the CURIUM Key Exploitable Results (adapted from Strategyzer).

4.3.3.2. Canvas Dimensions

The Value Proposition Canvas methodology used within the CURIUM project focused on the following core dimensions:

Customer Segments

Customer segments represent the stakeholder groups targeted by the identified KERs, including SMEs, cybersecurity providers, consultants, public authorities, conformity assessment actors, and organisations involved in CRA-related cybersecurity compliance activities.

Customer Jobs

Customer Jobs refer to the tasks, objectives, and activities that the targeted stakeholders are trying to accomplish in the context of cybersecurity and CRA compliance activities. These may include:

- **Functional jobs**, such as understanding CRA obligations, preparing compliance documentation, managing internal audits, or performing cybersecurity assessments;
- **Social jobs**, such as increasing trustworthiness as a supplier, demonstrating compliance readiness, or aligning with European cybersecurity expectations;
- **Emotional jobs**, such as reducing uncertainty regarding compliance obligations and increasing confidence in cybersecurity preparedness;
- **Basic needs**, such as access to reliable tools, guidance, support services, and communication mechanisms.

Within this dimension, consortium partners analysed both operational activities and higher-level organisational objectives associated with the adoption and use of the identified KERs.

Gains

Gains represent the positive outcomes, benefits, and improvements expected by stakeholders when using the identified KERs. The analysis considered aspects such as:

- simplification and acceleration of compliance activities;
- reduction of documentation effort and operational complexity;
- improved audit-readiness and confidence in compliance activities;
- reduction of costs associated with external consultancy and manual processes;
- increased usability, accessibility, and interoperability;
- improved organisational reputation and trustworthiness.

These gains may be functional, operational, strategic, reputational, or organisational in nature.

Pains

Pains refer to the obstacles, risks, frustrations, and barriers experienced by stakeholders when attempting to achieve CRA-related cybersecurity compliance.

The analysis considered challenges such as:

- regulatory complexity and difficulty interpreting CRA obligations;
- lack of internal cybersecurity expertise;
- fragmented tools and disconnected compliance processes;
- high compliance and consultancy costs;
- difficulties in maintaining audit-ready documentation;
- operational uncertainty and limited organisational resources.

Value Propositions

The Value Proposition dimension focused on identifying how each KER contributes to addressing stakeholder pains and generating meaningful gains.

This included:

- automation and simplification of cybersecurity compliance activities;
- integrated support across the CRA-oriented compliance lifecycle;
- provision of structured assessment, testing, and compliance services;
- support for modular and scalable adoption;
- enhancement of cybersecurity awareness, preparedness, and organisational capabilities.

4.3.3.3. Results and Exploitation Insights

The Value Proposition Canvas activities provided important insights regarding the expected adoption, usability, and exploitation potential of the identified Key Exploitable Results (KERs). The analysis additionally considered:

- CRA-related compliance challenges;

- usability and accessibility requirements;
- cost and resource limitations of SMEs;
- interoperability and integration needs;
- expectations related to trust, audit-readiness, and cybersecurity assurance.

The results of the Value Proposition Canvas activities contributed directly to:

- the refinement of the identified KERs;
- the development of exploitation pathways;
- the identification of suitable business and service models;
- the positioning of the KERs within the CURIUM Compliance Continuum;
- the preparation of the individual exploitation plans presented in the following sections.

4.3.4. Exploitation Intentions Overview

As part of the exploitation planning activities, consortium partners provided structured exploitation-related information and preliminary exploitation intentions through dedicated exploitation input templates developed for each identified KER.

The collected information supported the analysis of:

- the intended use and positioning of each KER;
- target markets and end-user groups;
- competitive advantages and differentiation aspects;
- intended exploitation and deployment models;
- ownership structures and partner involvement;
- timing and expected post-project continuation activities;
- Intellectual Property Rights (IPR) considerations and exploitation constraints.

This information was aggregated and analysed in order to:

- identify common exploitation patterns across the project;
- support alignment between standalone partner-driven exploitation activities and coordinated ecosystem-oriented exploitation approaches;
- evaluate sustainability and market potential;
- facilitate coordination between partners and jointly owned KERs.

The analysis demonstrated that the identified KERs present different levels of exploitation maturity and commercial readiness. While some KERs are positioned closer to market-oriented service provision and commercial exploitation, others primarily operate as supporting, enabling, or ecosystem-oriented components within the broader CURIUM Compliance Continuum.

The exploitation intentions additionally confirmed the importance of:

- modular adoption pathways;

- service-oriented exploitation approaches;
- integration between complementary KERs;
- support for SMEs and organisations with limited cybersecurity expertise;
- alignment with evolving CRA-related regulatory and market requirements.

Detailed exploitation information and partner-specific considerations are further reflected within the individual exploitation plans of each KER.

The analysis additionally confirmed that several KERs build upon pre-existing partner capabilities, services, and background assets, which may continue to evolve independently beyond the duration of the project while remaining interoperable within the broader CURIUM ecosystem.

4.3.5. Market Context and Stakeholder Ecosystem

The exploitation strategy of the CURIUM project is grounded on the evolving cybersecurity and regulatory landscape shaped by the Cyber Resilience Act (CRA) and the increasing demand for cybersecurity compliance services across the EU market.

The CRA introduces new obligations for organisations developing, integrating, distributing, or maintaining products with digital elements, creating significant operational, technical, and compliance-related challenges, particularly for SMEs and micro-enterprises with limited cybersecurity resources and expertise.

Within this context, CURIUM addresses a growing need for:

- simplified and accessible cybersecurity compliance services;
- integrated cybersecurity assessment and testing capabilities;
- cost-effective and modular cybersecurity solutions;
- support for audit-readiness and conformity assessment activities;
- continuous cybersecurity monitoring and improvement mechanisms.

The primary target group of the CURIUM ecosystem consists of SMEs and micro-enterprises directly affected by CRA-related requirements. For these organisations, the project aims to provide:

- user-friendly and accessible cybersecurity services;
- modular adoption options depending on organisational maturity;
- reduced dependency on external consultancy;
- improved cybersecurity and compliance readiness.

Additional stakeholder groups include:

- cybersecurity providers and consultants;
- certification and conformity assessment actors;
- public authorities and policy stakeholders;
- Digital Innovation Hubs and competence centres;

- research and innovation organisations;
- technology providers and cybersecurity ecosystems.

The identified stakeholder groups share several common needs and expectations, including:

- reduction of regulatory complexity;
- lower compliance and operational costs;
- interoperability with existing systems and workflows;
- improved usability and accessibility;
- increased confidence in cybersecurity and compliance activities.

The modular structure of the CURIUM Compliance Continuum additionally supports progressive adoption and integration, enabling organisations to gradually expand the use of cybersecurity and compliance services according to their operational capabilities and evolving needs.

4.3.5.1. Market Opportunity

The market opportunity addressed by the CURIUM project is strongly linked to the increasing cybersecurity and compliance obligations introduced by the Cyber Resilience Act (CRA), as well as the broader evolution of the European cybersecurity regulatory landscape.

The introduction of the CRA is expected to significantly increase the demand for:

- cybersecurity compliance services;
- vulnerability assessment and testing solutions;
- conformity assessment and audit-readiness support;
- lifecycle-oriented cybersecurity management mechanisms;
- affordable and accessible cybersecurity tools for SMEs and micro-enterprises.

At the same time, SMEs represent more than 99% of businesses operating within the European Union¹, while many organisations continue to face substantial limitations related to cybersecurity expertise, operational resources, and compliance preparedness.

This creates a growing market need for:

- modular and scalable cybersecurity compliance services;
- simplified and user-friendly assessment and compliance mechanisms;
- integrated cybersecurity and compliance ecosystems;
- low-cost and interoperable solutions that can support progressive adoption depending on organisational maturity and operational capabilities.

In parallel, the continuous growth of the European cybersecurity market, driven by increasing cyber threats, supply-chain vulnerabilities, digital transformation initiatives,

¹ https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en

and evolving regulatory obligations, further reinforces the long-term relevance and exploitation potential of the CURIUM Compliance Continuum and its associated Key Exploitable Results (KERs).

Within this context, CURIUM Continuum aims to position itself as a modular and accessible cybersecurity compliance ecosystem capable of supporting organisations throughout different stages of the CRA-oriented cybersecurity compliance lifecycle.

4.3.5.2. Adoption and Go-to-Market Considerations

The adoption and go-to-market approach of the CURIUM ecosystem is designed to support the progressive uptake of the identified Key Exploitable Results (KERs), with particular emphasis on SMEs and micro-enterprises affected by the Cyber Resilience Act (CRA).

Rather than relying on a single commercialisation pathway, the CURIUM approach combines modular adoption, ecosystem-oriented collaboration, validation-driven refinement, and service-oriented exploitation pathways. This approach enables different stakeholders to adopt and utilise the identified KERs according to their operational needs, cybersecurity maturity level, and available resources.

The adoption logic of the CURIUM ecosystem supports different levels of engagement, including:

- initial adoption of standalone cybersecurity and compliance services addressing specific organisational needs;
- progressive integration of complementary KERs and services;
- coordinated use of interoperable services through the CURIUM Compliance Continuum.

This staged adoption approach supports gradual onboarding while reducing operational and financial barriers for organisations with limited cybersecurity expertise.

The go-to-market activities of the project are additionally supported through:

- the existing networks and ecosystems of consortium partners;
- collaboration with SMEs, cybersecurity providers, and innovation ecosystems;
- engagement with Digital Innovation Hubs (DIHs), competence centres, and cybersecurity communities;
- dissemination and communication activities implemented within the project;
- pilot activities and validation exercises involving early adopters and stakeholder feedback.

Particular emphasis is placed on validation-driven adoption and iterative refinement of the identified KERs. Feedback collected through pilot activities, demonstrations, stakeholder engagement, and validation exercises contributes to:

- refinement of functionalities and service delivery approaches;

- alignment with real operational and compliance-related needs;
- improvement of usability, accessibility, and interoperability aspects;
- increased trustworthiness and market relevance of the identified KERs.

The exploitation and adoption strategy additionally considers potential barriers affecting SMEs and organisations with limited cybersecurity resources, including:

- regulatory complexity and uncertainty related to CRA obligations;
- limited internal cybersecurity expertise;
- high operational and consultancy costs;
- difficulties integrating cybersecurity and compliance activities into existing workflows.

To address these challenges, the CURIUM ecosystem emphasises:

- modular and scalable adoption pathways;
- user-friendly and accessible cybersecurity services;
- service-oriented and support-based exploitation approaches;
- integration of low-cost and interoperable solutions;
- training, awareness, and capacity-building activities supporting long-term adoption and operational sustainability.

Overall, the adoption and go-to-market considerations of the CURIUM project aim to facilitate the transition of the identified KERs from project outcomes to sustainable and operational cybersecurity compliance services capable of supporting organisations throughout different stages of the CRA-oriented cybersecurity compliance lifecycle.

4.3.6. Competitive Positioning of CURIUM's Compliance Continuum

The CURIUM Compliance Continuum differentiates itself from existing cybersecurity and Governance-Risk-Compliance (GRC) solutions through its integrated, modular, and CRA-oriented approach.

While many existing solutions focus on isolated functionalities such as vulnerability assessment, documentation management, or generic compliance monitoring, the CURIUM ecosystem combines:

- CRA scoping and classification;
- cybersecurity risk assessment;
- vulnerability testing and security validation;
- compliance verification and conformity support;
- maturity assessment and continuous improvement activities;
- training and capacity-building services.

This coordinated and interoperable approach enables organisations to address multiple cybersecurity and compliance needs through a federated ecosystem of interoperable cybersecurity services and tools.

At the same time, the modular architecture of the CURIUM ecosystem supports:

- standalone adoption of individual KERs;
- gradual integration of complementary services;
- scalability across different organisational profiles and maturity levels;
- adaptation to different operational and regulatory contexts.

Emphasis is placed on accessibility and usability for SMEs and organisations with limited cybersecurity expertise, which are often underserved by existing cybersecurity compliance and GRC solutions.

The positioning of the CURIUM Compliance Continuum is additionally strengthened by:

- alignment with CRA-related regulatory developments;
- support for lifecycle-oriented cybersecurity management;
- integration of assessment, testing, and compliance activities;
- combination of technical services and capacity-building mechanisms;
- ecosystem-oriented exploitation and adoption logic.

Within this context, CURIUM aims to position itself not as a single-purpose cybersecurity tool, but as a coordinated and scalable cybersecurity compliance ecosystem supporting organisations throughout different stages of the CRA-oriented compliance lifecycle.

4.3.7. IPR & Exploitation Governance

The exploitation of CURIUM results is supported by a structured Intellectual Property Rights (IPR) and governance framework, ensuring clarity in ownership, access rights, and responsibilities among the consortium partners. This framework builds upon the principles and agreements defined in Deliverable D5.1 and the project's contractual arrangements, providing the foundation for coordinated and sustainable exploitation activities.

4.3.7.1. IPR Framework

The ownership of the Key Exploitable Results (KERs) remains with the partners that have generated them, in accordance with the rules established in the Grant Agreement and the Consortium Agreement. Each partner retains the rights to exploit its results individually, while also contributing to the collective value of the CURIUM Compliance Continuum.

Access rights to background and foreground knowledge are defined to enable effective collaboration during the project and to support the exploitation of results after its

completion. These rights ensure that partners can utilise relevant components developed within the project, where necessary, while respecting ownership boundaries.

4.3.7.2. Exploitation Responsibilities

Each consortium partner is responsible for the exploitation of the results it owns or co-develops, either independently or in collaboration with other partners. This includes:

- further development and refinement of tools and services;
- integration into existing products or service portfolios;
- delivery of related services (e.g. consulting, training, support);
- engagement with target markets and stakeholders.

At the same time, the consortium as a whole contributes to the coordinated positioning and promotion of the CURIUM ecosystem, particularly in relation to the Compliance Continuum.

4.3.7.3. Governance Structure

The governance of exploitation activities is coordinated at project level, ensuring alignment between individual partner strategies and the overall exploitation objectives of CURIUM. This includes:

- coordination of exploitation planning and monitoring activities;
- alignment with dissemination and communication efforts;
- identification of synergies between KERs;
- support for joint exploitation initiatives where relevant.

The role of the Innovation Manager is particularly important in this context, facilitating coordination, monitoring exploitation progress, and ensuring that relevant aspects such as market potential, commercial interest, and sustainability are consistently addressed.

Following project completion, the consortium partners shall explore a coordinated operational governance mechanism for the CURIUM Compliance Continuum. This mechanism could define responsibilities related to platform hosting, maintenance, integration management, user support, and evolution of the integrated ecosystem.

Depending on the final exploitation configuration, these responsibilities may be assigned to a lead operational partner or managed through a federated collaboration model among the involved consortium partners.

The governance framework will additionally support:

- coordinated technical updates and maintenance activities;
- interoperability and integration management between KERs;
- onboarding of additional services and ecosystem partners;
- alignment of branding and market positioning activities;
- monitoring of exploitation KPIs and sustainability objectives.

Coordination activities may additionally be supported through periodic governance meetings, operational working groups, and partner-level agreements defining responsibilities related to maintenance, updates, onboarding of new functionalities, and commercial collaboration activities.

This governance approach is designed to ensure both flexibility and long-term operational continuity while allowing the Compliance Continuum to evolve according to market needs and regulatory developments.

4.3.7.4. Collaboration and Joint Exploitation

Given the interoperable and ecosystem-oriented nature of the CURIUM results, several exploitation scenarios involve collaboration between partners. These may include:

- joint service offerings combining multiple KERs;
- integration of complementary tools and functionalities;
- shared participation in market-oriented activities (e.g. pilots, demonstrations, stakeholder engagement).

Such collaboration enhances the overall value proposition of the CURIUM Compliance Continuum and supports its positioning as a cohesive ecosystem rather than a collection of disconnected components.

4.3.7.5. Alignment with Sustainability Objectives

The IPR and governance framework supports the long-term sustainability of CURIUM results by:

- enabling both individual and joint exploitation pathways;
- ensuring clear ownership and responsibility structures;
- facilitating the continuation of collaboration beyond the project duration;
- supporting the transition from project outputs to operational services and market offerings.

4.3.8. Sustainability and Future Evolution

The sustainability of CURIUM results beyond the project duration is a key priority, ensuring that the developed tools, services, and methodologies continue to deliver value to the targeted stakeholders and contribute to the broader cybersecurity ecosystem. The exploitation strategy is therefore designed not only to enable initial market uptake but also to support the **operational continuity, evolution, and coordinated uptake** of the CURIUM Compliance Continuum.

4.3.8.1. Post-Project Continuation

Following the completion of the project, the continuation of CURIUM results is expected to be supported through multiple pathways, including:

- further development and maintenance of individual tools and services by the respective partners;

- integration of CURIUM components into existing products, platforms, or service portfolios;
- continuation of service-based offerings such as consulting, assessment, and compliance support;
- ongoing use of training materials and capacity-building activities.

This approach ensures that the results remain active and relevant beyond the project lifecycle.

4.3.8.2. Evolution and Scaling

The modular design of the CURIUM Compliance Continuum enables continuous evolution and scalability. Future developments may include:

- extension of functionalities to address additional regulatory frameworks or standards;
- enhancement of existing tools based on user feedback and technological advancements;
- adaptation to new market needs and emerging cybersecurity challenges;
- expansion to additional sectors or geographical markets.

This capacity for evolution supports the long-term relevance and competitiveness of the CURIUM offering.

4.3.8.3. Integration into the Cybersecurity Ecosystem

CURIUM results are designed to operate within a broader ecosystem of stakeholders, standards, and initiatives. Their sustainability is reinforced through:

- alignment with European policies and regulatory frameworks (e.g. CRA and related initiatives);
- engagement with standardisation bodies and certification schemes;
- collaboration with Digital Innovation Hubs, competence centres, and industry networks;
- contribution to ongoing knowledge sharing and capacity-building efforts.

This ecosystem integration enhances both visibility and long-term impact.

4.3.8.4. Business Sustainability

The long-term sustainability of the CURIUM Compliance Continuum will additionally rely on coordinated maintenance activities among involved partners, continuous alignment with evolving CRA requirements, integration of new functionalities and services, and reuse of developed components within future projects and commercial activities.

Operational sustainability may be supported through subscription-based services, consulting activities, ecosystem partnerships, and integration into existing partner service portfolios.

4.4. Exploitation Plans per Key Exploitable Result

4.4.1. KER1 – CURIUM Continuum – Responsible Partner: Consortium

The CURIUM Continuum represents the overarching orchestration and integration ecosystem of the CURIUM project, enabling the coordinated use of interoperable cybersecurity and compliance-related services across different stages of the CRA-oriented cybersecurity compliance lifecycle.

Rather than constituting a single monolithic platform or standalone commercial product, the CURIUM Continuum operates as a modular and interoperable environment integrating partner-owned tools, services, methodologies, and cybersecurity capabilities developed or utilised within the project framework.

The Continuum is designed to support organisations—particularly SMEs and micro-enterprises—in addressing cybersecurity and compliance obligations introduced by the Cyber Resilience Act (CRA), while facilitating coordinated access to assessment, testing, compliance verification, maturity evaluation, and capacity-building services.

The CURIUM Continuum supports activities related to:

- CRA scoping and product classification;
- cybersecurity risk assessment and management;
- vulnerability assessment and penetration self-testing;
- compliance verification and audit-readiness;
- cybersecurity maturity assessment and continuous improvement;
- training, awareness, and capacity-building activities.

The ecosystem-oriented approach of the CURIUM Continuum enables the individual KERs to operate both independently and as interoperable components contributing to a coordinated cybersecurity compliance environment.

4.4.1.1. *Target Stakeholders and End Users*

The primary target stakeholders of the CURIUM Continuum include:

- SMEs and micro-enterprises developing, integrating, or maintaining products with digital elements;
- cybersecurity service providers and consultants;
- conformity assessment and certification-related actors;
- Digital Innovation Hubs (DIHs) and competence centres;
- public authorities and policy-related stakeholders;

- research and innovation organisations involved in cybersecurity and CRA-related activities.

The CURIUM Continuum is particularly intended to support organisations with limited cybersecurity expertise and operational resources by enabling progressive and modular adoption of cybersecurity compliance services.

4.4.1.2. Value Proposition and Competitive Positioning

The main value proposition of the CURIUM Continuum lies in its coordinated and interoperable approach to CRA-oriented cybersecurity compliance support.

Existing cybersecurity and compliance solutions often address isolated activities such as vulnerability testing, documentation management, or generic compliance monitoring. In contrast, the CURIUM Continuum enables coordinated interaction between multiple interoperable cybersecurity services and assessment mechanisms across different stages of the cybersecurity compliance lifecycle.

The main differentiating elements of the CURIUM Continuum include:

- modular and scalable architecture supporting gradual adoption;
- interoperability between complementary cybersecurity services and KERs;
- support for coordinated CRA-oriented compliance activities;
- accessibility for SMEs and organisations with limited cybersecurity expertise;
- integration of assessment, testing, compliance, and capacity-building activities within a coordinated ecosystem-oriented environment.

The CURIUM Continuum additionally supports the generation of structured outputs contributing to audit-readiness, cybersecurity preparedness, and operational compliance support.

4.4.1.3. Exploitation Approach

The exploitation approach of the CURIUM Continuum is based on coordinated ecosystem-oriented exploitation rather than the commercialisation of a single unified product.

The Continuum enables:

- coordinated use of interoperable partner-owned services and tools;
- standalone exploitation of individual KERs by the respective partners;
- integration of complementary cybersecurity and compliance capabilities;
- service-oriented exploitation scenarios combining assessment, consulting, training, and compliance support activities.

Different partners may independently exploit their respective services, methodologies, tools, and background assets while contributing to the broader interoperability and coordinated operation of the CURIUM ecosystem.

The CURIUM Continuum therefore acts primarily as:

- an orchestration environment;
- a cross-selling environment;
- a tool for the identification of the requirements of the CRA in order to help SMEs and attract them to other services;
- a coordinated access layer for complementary cybersecurity compliance services.

4.4.1.4. Adoption and Deployment Logic

The adoption logic of the CURIUM Continuum supports progressive and modular engagement depending on organisational needs, maturity level, and operational capabilities.

Possible adoption pathways include:

- initial use by SMEs to support them on their CRA compliance journey;
- initial use of standalone assessment or testing services;
- used as a tool by project partners to attract new or existing customers for complimentary products or services;
- progressive onboarding of complementary KERs and cybersecurity capabilities;
- coordinated use of interoperable services through the CURIUM ecosystem.

Training materials, awareness activities, user guidance resources, and capacity-building services are additionally expected to support adoption and operational usability.

4.4.1.5. Ownership and Governance Considerations

The CURIUM Continuum incorporates interoperable services, tools, methodologies, and background assets contributed by different consortium partners in accordance with the Grant Agreement and the Consortium Agreement of the project.

Ownership of individual tools, services, and exploitable components remains with the respective partners generating or contributing them. The Continuum itself operates as a coordinated interoperability and exploitation framework supporting the combined use of these complementary capabilities.

Operational governance activities following the completion of the project may include:

- coordination of interoperability and integration activities;
- maintenance and evolution of integration mechanisms;
- alignment of service delivery approaches;
- coordinated positioning and ecosystem-oriented dissemination activities;
- support for onboarding of additional services and functionalities.

Depending on the post-project operational model, governance activities may be coordinated through a federated collaboration approach among the involved partners.

4.4.1.6. *Technical Maturity and Market Readiness*

The CURIUM Continuum started from an initial conceptual maturity corresponding to Technology Readiness Level (TRL) 1 and has reached TRL 8 at end of the project. The progression in maturity is associated with the development and integration of the individual CURIUM KERs into a coordinated cybersecurity compliance ecosystem, the implementation of interoperability mechanisms, and the validation of the integrated environment through project activities. Additional activities planned before project completion include external testing of the integrated environment, including single sign-on and full portal functionality. The achievement of TRL 8 is expected to be supported by the completion of these integration, validation, and testing activities.

4.4.1.7. *Sustainability and Future Evolution*

The long-term sustainability of the CURIUM Continuum is expected to rely on:

- continued exploitation of individual KERs by the respective partners;
- integration of additional functionalities and services over time;
- reuse of project outcomes within future initiatives and operational environments;
- alignment with evolving CRA-related regulatory and market developments.

Future evolution activities may include:

- enhancement of interoperability and orchestration capabilities;
- integration of additional cybersecurity tools supporting CRA compliance;
- further refinement of coordinated reporting and compliance-support mechanisms.

The modular architecture of the CURIUM ecosystem supports gradual evolution while maintaining flexibility regarding ownership, deployment, and exploitation approaches.

4.4.1.8. *Planned Post-Project Actions*

Following the completion of the project, the consortium partners intend to further evaluate possible coordinated operational and exploitation scenarios related to the CURIUM Continuum.

Potential post-project activities may include:

- further refinement and integration of interoperable services and tools;
- enhancement of coordinated reporting and compliance-support functionalities;
- identification of future funding and sustainability opportunities;
- continuation of validation and pilot-oriented activities;
- exploration of possible ecosystem-oriented operational models and collaboration mechanisms.

Depending on market interest, operational feasibility, available resources, and partner agreements, future activities may additionally explore more advanced integration and

coordinated service delivery approaches supporting the long-term evolution of the CURIUM ecosystem.

4.4.2. KER2 – Penetration Self-Testing and Vulnerability Assessment Services and tools (PSTVA) - Responsible Partner: AEGIS

The Penetration Self-Testing and Vulnerability Assessment Services and Tools (PSTVA) KER focuses on providing organisations with an integrated security assessment environment supporting vulnerability identification, penetration self-testing activities, and CRA-oriented security validation processes.

The PSTVA solution is designed to support organisations in identifying and assessing vulnerabilities affecting products, infrastructures, web services, and user management systems. The KER combines vulnerability assessment functionalities, penetration testing support mechanisms, reporting capabilities, and orchestration functionalities within a unified environment aligned with CRA-related cybersecurity and compliance requirements.

The PSTVA KER aims to simplify and automate security assessment activities while reducing the operational complexity typically associated with fragmented cybersecurity testing tools and manual reporting processes. The solution additionally supports the generation of standardised outputs that can be utilised within compliance documentation, audit-readiness activities, and cybersecurity assurance processes.

The KER is positioned within the “Security Validation & Testing” stage of the CURIUM Compliance Continuum and contributes to the broader CRA-oriented cybersecurity compliance lifecycle through interoperable integration with other CURIUM services and tools.

4.4.2.1. Target Market and Stakeholders

The PSTVA KER primarily targets organisations that require cybersecurity validation and vulnerability assessment capabilities in the context of CRA-related cybersecurity obligations.

The main target stakeholder groups include:

- SMEs and mid-sized enterprises developing or operating products with digital elements;
- organisations lacking dedicated internal cybersecurity expertise;
- cybersecurity service providers and consultants seeking integrated assessment capabilities;
- public sector organisations and authorities supporting cybersecurity preparedness initiatives;
- industry associations, competence centres, and Digital Innovation Hubs (DIHs);

- organisations operating in sectors such as Information Technology, Healthcare, Energy, Financial Services, Retail, and e-Commerce.

Emphasis is placed on SMEs and organisations with limited cybersecurity resources, where simplified, automated, and user-friendly assessment mechanisms can significantly reduce adoption barriers and operational complexity.

4.4.2.2. Value Proposition and Competitive Positioning

The PSTVA KER differentiates itself from traditional vulnerability assessment and penetration testing solutions through its integrated, modular, and compliance-oriented approach.

Unlike fragmented assessment environments requiring multiple disconnected tools and manual consolidation of results, PSTVA provides:

- centralised orchestration of vulnerability assessment and penetration testing activities;
- automated and semi-automated scanning capabilities;
- standardised reporting outputs aligned with CRA-related compliance activities;
- simplified operational workflows suitable for organisations with limited cybersecurity expertise;
- support for recurring and continuous assessment activities.

The solution additionally supports:

- reduction of manual effort and duplicated assessment activities;
- improved audit-readiness and compliance documentation;
- enhanced visibility of cybersecurity risks and vulnerabilities;
- improved operational efficiency through automation and integrated reporting;
- reduced dependency on external penetration testing services for basic assessment activities.

Through its integration within the CURIUM Compliance Continuum, the PSTVA KER additionally contributes to coordinated cybersecurity compliance workflows spanning risk management, compliance verification, and continuous monitoring activities.

4.4.2.3. Exploitation and Use Model

The PSTVA KER is expected to be commercially exploited primarily by AEGIS as a software-based cybersecurity assessment solution integrated within the broader CURIUM ecosystem. The exploitation approach may include:

- standalone licensing of the PSTVA platform;
- subscription-based Software-as-a-Service (SaaS) deployment models;
- integration within broader CURIUM Compliance Continuum service offerings;
- service-oriented deployment through consulting and managed security service activities;

- white-label or partner-oriented licensing arrangements.

The PSTVA KER may be offered through different deployment models depending on customer operational requirements, including cloud-based, SaaS, and potentially on-premise deployment approaches.

The exploitation approach additionally supports:

- recurring vulnerability assessment services;
- integration into cybersecurity consulting activities;
- support for CRA-related audit-readiness and compliance activities;
- integration with complementary cybersecurity assessment and governance services.

The KER may additionally support coordinated exploitation scenarios through interoperability with other CURIUM KERs and ecosystem-oriented service offerings.

4.4.2.4. IPR and Ownership Considerations

The PSTVA KER builds upon a combination of:

- existing AEGIS assets and know-how;
- integrated open-source components;
- project-developed orchestration and automation functionalities.

Ownership and exploitation rights remain aligned with the provisions of the Grant Agreement and the Consortium Agreement governing the CURIUM project.

AEGIS is expected to retain ownership of the core PSTVA integration framework, orchestration mechanisms, and value-added functionalities developed within the project context, while open-source components remain subject to their respective licensing conditions.

Jointly developed components and interoperability-related elements remain subject to the access-rights and collaboration provisions established within the Consortium Agreement and the broader governance framework of the CURIUM ecosystem.

4.4.2.5. Technical Maturity and Market Readiness

At the beginning of the project, the PSTVA KER was positioned at approximately TRL 7, reflecting an operational prototype and integrated assessment environment validated within relevant environments.

By the end of the project, the KER is expected to reach TRL 8 through:

- additional technical integration and refinement activities;
- validation within operational and pilot environments;
- enhancement of platform stability and deployment capabilities;
- improvement of reporting and orchestration functionalities;

- validation of CRA-oriented compliance support capabilities.

The post-project exploitation roadmap additionally foresees:

- market-oriented refinement activities;
- deployment hardening and scalability improvements;
- commercial packaging and licensing preparation;
- customer onboarding and validation with early adopters.

4.4.2.6. Adoption Challenges and Pain Relievers

The PSTVA exploitation approach addresses several key challenges currently affecting organisations attempting to implement CRA-related cybersecurity assessment activities.

The identified stakeholder challenges include:

- difficulty interpreting CRA-related cybersecurity obligations;
- fragmented and disconnected assessment tools;
- lack of dedicated internal cybersecurity expertise;
- high costs associated with external penetration testing services;
- complexity of generating standardised compliance-ready outputs;
- operational inefficiencies caused by manual reporting and result consolidation.

The PSTVA KER addresses these challenges through:

- automation of vulnerability assessment activities;
- centralised orchestration and reporting mechanisms;
- simplified operational workflows;
- reusable and standardised compliance-oriented outputs;
- recurring assessment capabilities supporting continuous monitoring;
- reduction of dependency on highly specialised external resources.

4.4.2.7. Post-Project Exploitation Actions

Following project completion, AEGIS is expected to continue the transition of PSTVA towards a commercially exploitable cybersecurity assessment solution.

The planned post-project activities may include:

- technical refinement and optimisation of the platform;
- deployment hardening and production-readiness activities;
- performance testing and infrastructure stabilisation;
- preparation of commercial licensing and service models;
- onboarding of pilot customers and early adopters;
- development of customer support and maintenance processes;
- alignment with evolving CRA implementing acts and cybersecurity requirements;

- establishment of partnerships with cybersecurity providers and certification-related stakeholders.

Additional activities may include:

- preparation of End-User License Agreements (EULAs);
- compliance evaluation of integrated open-source components;
- commercial packaging of standalone and integrated deployment models;
- participation in demonstrations, webinars, and ecosystem-oriented dissemination activities.

4.4.2.8. Roles and Responsibilities

AEGIS is expected to act as the primary exploitation lead for the PSTVA KER and to coordinate the post-project commercialisation and operational roadmap.

Additional consortium partners may contribute through:

- technical refinement and interoperability support activities;
- dissemination and communication support;
- pilot validation and early adoption activities;
- regulatory, compliance, and standardisation guidance;
- integration support within the broader CURIUM Compliance Continuum.

The exploitation activities may additionally involve collaboration with:

- cybersecurity service providers;
- Digital Innovation Hubs (DIHs);
- certification and conformity assessment actors;
- public-sector cybersecurity support initiatives.

4.4.2.9. Milestones and KPIs

Indicative post-project milestones may include:

Milestone	Indicative Timeline
Initial business and licensing framework	Months 1–3
Production-ready PSTVA release	Months 3–6
Initial pilot customer onboarding	Months 6–9
Commercial deployment preparation	Months 9–12
Expansion of deployment and partnership activities	Year 2 onwards

Table 9: PSTVA (KER2) – Indicative Post-Project Milestones and KPIs

Indicative KPIs may include:

- number of pilot users and early adopters;
- number of recurring assessment deployments;
- customer satisfaction indicators;
- number of integrated cybersecurity workflows;
- number of service-provider partnerships;
- growth of recurring subscription or service revenues.

4.4.2.10. Cost and Revenue Considerations

The methodology includes an analysis for cost and revenue considerations. This information due to their sensitive business nature is not included in the public version of the document.

4.4.2.11. Sustainability and Long-Term Evolution

The long-term sustainability of the PSTVA KER is expected to be supported through:

- continuous alignment with CRA-related cybersecurity requirements;
- recurring vulnerability assessment and monitoring services;
- integration into broader cybersecurity compliance workflows;
- interoperability with complementary CURIUM services and external ecosystems;
- ongoing technical evolution based on stakeholder feedback and operational validation activities.

The modular architecture of the KER additionally supports future scalability, integration of additional assessment functionalities, and adaptation to evolving cybersecurity and regulatory requirements.

4.4.3. KER3 – CRA Scoping and Product Classification Service (CyReA) - Responsible Partner: NLG

The CRA Scoping and Product Classification Service (CyReA) is designed to support organisations in determining whether products fall within the scope of the Cyber Resilience Act (CRA) and in identifying the corresponding compliance obligations and classification requirements.

The CyReA KER operates as a structured, question-based guidance and scoping service enabling users to perform initial CRA applicability and product classification activities in a systematic and user-friendly manner. It supports organisations in identifying whether their products fall within the scope of the CRA and in initiating the compliance process based on the characteristics of products with digital elements.

The service is designed to simplify the interpretation of CRA-related obligations and reduce the complexity associated with product scoping and regulatory understanding,

particularly for SMEs and organisations with limited regulatory and cybersecurity expertise.

Within the CURIUM Compliance Continuum, CyReA contributes to the “Scope & Classification” stage of the CRA-oriented cybersecurity compliance lifecycle. It serves as an entry-point for the organizations, facilitating the transition to subsequent compliance activities, including assessment, testing, and risk management.

4.4.3.1. Target Market and Stakeholders

The CyReA KER primarily targets organisations involved in the development, import, distribution, operation, or maintenance of products with digital elements affected by CRA-related obligations.

The main target stakeholders include:

- SMEs and micro-enterprises;
- manufacturers and product developers;
- importers and distributors;
- service providers and integrators;
- organisations with limited internal regulatory expertise;
- cybersecurity consultants and compliance-support providers;
- public authorities and ecosystem-support organisations.

Emphasis is placed on organisations requiring simplified and accessible guidance mechanisms supporting the interpretation of CRA applicability and product classification obligations.

4.4.3.2. Value Proposition and Competitive Positioning

The CyReA KER provides a structured and accessible approach for determining CRA applicability and product classification requirements.

The service differentiates itself through:

- simplified and guided CRA scoping workflows;
- reduction of manual effort related to regulatory interpretation;
- user-friendly question-based interaction mechanisms;
- support for organisations lacking specialised CRA expertise;
- integration within the broader CURIUM Compliance Continuum.

The CyReA KER supports organisations by:

- reducing uncertainty regarding CRA applicability;
- simplifying initial product classification activities;
- supporting internal understanding of CRA obligations;
- reducing dependency on external regulatory consultants;
- enabling organisations to initiate CRA compliance activities more efficiently.

Through its integration with other CURIUM KERs, CyReA additionally contributes to the creation of coordinated cybersecurity and compliance workflows spanning assessment, risk management, testing, and compliance verification activities.

4.4.3.3. Exploitation and Use Model

The CyReA KER is expected to operate as a digital guidance and CRA scoping service integrated within the broader CURIUM ecosystem.

The exploitation approach may include:

- integration within the CURIUM Compliance Continuum;
- standalone access to CRA scoping functionalities;
- service-oriented deployment through compliance-support activities;
- integration into consulting and advisory services;
- support for training and awareness activities related to CRA obligations.

The CyReA service is expected to support recurring usage scenarios, particularly during:

- product onboarding activities;
- initial compliance preparation phases;
- product portfolio assessments;
- internal compliance readiness activities.

The exploitation logic additionally supports interoperability with complementary CURIUM services related to risk assessment, compliance verification, maturity assessment, and vulnerability testing.

4.4.3.4. IPR and Ownership Considerations

The CyReA KER builds upon:

- project-developed CRA scoping methodologies;
- partner expertise related to cybersecurity and regulatory compliance;
- structured guidance workflows and classification logic developed within the CURIUM project context.

Ownership and access-rights considerations remain aligned with the Grant Agreement and Consortium Agreement governing the CURIUM project.

The exploitation and reuse of CyReA components are expected to follow the governance and interoperability principles defined for the broader CURIUM ecosystem and Compliance Continuum.

4.4.3.5. Technical Maturity and Market Readiness

At the beginning of the project, the CyReA KER was positioned at TRL 6. The current technical maturity of the solution is assessed at TRL 7, while the envisaged technical maturity at the end of the project is TRL 8.

The CyReA KER is positioned as a structured digital guidance and assessment support service intended to facilitate early-stage CRA compliance preparation activities.

The post-project roadmap foresees:

- refinement of question-based scoping workflows;
- validation of usability and stakeholder interaction mechanisms;
- enhancement of guidance and classification functionalities;
- integration with complementary CURIUM services and workflows;
- validation with pilot users and early adopters.

The exploitation activities additionally aim to support:

- increased usability for non-expert stakeholders;
- scalability across different organisational profiles;
- alignment with evolving CRA implementation requirements and regulatory guidance.

4.4.3.6. Adoption Challenges and Pain Relievers

The CyReA exploitation approach addresses several key barriers affecting organisations attempting to understand and implement CRA-related obligations.

The identified stakeholder challenges include:

- difficulty understanding CRA applicability and classification requirements;
- limited regulatory and cybersecurity expertise;
- uncertainty regarding compliance obligations;
- dependency on external experts and consultants;
- complexity of interpreting regulatory terminology and obligations.

The CyReA KER addresses these challenges through:

- structured and guided scoping workflows;
- simplified user interaction mechanisms;
- reduction of manual interpretation effort;
- accessible and user-friendly guidance approaches;
- support for internal understanding and decision-making activities.

The service additionally supports increased organisational confidence during the early stages of CRA compliance preparation.

4.4.3.7. Post-Project Exploitation Actions

Following project completion, NLG intends to continue the technical, operational, and commercial evolution of CyReA through:

- refinement of CRA scoping methodologies;
- expansion of product classification and guidance capabilities;

- integration with additional compliance-support services;
- enhancement of usability and accessibility mechanisms;
- validation with pilot users and stakeholder communities;
- integration into broader cybersecurity consulting and compliance-support activities.

Additional activities may include:

- adaptation to evolving CRA implementing acts and guidance;
- development of additional training and awareness materials;
- support for ecosystem-oriented onboarding and adoption activities;
- integration into Digital Innovation Hub and SME-support initiatives.

In parallel, NLG intends to finalise the exploitation and commercialisation strategy, establish partnerships with industry stakeholders, complete the necessary intellectual property and governance arrangements, prepare user support and training resources, validate operational and compliance requirements, and establish the organisational processes and resources required for the long-term maintenance and evolution of the service.

4.4.3.8. Roles and Responsibilities

NLG will be primarily responsible for the exploitation of CyReA, including the implementation of the exploitation roadmap, business planning, stakeholder engagement, commercialisation activities, and long-term maintenance of the solution.

Other consortium partners are expected to contribute through technical support, dissemination and communication activities, training and capacity-building actions, networking, stakeholder engagement, and the exploration of future collaboration and funding opportunities.

The governance and operational coordination of the CyReA KER are expected to remain aligned with the broader governance framework established for the CURIUM ecosystem.

4.4.3.9. Milestones and KPIs

Indicative post-project milestones may include:

Milestone	Indicative Timeline
Refinement of CRA scoping workflows	Months 1–3
Stakeholder outreach and market engagement	Months 1–6
Validation with pilot users	Months 3–6
Exploration of follow-up funding opportunities	Months 1–6
Integration with complementary KERs	Months 6–9
Technical improvements and feature enhancements	Months 1–9

Expansion of stakeholder onboarding activities	Months 9–12
Broader ecosystem-oriented deployment activities	Year 2 onwards

Table 10: CyReA (KER3) – Indicative Post-Project Milestones and KPIs

Indicative KPIs may include:

- number of organisations using the service;
- number of CRA scoping assessments performed;
- stakeholder satisfaction indicators;
- integration with complementary compliance workflows;
- number of ecosystem and dissemination activities supported;
- level of adoption by SMEs and micro-enterprises.

4.4.3.10. Cost and Revenue Considerations

The methodology includes an analysis for cost and revenue considerations. This information due to their sensitive business nature is not included in the public version of the document.

4.4.3.11. Sustainability and Long-Term Evolution

The long-term sustainability of the CyReA KER is expected to be supported through:

- continuous alignment with evolving CRA-related requirements;
- integration within the CURIUM Compliance Continuum;
- recurring use during product onboarding and compliance preparation activities;
- integration into broader cybersecurity compliance ecosystems;
- ongoing refinement based on stakeholder feedback and regulatory developments.

The costs associated with further development and exploitation of CyReA are expected to be covered primarily through NLG's own resources and budget, complemented where appropriate by external funding opportunities and future collaborative initiatives.

The modular nature of the service additionally supports future scalability, interoperability, and extension towards additional cybersecurity and regulatory guidance functionalities.

4.4.4. KER4 – Digital Product Risk Management (DPRA) - Responsible Partner: NLG

The Digital Product Risk Management (DPRA) KER supports organisations in identifying, assessing, modelling, and managing cybersecurity risks associated with products with digital elements within the context of the Cyber Resilience Act (CRA).

The solution enables dynamic cybersecurity risk assessment by incorporating temporal and contextual parameters related to ICT products, including vulnerabilities, asset

dependencies, attack paths, and cascading risk scenarios. It provides a structured, holistic, and cost-effective approach to assess cybersecurity risk, while supporting decision-making processes for compliance and risk mitigation.

The DPRA KER integrates multiple risk-management-related functionalities, including:

- vulnerability identification and management;
- ICT product and asset declaration;
- asset dependency modelling;
- threat and control declaration mechanisms;
- support for cybersecurity taxonomy and standards integration.

Within the CURIUM Compliance Continuum, DPRA contributes to the Risk Management stage of the CRA aligned cybersecurity lifecycle. It supports broader compliance workflows through interoperability with complementary assessment, testing, and compliance-support services.

4.4.4.1. Target Market and Stakeholders

The DPRA KER primarily targets organisations requiring cybersecurity risk-management capabilities related to products with digital elements and CRA-related obligations.

The main target stakeholders include:

- risk and compliance managers;
- cybersecurity analysts and auditors;
- product security engineers;
- organisations operating critical infrastructure;
- organisations in the financial and healthcare sectors;
- cybersecurity service providers and consultants;
- SMEs and organisations lacking mature internal risk-management capabilities.

The KER is designed to support both technically mature organisations and organisations with limited cybersecurity expertise requiring structured risk-assessment and compliance-support mechanisms.

4.4.4.2. Value Proposition and Competitive Positioning

The DPRA KER differentiates itself through its integrated and dynamic approach to cybersecurity risk management within CRA-oriented compliance environments.

The solution provides:

- dynamic assessment of cybersecurity risks;
- modelling of asset dependencies and attack paths;
- real-time identification of relevant vulnerabilities;
- integration of recognised cybersecurity taxonomies and standards;
- support for structured threat and mitigation management activities.

The KER additionally supports:

- integration of open intelligence sources and cybersecurity catalogues;
- alignment with recognised standards and frameworks such as NIST, MITRE, FIRST, NIST 800-53, and ISO/IEC 15408;
- improved visibility of asset relationships and cascading cybersecurity risks;
- enhanced organisational understanding of threats, vulnerabilities, and mitigation controls.

Compared to fragmented or static risk-management approaches, the DPRA KER provides a more integrated and operationally oriented environment supporting both cybersecurity analysis and CRA-related compliance activities.

4.4.4.3. Exploitation and Use Model

The DPRA KER is expected to operate as an integrated risk-management component within the broader CURIUM Compliance Continuum.

DPRA may be deployed either as a standalone service accessible through a standard web browser or as an integrated component of the broader CURIUM Compliance Continuum through the CURIUM Portal.

The exploitation approach may include:

- subscription-based access to the DPRA platform and services;
- integration within the CURIUM Portal and ecosystem;
- service-oriented deployment through cybersecurity consulting and assessment activities;
- support for recurring risk assessment and monitoring activities;
- integration into broader governance, risk, and compliance (GRC) workflows.

The DPRA KER is expected to support:

- recurring risk-assessment activities;
- continuous vulnerability and dependency monitoring;
- cybersecurity decision-support activities;
- internal audit and compliance-support processes;
- risk prioritisation and mitigation planning activities.

The exploitation logic additionally supports interoperability with complementary CURIUM KERs related to scoping, testing, compliance verification, and maturity assessment.

4.4.4.4. IPR and Ownership Considerations

The DPRA KER builds upon:

- project-developed cybersecurity risk-management methodologies;
- partner expertise and background assets;

- integrated threat intelligence and open-source components;
- interoperability and orchestration functionalities developed within the CURIUM project context.

Ownership and exploitation rights remain aligned with the provisions of the Grant Agreement and Consortium Agreement governing the CURIUM project.

The Consortium Agreement defines the copyright and usage-rights framework related to the project outputs and associated platform components. The exploitation and operational governance of the DPRA KER remain aligned with the broader governance structure established for the CURIUM Compliance Continuum.

4.4.4.5. Technical Maturity and Market Readiness

At the beginning of the project, the DPRA KER was positioned at TRL 6. The current technical maturity of the solution is assessed at TRL 7, while the envisaged technical maturity at the end of the project is TRL 8.

The DPRA KER is positioned as an operational cybersecurity risk-management environment supporting CRA-related compliance and security management activities.

The exploitation roadmap foresees:

- additional refinement and customisation activities;
- enhancement of modelling and dependency-analysis capabilities;
- validation within pilot and operational environments;
- integration of additional threat intelligence and taxonomy sources;
- improvement of usability and interoperability functionalities.

According to the current exploitation expectations, broader market-readiness activities are expected to continue during the post-project phase through iterative refinement and stakeholder-driven evolution activities.

4.4.4.6. Adoption Challenges and Pain Relievers

The DPRA exploitation approach addresses several key challenges affecting organisations attempting to implement cybersecurity risk-management and CRA-related compliance processes.

The identified stakeholder challenges include:

- complexity of cybersecurity risk-management activities;
- fragmented visibility of vulnerabilities and asset dependencies;
- difficulty identifying cascading risks and attack paths;
- lack of structured risk-management methodologies;
- limited cybersecurity expertise and operational resources;
- challenges associated with integrating technical and compliance-related activities.

The DPRA KER addresses these challenges through:

- centralised and integrated risk-management functionalities;
- dynamic modelling of asset dependencies and vulnerabilities;
- structured threat and mitigation management mechanisms;
- integration of recognised cybersecurity standards and taxonomies;
- support for continuous monitoring and recurring assessment activities;
- reduction of manual effort associated with cybersecurity analysis and documentation activities.

The solution additionally supports improved organisational awareness and more informed cybersecurity decision-making processes.

4.4.4.7. Post-Project Exploitation Actions

Following project completion, the DPRA KER is expected to continue evolving through:

- refinement of cybersecurity modelling and analysis functionalities;
- expansion of interoperability and orchestration capabilities;
- integration of additional threat intelligence sources and frameworks;
- enhancement of usability and stakeholder interaction mechanisms;
- validation through pilot and operational deployments;
- integration into broader cybersecurity and compliance-support services.

Additional post-project activities may include:

- development of additional deployment and licensing models;
- support for ecosystem-oriented service offerings;
- integration into managed cybersecurity and consulting services;
- expansion of support for evolving CRA-related requirements and standards.

In parallel, NLG will finalise the exploitation and commercialisation strategy, complete the necessary intellectual property and governance arrangements, engage with potential users and industry stakeholders, prepare user documentation and training materials, address relevant compliance requirements, and establish the resources and responsibilities required for the long-term maintenance, operation, and further development of DPRA.

4.4.4.8. Roles and Responsibilities

NLG will be primarily responsible for the exploitation of DPRA, including the implementation of the exploitation roadmap, business planning, stakeholder engagement, commercialisation activities, and long-term maintenance of the solution. Other consortium partners are expected to contribute through technical support, dissemination activities, training and capacity-building actions, networking activities, and the exploration of future collaboration and funding opportunities.

The governance and operational coordination of DPRA remain aligned with the broader governance framework established for the CURIUM Compliance Continuum and the associated Consortium Agreement provisions.

4.4.4.9. Milestones and KPIs

Indicative post-project milestones may include:

Milestone	Indicative Timeline
Refinement of risk-modelling functionalities	Months 1–3
Stakeholder outreach and market engagement	Months 1–6
Integration of additional intelligence sources	Months 3–6
Exploration of follow-up funding opportunities	Months 1–6
Pilot validation and usability refinement	Months 6–9
Technical improvements and feature enhancements	Months 1–9
Expanded deployment and ecosystem integration	Months 9–12
Broader operational and commercial deployment	Year 2 onwards

Table 11: DPRA (KER4) – Indicative Post-Project Milestones and KPIs

Indicative KPIs may include:

- number of organisations using the DPRA service;
- number of risk assessments performed;
- number of integrated assets and dependencies analysed;
- stakeholder satisfaction indicators;
- number of recurring assessment workflows;
- integration with complementary cybersecurity and compliance services.

4.4.4.10. Cost and Revenue Considerations

The methodology includes an analysis for cost and revenue considerations. This information due to their sensitive business nature is not included in the public version of the document.

4.4.4.11. Sustainability and Long-Term Evolution

The long-term sustainability of the DPRA KER is expected to be supported through:

- continuous alignment with evolving CRA requirements and cybersecurity standards;
- integration within the CURIUM Compliance Continuum;
- recurring use in operational risk-management and compliance workflows;
- integration of additional threat intelligence and cybersecurity taxonomies;

- ongoing refinement based on stakeholder feedback and operational validation activities.

The costs associated with further development and exploitation of DPRA are expected to be covered primarily through NLG's own resources and budget, complemented where appropriate by external funding opportunities and future collaborative initiatives.

The modular and interoperable architecture of the DPRA KER additionally supports future scalability, integration with complementary cybersecurity ecosystems, and adaptation to evolving cybersecurity and regulatory challenges.

4.4.5. KER5 – Conformity Assessment and Compliance Service (CAC) - Responsible Partner: CYS

The Conformity Assessment and Compliance Service (CAC) is designed to support organisations in evaluating and managing compliance with the Cyber Resilience Act (CRA). The service assists organisations in identifying compliance gaps, supporting technical documentation management, performing post-market analysis activities, and facilitating the preparation of evidence required for conformity assessment processes.

The CAC service integrates multiple functionalities within a unified environment, including:

- automated compliance verification mechanisms;
- SBOM parsing and analysis;
- technical documentation management;
- post-market monitoring support;
- generation of audit-oriented compliance evidence and reports.

The service aims to simplify CRA-related compliance activities and reduce the operational burden associated with conformity assessment and audit-readiness processes, particularly for SMEs and organisations with limited cybersecurity expertise.

4.4.5.1. Target Market and Stakeholders

The primary target stakeholders of CAC include:

- SMEs and micro-enterprises developing or distributing products with digital elements;
- manufacturers, importers, and distributors affected by CRA obligations;
- product managers and technical leads responsible for compliance activities;
- non-expert users involved in regulatory or documentation processes;
- organisations preparing for external audits, conformity assessments, or certification activities.

CAC is positioned as a modular and user-oriented compliance support service that combines technical assessment, compliance guidance, and automated documentation support within the broader CURIUM Compliance Continuum.

4.4.5.2. Value Proposition and Competitive Positioning

The CAC service differentiates itself through:

- integrated compliance-oriented workflows;
- automated SBOM parsing and evidence generation;
- support for post-market monitoring activities;
- user-friendly interfaces designed for organisations with limited cybersecurity expertise;
- interoperability with broader CURIUM ecosystem services.

The value proposition of CAC focuses on:

- reducing manual compliance effort;
- improving audit-readiness and documentation consistency;
- lowering dependency on external consultancy services;
- enabling organisations to internally manage parts of CRA compliance activities;
- supporting continuous compliance monitoring and post-market obligations.

The service additionally supports the generation of structured outputs that can be used during conformity assessment and audit activities, including:

- technical documentation support;
- compliance reports;
- assessment outputs and compliance-related artefacts.

4.4.5.3. Exploitation and Use Model

The CAC service is expected to operate both:

- as a standalone compliance support service;
- and as an integrated component of the CURIUM Compliance Continuum.

The exploitation approach includes:

- cloud-based access through the CURIUM portal;
- modular integration with complementary KERs;
- advisory and support services;
- training and awareness activities supporting adoption and operational use.

The service is additionally expected to support:

- SME-oriented compliance assistance;
- pilot validation activities;

- collaboration with Digital Innovation Hubs and cybersecurity ecosystems;
- future interoperability with certification and conformity assessment ecosystems.

4.4.5.4. IPR and Ownership Considerations

The CAC service is developed within the framework of the CURIUM Consortium Agreement and follows the project's IPR and exploitation governance principles.

Ownership and exploitation rights are managed according to:

- the Grant Agreement;
- the Consortium Agreement;
- partner-specific ownership and exploitation responsibilities.

The exploitation of CAC is expected to follow a coordinated and federated model, where specific partners contribute complementary technical, operational, dissemination, commercialisation, infrastructure, and regulatory-support capabilities. The CAC service is intended to remain interoperable with other CURIUM KERs while allowing individual partners to exploit specific components, services, or supporting activities according to their respective ownership rights and exploitation strategies.

The exploitation roadmap foresees a combination of:

- partner-owned background assets and services;
- project-developed functionalities and integrations;
- modular deployment and interoperability mechanisms;
- service-oriented and ecosystem-oriented exploitation approaches.

The service is designed to remain interoperable with external certification, audit, and cybersecurity services while supporting both standalone and integrated exploitation approaches within the broader CURIUM ecosystem.

The post-project exploitation activities may additionally include:

- refinement of licensing and access models;
- definition of operational ownership and long-term maintenance responsibilities;
- exploration of open-source and commercial deployment approaches;
- establishment of collaboration mechanisms with external cybersecurity, certification, and Digital Innovation Hub ecosystems.

4.4.5.5. Technical Maturity and Market Readiness

The CAC service evolved during the project from an initial maturity level of approximately TRL 6 towards TRL 7–8 by the end of the project through:

- integration of compliance-oriented functionalities;
- pilot validation activities;

- refinement based on stakeholder feedback;
- enhancement of usability and interoperability aspects.

Future evolution activities may include:

- extension of post-market monitoring functionalities;
- enhanced automation capabilities;
- integration with additional regulatory and conformity assessment frameworks;
- expansion of interoperability with external cybersecurity and certification ecosystems.

4.4.5.6. Adoption Challenges and Pain Relievers

The adoption of the CAC service is expected to be influenced by several operational, technical, and organisational challenges commonly faced by SMEs and organisations affected by CRA-related compliance obligations.

The main adoption challenges identified include:

- limited internal expertise related to CRA compliance and conformity assessment processes;
- complexity of technical documentation and evidence management activities;
- difficulty interpreting regulatory obligations and post-market requirements;
- high dependency on external consultancy and specialised cybersecurity services;
- fragmented compliance workflows and disconnected assessment activities;
- limited organisational resources available for continuous compliance monitoring and audit preparation.

In order to address these challenges, the CAC service incorporates several pain-relieving and adoption-support mechanisms, including:

- automation of compliance-oriented assessment and reporting activities;
- user-friendly interfaces supporting non-expert users;
- integrated technical documentation and evidence management functionalities;
- SBOM parsing and automated compliance evidence generation;
- support for post-market monitoring and compliance tracking activities;
- modular integration with complementary CURIUM KERs and services.

The service additionally aims to reduce operational complexity and compliance effort by:

- simplifying conformity assessment preparation activities;
- improving consistency and traceability of compliance-related artefacts;
- supporting gradual adoption according to organisational maturity levels;

- facilitating interoperability between assessment, testing, and compliance activities;
- providing structured outputs suitable for audit-readiness and regulatory-support processes.

Training, awareness, and support activities integrated within the broader CURIUM ecosystem are additionally expected to contribute to:

- increased stakeholder confidence and usability;
- improved adoption by organisations with limited cybersecurity expertise;
- reduction of barriers associated with CRA-related compliance obligations;
- long-term operational sustainability and ecosystem-oriented uptake of the service.

4.4.5.7. Post-Project Exploitation Actions

Following project completion, the consortium partners involved in CAC intend to:

- further refine and stabilise the service for operational deployment;
- enhance automation and reporting functionalities;
- improve integration with complementary CURIUM services;
- validate the service through additional pilot and early-adopter activities;
- support market uptake through dissemination, training, and ecosystem engagement activities.

Additional activities may include:

- preparation of commercial and operational deployment models;
- development of service-level support mechanisms;
- participation in future cybersecurity and compliance initiatives;
- exploration of sustainability and long-term operational governance approaches.

4.4.5.8. Roles and Responsibilities

The exploitation and operational responsibilities related to the CAC service are expected to be distributed among the involved consortium partners according to their respective technical expertise, ownership rights, operational capabilities, and exploitation interests.

Indicative responsibilities may include:

- development and maintenance of compliance-oriented functionalities;
- integration of SBOM parsing and technical documentation management capabilities;
- provision of infrastructure and operational support services;
- coordination of interoperability with complementary CURIUM KERs;

- support for pilot validation and stakeholder engagement activities;
- dissemination, training, and awareness activities related to CRA compliance and conformity assessment support;
- contribution to future commercialisation, sustainability, and ecosystem integration activities.

The governance and coordination of the service are expected to follow the broader operational and interoperability principles defined for the CURIUM Compliance Continuum, while allowing individual partners to maintain ownership and exploitation rights over their respective components and services.

Additional responsibilities related to operational governance, service maintenance, onboarding of additional functionalities, and ecosystem collaboration mechanisms may be further refined during post-project exploitation and sustainability activities.

4.4.5.9. Milestones and KPIs

The post-project evolution and exploitation of the CAC service are expected to follow a progressive roadmap focused on technical refinement, interoperability enhancement, validation activities, and gradual operational deployment.

Milestone	Indicative Timeline
Refinement of compliance verification and documentation management functionalities	Months 1–3
Enhancement of SBOM parsing and automated reporting capabilities	Months 3–6
Pilot validation and usability refinement activities	Months 6–9
Expanded interoperability with complementary CURIUM KERs and external services	Months 9–12
Broader operational deployment and ecosystem-oriented exploitation activities	Year 2 onwards

Table 12: CAC (KER5) – Indicative Post-Project Milestones and KPIs

Indicative KPIs associated with the CAC service may include:

- number of organisations using the service during pilot and validation activities;
- number of generated compliance reports and assessment artefacts;
- level of interoperability achieved with complementary CURIUM services;
- user satisfaction and usability evaluation results;
- number of dissemination, training, and awareness activities related to CAC;

- level of adoption by SMEs and organisations with limited cybersecurity expertise;
- number of ecosystem collaborations and integration activities established post-project.

The KPIs are expected to evolve progressively according to the maturity, deployment scope, and operational adoption of the service.

4.4.5.10. Cost and Revenue Considerations

The methodology includes an analysis for cost and revenue considerations. This information due to their sensitive business nature is not included in the public version of the document.

4.4.5.11. Sustainability and Long-Term Evolution

The sustainability of CAC may be supported through:

- subscription-based access models;
- consulting and advisory services;
- integration into partner service portfolios;
- training and support activities;
- participation in future funded initiatives and cybersecurity ecosystems.

The exploitation approach aims to balance:

- accessibility for SMEs and organisations with limited resources;
- operational sustainability;
- long-term evolution and interoperability within the broader CURIUM Compliance Continuum.

4.4.6. KER6 – Digital Product Maturity Assessment (DPMA) - Responsible Partner: APIRO

The Digital Product Maturity Assessment (DPMA) tool is designed to support organisations in assessing cybersecurity maturity and identifying appropriate cybersecurity measures aligned with recognised standards and frameworks. The tool combines multiple standardisation resources, international publications, and cybersecurity references to support organisations in selecting and prioritising cybersecurity controls according to maturity levels and risk management needs.

The DPMA tool additionally supports the mapping of cybersecurity measures against maturity scales and ISO/IEC 27001-related controls, enabling organisations to evaluate their current security posture and identify potential improvement areas.

The service aims to simplify the cybersecurity compliance journey by providing structured and searchable access to cybersecurity controls, standards, and

implementation guidance, particularly for organisations with limited cybersecurity expertise.

4.4.6.1. Target Market and Stakeholders

The primary target stakeholders of DPMA include:

- organisations implementing cybersecurity and risk management measures;
- SMEs and manufacturers involved in CRA-related compliance activities;
- cybersecurity consultants and service providers;
- risk and compliance managers;
- organisations seeking structured maturity assessment and cybersecurity improvement support.

The DPMA service is positioned as a maturity-oriented cybersecurity support mechanism capable of assisting organisations in identifying, selecting, and prioritising cybersecurity measures according to operational and regulatory needs.

4.4.6.2. Value Proposition and Competitive Positioning

The DPMA service differentiates itself through:

- integration of multiple cybersecurity standards and publications;
- structured mapping of cybersecurity measures against maturity levels;
- searchable and consolidated access to cybersecurity controls and guidance;
- support for self-assessment and progressive cybersecurity improvement;
- reduction of dependency on costly expert advisory services.

The value proposition of DPMA focuses on:

- simplifying the identification of cybersecurity measures and controls;
- reducing the effort required to analyse multiple standards and publications manually;
- supporting organisations in understanding cybersecurity maturity progression;
- improving accessibility of cybersecurity knowledge for non-expert users;
- supporting internal cybersecurity planning and decision-making activities.

The tool additionally supports:

- identification of cybersecurity measures applicable to specific threats or domains;
- identification of controls aligned with ISO/IEC 27001 requirements;
- maturity-based assessment of implemented cybersecurity measures;
- structured cybersecurity self-assessment activities.

4.4.6.3. Exploitation and Use Model

The DPMA functionality is expected to operate primarily as an integrated or bundled component within broader cybersecurity risk assessment or compliance-oriented services rather than as a fully standalone product.

The current exploitation approach focuses on:

- integration with complementary cybersecurity or compliance services;
- incorporation into broader CRA-related assessment environments;
- support of risk assessment and maturity evaluation activities;
- gradual enhancement of AI-assisted and standards-based functionalities.

Although standalone deployment scenarios may be explored in the future, the current business and exploitation assumption is that DPMA will create higher value as part of integrated cybersecurity or compliance offerings.

4.4.6.4. IPR and Ownership Considerations

The DPMA tool is based on pre-existing partner-owned knowledge assets and cybersecurity resources introduced into the project framework.

According to the Consortium Agreement and project exploitation framework:

- ownership of the original DPMA tool and related background assets remains with APIROPLUS Services Ltd.;
- project-developed enhancements and integrations are governed according to the project's IPR framework;
- access and exploitation rights are managed according to the provisions of the Grant Agreement and Consortium Agreement;
- access to specific internal functionalities, mappings, and supporting resources may be subject to partner-defined restrictions and usage conditions.

The tool additionally incorporates references and mappings derived from standards and publications protected under their respective copyright and licensing conditions.

4.4.6.5. Technical Maturity and Market Readiness

The DPMA tool evolved during the project from an initial maturity level of approximately TRL 6 towards TRL 7–8 by the end of the project through:

- refinement of cybersecurity mappings and maturity models;
- integration of additional cybersecurity references and standards;
- enhancement of usability and search capabilities;
- progressive automation and AI-supported functionalities.

Future evolution activities may include:

- further enhancement of AI-supported recommendation mechanisms;
- extension of supported cybersecurity standards and frameworks; additional interoperability and integration capabilities;
- enhanced maturity analytics and reporting functionalities.

4.4.6.6. Adoption Challenges and Pain Relievers

The adoption of the DPMA service may be affected by several operational and organisational challenges, particularly for SMEs and organisations with limited cybersecurity expertise and resources.

The identified challenges include:

- limited access to expert cybersecurity resources and consultancy services;
- high costs associated with cybersecurity advisory and maturity assessment activities;
- difficulty understanding and interpreting cybersecurity standards and publications;
- limited awareness regarding the existence of applicable cybersecurity standards and controls;
- lack of structured correlation between cybersecurity controls and maturity levels across different standards and publications;
- time-consuming manual analysis and comparison of cybersecurity measures and requirements.

Within this context, the DPMA service aims to reduce operational complexity and improve accessibility to cybersecurity maturity assessment activities by:

- providing structured and searchable access to cybersecurity measures and controls;
- simplifying the identification of cybersecurity measures applicable to specific threats, domains, or requirements;
- supporting cybersecurity self-assessment and maturity evaluation activities;
- reducing dependency on external expert advisory services;
- facilitating understanding of cybersecurity maturity progression and control implementation priorities;
- improving accessibility and usability of cybersecurity standards and related publications for non-expert users.

The service additionally supports organisations in reducing the effort required to identify, analyse, and prioritise cybersecurity controls, while contributing to more structured cybersecurity planning and decision-making activities.

4.4.6.7. Post-Project Exploitation Actions

Following project completion, the consortium partners involved in DPMA intend to:

- identify possible products and operational environments where the DPMA service may be integrated or bundled, particularly within cybersecurity risk assessment and compliance-oriented services;
- further enhance the platform based on validation workshop feedback and stakeholder recommendations;

- improve functionalities supporting identification and selection of cybersecurity measures already implemented within organisations;
- support easier identification of missing cybersecurity measures and maturity gaps;
- reduce duplication and inconsistencies originating from multiple cybersecurity publications and standards;
- explore additional normalisation mechanisms for cybersecurity maturity levels and mappings across different standards and resources;
- enhance AI-supported functionalities and recommendation mechanisms.

4.4.6.8. Roles and Responsibilities

The exploitation and operational evolution of the DPMA service is expected to be primarily coordinated by APIROPLUS Services LTD, which will lead:

- the exploitation roadmap and operational planning activities;
- the technical evolution and enhancement of the service;
- the integration and interoperability activities with complementary products and services;
- stakeholder engagement and future market-oriented activities related to the DPMA service.

4.4.6.9. Milestones and KPIs

Indicative post-project milestones may include:

Milestone	Indicative Timeline
Identification of potential integration products and operational use cases	Months 1–3
Refinement of maturity-assessment functionalities and usability improvements	Months 3–6
Implementation of technical enhancements based on validation workshop feedback	Months 4–6
Integration of additional cybersecurity standards, publications, and control mappings	Months 6–9
Introduction of AI-enhanced search and recommendation functionalities	Months 6–9
Pilot validation and refinement of maturity-level normalisation mechanisms	Months 9–12

Integration within broader cybersecurity risk assessment or compliance products/services	Year 2 onwards
Expanded operational deployment and ecosystem-oriented exploitation activities	Year 2 onwards

Table 13: DPMA (KER6) – Indicative Post-Project Milestones and KPIs

Indicative KPIs may include:

- number of integrated cybersecurity standards and publications;
- number of supported cybersecurity controls and maturity mappings;
- number of organisations using the service in pilot or operational environments;
- reduction of manual effort required for identifying cybersecurity measures;
- user satisfaction and usability evaluation results;
- number of integrations with complementary cybersecurity or compliance services;
- level of adoption within SME-oriented cybersecurity support activities.

4.4.6.10. Cost and Revenue Considerations

The methodology includes an analysis for cost and revenue considerations. This information due to their sensitive business nature is not included in the public version of the document.

4.4.6.11. Sustainability and Long-Term Evolution

The sustainability of DPMA may be supported through:

- partner-operated SaaS delivery models;
- integration into broader cybersecurity consulting and assessment activities;
- continuous enhancement of cybersecurity mappings and maturity resources;
- integration with future cybersecurity and compliance initiatives;
- reuse of the developed capabilities within future operational and research activities.

The long-term evolution of the DPMA service is expected to focus on:

- continuous alignment with evolving cybersecurity standards and frameworks;
- expansion of AI-supported functionalities;
- improvement of accessibility and usability for non-expert users;
- support for broader cybersecurity maturity and compliance ecosystems.

4.4.7. KER7 – CURIUM Capacity Building Plan and Services

The CURIUM Capacity Building Materials and Services portfolio brings together the knowledge resources, training activities, experimentation facilities, and support

services developed by the CURIUM consortium to facilitate the understanding, adoption, and practical application of the Cyber Resilience Act (CRA) and the project's key methodologies and tools.

The portfolio comprises a set of complementary capacity building assets developed and maintained by different consortium partners according to their areas of expertise. These assets combine reusable learning materials with practical support services, enabling organisations to acquire knowledge, assess their understanding, experiment with CURIUM methodologies and tools, and receive technical guidance throughout their adoption journey.

The portfolio is organised into two complementary categories:

- **Capacity Building Materials**, including training presentations, knowledge assessment materials, webinar recordings, and specialised training programmes.
- **Capacity Building Services**, including physical and online training, one-to-one consultations, experimentation and testing facilities, cyber range activities, and helpdesk services.

Together, these materials and services support different stages of organisational capacity building, ranging from awareness raising and knowledge acquisition to practical experimentation and operational support. Their complementary nature enables organisations with different stakeholder groups, technical expertise, and regulatory preparedness to access the resources and services that best address their specific needs, while supporting the effective adoption of the CURIUM Compliance Continuum.

4.4.7.1. Portfolio Composition

The CURIUM Capacity Building Materials and Services portfolio comprises a diverse set of learning resources, training materials, and support services developed by consortium partners throughout the project. Each portfolio component addresses specific capacity building needs, ranging from awareness raising and knowledge acquisition to hands-on experimentation and operational support.

The table below presents the capacity building materials and services included in the portfolio, together with their type, component, contributing partner(s), ownership model, and a brief description.

Type	Component	Partner(s)	Ownership	Description
Capacity Building Material	Training material / presentations	APIRO, 28D	Joint ownership	An introduction to the EU Cyber Resilience Act (CRA) and its implications for products with digital elements. The material

Type	Component	Partner(s)	Ownership	Description
				covers the scope of the CRA, essential cybersecurity requirements, economic operators and key obligations for organisations preparing for compliance.
Capacity Building Material	Webinar and workshop recordings	p-NET	100% owned by p-NET	Recordings from webinars and workshops organised by p-NET
Capacity Building Material	Training material / presentations	NCSA	100% owned by NCSA	An overview of the authorities involved in CRA implementation and the procedures for market surveillance, addressing product risks and handling non-compliance.
Capacity Building Material	Training material / presentations	NCSA	100% owned by NCSA	An overview of the CRA's scope, key definitions, product categories, obligations for manufacturers and other economic operators, and conformity assessment and CE marking.
Capacity Building Material	Training material / presentations	APIRO, P-NET	Joint ownership	A practical guide for SMEs exploring the European cybersecurity compliance landscape, with a focus on the Cybersecurity Act (CSA) and Cyber Resilience Act (CRA). The presentation introduces European cybersecurity

Type	Component	Partner(s)	Ownership	Description
				certification, CRA requirements, products with digital elements, conformity assessment and manufacturers' compliance responsibilities.
Capacity Building Material	Sphynx Cyber Range material	SPHYNX	100% owned by SPHYNX	A practical training resource designed to strengthen understanding of the Cyber Resilience Act and its application. Through scenario-based training and assessment activities, users explore CRA scope, cybersecurity obligations, vulnerability management, incident reporting and compliance requirements.
Capacity Building Material	Training material / presentations	APIRO	100% owned by APIRO	An exploration of the relationship between the EU AI Act and the Cyber Resilience Act, focusing on areas where cybersecurity and conformity requirements overlap. The presentation examines high-risk AI systems that also qualify as products with digital elements and how CRA cybersecurity requirements interact with the AI Act.

Type	Component	Partner(s)	Ownership	Description
Capacity Building Material	Training material / presentations	APIRO	100% owned by APIRO	A focused resource examining conformity assessment for high-risk AI systems under the EU AI Act and the role of testing in demonstrating compliance. It covers conformity assessment activities and bodies, internal and third-party assessment, quality management systems, technical documentation and testing requirements.
Capacity Building Material	CRA Technical Documentation Guidelines	CYS	100% owned by CYS	These guidelines follow the structure of Annex V of the Cyber Resilience Act (CRA). It is designed to help manufacturers, especially SMEs, to prepare compliant technical documentation.
Capacity Building Material	Questions for Knowledge Assessment	P-NET	100% owned by P-NET	Questions for Knowledge Assessment
Capacity Building Material	CRA awareness stickers	APIRO	100% owned by APIRO	CRA awareness stickers
Services	Physical or online training	APIRO	100% owned by APIRO	Provision of training services
Services	One-to-one consultations	APIRO	100% owned by APIRO	Provision of consultations on the use

Type	Component	Partner(s)	Ownership	Description
				of various CURIUM Continuum tools
Services	Cyber Range training	SPHYNX	100% owned by SPHYNX	Training programme for CRA awareness, accessible through Sphynx Cyber Range Platform
Services	Experimentation and testing facilities	p-NET	100% owned by p-NET	Offered to project partners and the project community following Testbed as a Service and Bring Your Own Use Case Business Models
Services	Helpdesk (physical at p-net)	p-NET	100% owned by p-NET	Provision of information and facilitation of meetings with project experts
Services	Experimentation and testing facilities	CYS	100% owned by CYS	Offered to project partners and external organisations as online or on-site training and support services to facilitate the adoption and effective use of the CAC methodology and related assessment tool.
Services	Helpdesk (online through portal and emails)	Consortium	Joint ownership	Technical support for CURIUM Compliance Continuum portal, individual tools, training and assessment resources.

Table 14: Overview of the CURIUM Capacity Building Materials and Services Portfolio

The portfolio combines reusable educational resources with practical support services, enabling organisations to progressively develop the knowledge and practical skills required for the adoption of the CRA and the effective use of CURIUM methodologies and tools. While some portfolio components support self-paced learning and awareness raising, others provide personalised guidance, hands-on experimentation, and technical assistance. Together, these complementary assets enable consortium partners to deliver tailored capacity building activities that address the diverse needs of different stakeholder groups and varying levels of cybersecurity maturity.

4.4.7.2. Exploitation and Use Model

The CURIUM Capacity Building Materials and Services portfolio is designed to support both standalone capacity building activities and the broader adoption of the CURIUM Compliance Continuum. The portfolio combines reusable learning resources with practical support services, allowing consortium partners to deliver training, awareness, experimentation, and technical assistance according to the needs of different stakeholder groups.

The exploitation model includes:

- provision of physical and online training activities;
- one-to-one consultation services supporting the adoption of CURIUM methodologies and tools;
- experimentation and testing facilities offered through partner infrastructures;
- cyber range-based training activities;
- webinar and workshop delivery supported by reusable educational material;
- helpdesk services providing technical guidance and user support;
- online access to selected materials and services through the CURIUM Compliance Continuum portal.

The portfolio enables individual partners to exploit and further develop their own materials and services while contributing to a common capacity building ecosystem supporting the adoption of CRA-related methodologies, tools, and services. Educational resources and support services may continue to be maintained, updated, and reused by their respective owners following the completion of the project, in accordance with the applicable ownership arrangements.

4.4.7.3. IPR and Ownership Considerations

The Capacity Building Materials and Services portfolio comprises both individually owned and jointly owned assets developed by consortium partners during the implementation of the CURIUM project. Ownership of each portfolio component remains with the partner(s) responsible for its development and is governed by the provisions of the Grant Agreement and the Consortium Agreement.

The table below summarises the ownership arrangements for the capacity building materials and services included in the portfolio.

Ownership Model	Portfolio Components
100% APIRO	Training material introducing the CSA and CRA; Training material on the CRA for National Cybersecurity Authorities (NCSAs)
100% SPHYNX	Cyber Range training programme
100% p-NET	Experimentation and testing facilities; Physical helpdesk services
100% NLG	Training materials related to CRA and CyReA; Experimentation and testing facilities supporting DPRA
100% CYS	Training materials related to CRA and CAC; Experimentation and testing facilities supporting CAC
Joint ownership	Knowledge assessment questions; Online helpdesk supporting the CURIUM Compliance Continuum

Table 15: Ownership of the CURIUM Capacity Building Materials and Services Portfolio

Individually owned portfolio components may continue to be maintained and exploited by their respective owners, while jointly owned assets are managed in accordance with the ownership and access rights defined in the Consortium Agreement. This ownership structure enables both partner-specific exploitation activities and the continued availability of shared capacity building resources within the CURIUM ecosystem.

4.4.7.4. Post-Project Exploitation Actions

Following the completion of the CURIUM project, consortium partners intend to continue exploiting and evolving the Capacity Building Materials and Services portfolio within their respective areas of responsibility. The post-project exploitation activities will focus on maintaining the relevance and usability of the portfolio while supporting the wider adoption of the CURIUM Compliance Continuum and its associated methodologies and tools.

The planned post-project actions include:

- maintaining and updating training and educational materials to reflect evolving CRA requirements and cybersecurity best practices;
- continuing the delivery of training, consultation, experimentation, and helpdesk services according to the expertise of the respective partners;
- expanding the portfolio with additional educational resources and awareness material where appropriate;
- supporting the onboarding and capacity building of organisations interested in adopting CURIUM methodologies and tools;
- continuing webinars, workshops, and other knowledge-sharing activities to promote the adoption of the portfolio and strengthen the CURIUM ecosystem.

The structure of the portfolio enables individual partners to further develop and exploit their own materials and services while contributing to a common capacity building ecosystem that can evolve beyond the lifetime of the project.

4.4.7.5. Cost and Revenue Considerations

The CURIUM Capacity Building Materials and Services portfolio is primarily intended to support knowledge transfer, capacity building, and the broader adoption of the CURIUM Compliance Continuum. Following project completion, the main costs associated with the portfolio are expected to relate to the maintenance and periodic update of educational materials, the organisation of training and awareness activities, the provision of support services, and the operation of online resources and experimentation facilities.

Although the portfolio has been developed primarily to support the project's capacity building objectives, individual portfolio components may also contribute to the wider service offerings of the respective consortium partners. Potential revenue-generating activities may include the provision of specialised training programmes, consultancy and support services, partner-specific experimentation and testing services, and the integration of capacity building activities within broader cybersecurity and compliance service portfolios.

Overall, the portfolio is expected to function as both a long-term knowledge resource and a complementary enabler for partner-specific exploitation activities, contributing to the continued uptake of CURIUM methodologies, tools, and services.

4.4.7.6. Sustainability and Long-Term Evolution

The long-term sustainability of the CURIUM Capacity Building Materials and Services portfolio will be supported through the continued maintenance and evolution of its educational resources and support services by the respective consortium partners. As cybersecurity requirements and the Cyber Resilience Act continue to evolve, the portfolio may be periodically updated to ensure its ongoing relevance and practical value.

The portfolio's modular structure enables individual materials and services to be maintained, expanded, and reused independently while remaining part of the broader CURIUM capacity building ecosystem. This approach supports the continuous delivery of training, awareness activities, experimentation services, technical guidance, and knowledge-sharing initiatives beyond the project's lifetime.

The portfolio may also be further enriched through additional educational resources, services provided by the respective consortium partners, and its reuse within future cybersecurity initiatives, contributing to the long-term adoption of the CURIUM Compliance Continuum and its associated methodologies and tools.

5. Standardization Activities

5.1. Introduction & Scope

Deliverable 5.1 of the CURIUM project, delivered in M6 (June 2025), provided the definition and strategy of the CURIUM project standardization activities. The deliverable based its content and approach on recognized standards and methods and included references, links and the current status.

Especially in relation to the adopted standardization strategy, a step wise approach was developed. This approach comprises of the steps depicted in Figure 24, implemented from the beginning until the very end of the project.

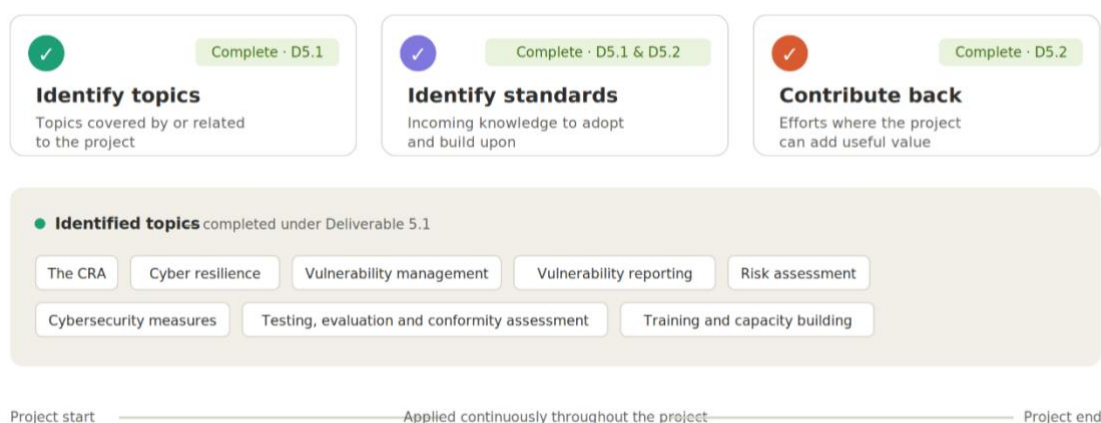


Figure 24 The CURIUM project standardization strategy steps

The CURIUM standardization strategy steps are presented below, along with high level results and the timeline of their achievement.

Step 1: Identification of topics covered / related to the project.

This step was carried out within the period M1-M6 of the project. Eight (8) key topics were identified as being very relevant to the work and objectives of the CURIUM project.

Step 2: Identification of standards that can be of use to the project as incoming knowledge or adopted and built upon.

This step was mainly carried out within the period M1-M6 of the project. Twelve (12) Standards Developing Organisations (SDOs) were identified and their activities related to the topics of interest of the project were analysed and monitored. Various project deliverables provide information and references for the cases where standards were utilized. For example: Deliverable 2.1, in section 7.1. provides an overview of standards

related to the CRA, Deliverable 2.2, in section 5.3, provides a description per tool of the CURIUM Continuum including references of standards used, Deliverable 3.2 and in section 4, where the final release of the CURIUM Continuum and its tools are presented.

Step 3: Identification of possible standardization efforts where the project could provide useful contribution.

This step was mainly carried out within the period M7-M21 of the project. Different types of standardization related activities were implemented, including: participation in CRA related projects clustering activities, provision of comments to draft standards, provision of comments to related regulatory / legislative activities, participation in working group meetings and activities of SDOs, participation in event promoting standards and others.

The following sections of this document provide further details on the activities exclusively related to Step 3.

5.2 Provision of feedback

5.2.1 Feedback on draft standards

prEN 40000-1-3: Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling

CEN/CENELEC published prEN 40000-1-3 - Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling for comments and the ballot approval process through its members. The period for comments was set between December 2025 and February 2026.

The CURIUM project provided comments through:

- the committee CYS/MC 8.06 (the national mirror committee of the SDO of Cyprus – CYS where members from APIRO and DSA participate),
- the activities of the CRA Cluster – technical subgroup. CURIUM lead the discussions and compiled the feedback provided by the CRA cluster through the EVS – Estonian centre for standardisation and accreditation,

prEN 40000-1-1:2025: Cybersecurity requirements for products with digital elements – Vocabulary and prEN 40000-1-2:2025: Cybersecurity requirements for products with digital elements - Principles for cyber resilience

CEN/CENELEC published prEN 40000-1-1:2025: Cybersecurity requirements for products with digital elements – Vocabulary and prEN 40000-1-2:2025: Cybersecurity requirements for products with digital elements - Principles for cyber resilience for comments and the ballot approval process through its members. The period for comments was set between October 2025 and December 2025.

The CURIUM project reviewed both documents provided comments (focused on through prEN 40000-1-2:2025):

- the committee CYS/MC 8.06 (the national mirror committee of the SDO of Cyprus – CYS where members from APIRO and DSA participate),

ETSI CYBER – CRA related standards

Exercising one of the Principles of International Standardization – Openness – and taking them to a different level, ETSI CYBER-EUSR conducted Open Consultations of the vertical standards in support of the Cyber-Resilience Act, at a much earlier stage than it is usual in the standardization world. This meant that draft versions of different maturity were provided to the public through the ETSI/CYBER/EUSR repository. During the last months 17 standards have been published. The CURIUM project has monitored this activity and reviewed some of the provided draft standards although no comments were provided in the end.

5.2.2 Participation in standardisation related working groups

Members of the CURIUM consortium regularly participate in the standardization activities through several members. CURIUM consortium members specifically have participated in the following:

- CEN/CLC/JTC 13/WG 9 “Horizontal cybersecurity for products with digital elements”,
- ISO/IEC JTC 1/SC 27/WG 1 “Information security management systems”,
- ISO/IEC JTC 1/SC 27/WG 3 “Security evaluation, testing and specification”
- CEN/CLC/JTC 21/WG 5 “Joint standardization on Cybersecurity for AI systems and
- ETSI Cyber Security Technical Committee (TC CYBER)

5.2.3 Feedback on draft regulatory (related) activities

CRA Cluster feedback on SBOMs

ENISA launched a survey at the end of 2025 to gather factual data on how organisations across industries and of varying sizes are approaching Software Bill of Materials (SBOM) adoption in response to the EU Cyber Resilience Act (CRA). The CRA Cluster members collaborated and provided feedback directly to ENISA on the level of SBOM adoption, the contribution of the SBOM in the CRA Cluster projects, the format of SBOMs used, the methods used for the generation of SBOMs etc. The collation of all the responses received by ENISA through the meetings and the survey, have been published in the document “SBOM Adoption State of Play – 2026”². Members of the CURIUM consortium also provided individual responses to the survey.

The review of the Cybersecurity Act

The Cybersecurity Act (CSA) came into force in 2019 as part of the EU's efforts to build strong cybersecurity. Since its introduction, the EU cybersecurity regulatory framework has become more complex in response to the rise in cyber-attacks. New EU rules, as well as changes in the geopolitical context, have impacted the CSA, and the regulation is currently under review. Since the CRA is interlinked to the CSA, CURIUM project partners were encouraged to submit comments. APIRO provided comments on the 07/06/2026³.

Technical description of important and critical products with digital elements

The Cyber Resilience Act requires the Commission to specify the technical description of the categories of important and critical products with digital elements listed in Annex III and IV to the Regulation. Such products may be subject to more stringent conformity assessment procedures, as set out in Article 32. The European Commission invited stakeholders to submit their feedback to a related consultation between March and April 2025. The CURIUM project, after careful review of the provided documents, submitted relevant feedback⁴.

² <https://www.enisa.europa.eu/sites/default/files/2026-06/SBOM%20Adoption%20State%20of%20Play%202026.pdf>

³ Contribution ID: ea84a798-8159-4112-81ef-a4da6708613f

⁴ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements/F3536318_en

5.3 Clustering

In 2025, the CRA cluster initiative started from the EU-funded projects around establishing tools and services to support compliance to the Cyber Resilience Act. The CRA Cluster aims to bring together all EU-funded projects working on Cyber Resilience Act compliance, tooling, guidance and standardisation. Its goal is to provide a unified support ecosystem for SMEs, manufacturers and policymakers working toward CRA implementation. The CURIUM project has been a member⁵ from the very beginning and has participated in many of the activities of the cluster.

The cluster is coordinated by the European funded project CYBERSTAND.eu and is organised in three working groups:

1. Technical Working Group

Chair: Ulrich Seldeslachts, LSEC & CRACY & Roberto Cascella, ECSO & Cyberstand

Purpose: Co-ordinate the technical interoperability between software products being built in projects

Deliverables: Map out CRA coverage in terms of tooling and identify any gaps. Work on a common, interoperable and machine-readable format for inputs/outputs for the various stages of the CRA. Where it makes sense integrate the tools through structured APIs and allow SMEs to move between tools based on choice/features/price.

2. Outreach and training Community Group

Chair: Nick Ferguson, Trust-IT & Cyberstand & James Philpott, DSME & Cyberstand.eu

Purpose: Co-ordinate outreach, education and training activities between projects to SMEs

Deliverables: Map training and education activities and materials (including guides) to target audiences and timelines. Look to streamline the material to avoid too much duplication and where possible integrate or link training material. Create a full calendar of engagement and outreach activities (events etc) from all dissemination work packages. Co-ordinate on timing and content, where it makes sense join up webinars or events with a common subject. Create common cluster online landing page on cyberstand.eu

3. Standardisation Community Group

⁵ <https://cyberstand.eu/cra-cluster>

Chair: Conor McGoveran, CyberCertLabs & CRA-AI & Lucia Lanfri, CEN-CENELEC & Cyberstand

Purpose: Co-ordinate feedback to standards and contributions to standardisation activities including information on use cases.

Deliverables: Cyberstand SSP to support project participation at WG/TC meetings.

CURIUM project members participate in all working groups and regularly participate in meetings and activities.

Indicative activities of the CRA Cluster include:

- Participation in the first CRA Cluster event under the auspices of CYBERSTAND.eu – panel with other related EU projects, 19th of June 2025.
- Participation in the closed-door meeting with all projects on the 9th of October 2025, with the attendance from DG Connect and ENISA.
- Participation in the provision of information in the CURIUM project through a MURAL board – on what and how each project of the cluster.(Figure 25).

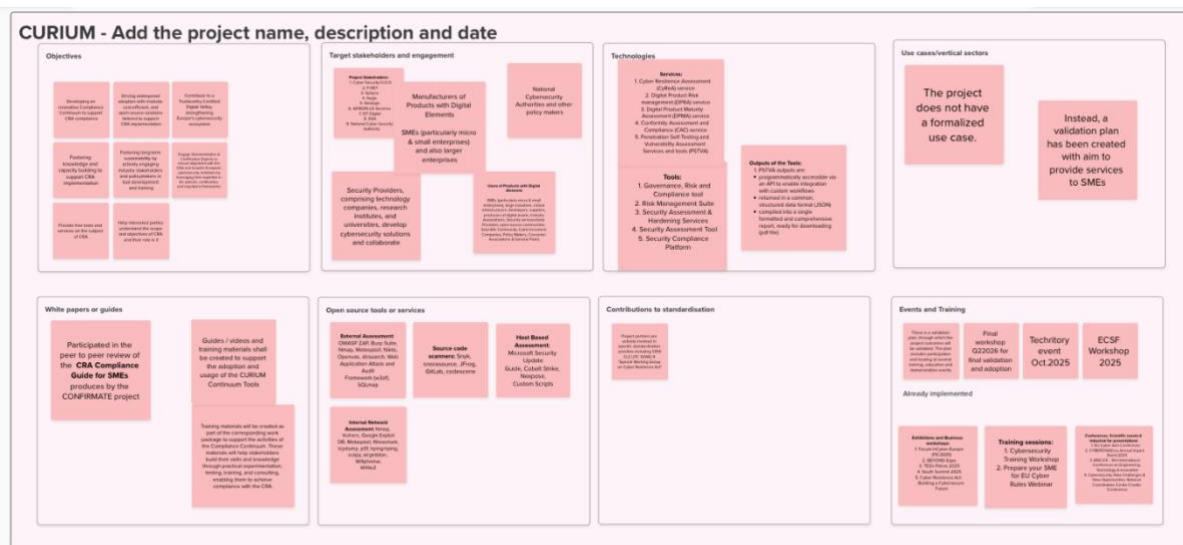


Figure 25 The CRA Cluster Miro board with the CURIUM project contribution

- Attendance to the standardization Workshop organized by CYBERSTAND, on the 18th of November 2025. The subject of the workshop was “Workshop on CEN/CLC JTC13/WG9 PT 1 - Principles for cyber resilience” and provided feedback on the request for a use case definition.
- Participated in the external review of the draft deliverable “Cyber Resilience Act Compliance Guide for SMEs” of the CONFIRMATE project (member of the CRA cluster), on the 3rd of October 2025. The comments received by the CONFIRMATE project were very positive on the comments provided by the CURIUM project.

- Participation in the series of events called CRA Standards Unlocked – EU tour. These events are organised by the EU-funded projects CYBERSTAND.eu and STAN4CRA.eu and the workshops bring together key EU-funded experts and projects working on the design of SME-friendly standards and CRA compliance tools.
- Provision of feedback on the SBOM adoption survey of ENISA (see 5.2.2).
- Provision of feedback on the draft prEN 40000-x-x standards (see 5.2.1).
- Participated in the activity to collect information on CRA Cluster tools & use cases - CRA SR mapping.

An initiative was announced to participate in the upcoming vertical standards workshops organized by the CRA Cluster, in collaboration with the CYBERSTAND.eu project and with the support of the European Standardization Organizations (**CEN/CENELEC** and **ETSI**). Although the workshops are planned for December 2026, partners are encouraged to participate and contribute to the discussions. The strategic value of these workshops lies in the standards-mapping activities, which are expected to provide valuable benchmarking opportunities.

To address this challenge and bridge the gap between regulatory expectations and engineering implementation, the CRA Cluster, in collaboration with CYBERSTAND.eu, will undertake a structured mapping and validation exercise. This exercise will demonstrate how existing EU-funded tools address the specific assessment criteria of the vertical standards, while simultaneously stress-testing the draft standards for practical, real-world applicability.

The objective of the workshops will be to review and resolve disputed mappings, finalize the validation of tooling coverage, and formally communicate to the European Standardization Organizations any gaps, ambiguities, or requirements within the draft standards that cannot be effectively tested.

Specifically, objectives are:

- Formally map the tools developed by the participating CRA Cluster projects against the specific clauses of the vertical standards, denoting "Full", "Partial" or "Supporting" coverage.
- Engage external cybersecurity and standardization experts to independently verify the technical accuracy of these mappings.
- Facilitate a direct feedback loop between tool developers, independent experts, and the ESOs (ETSI and CEN/CENELEC). As an example, if multiple advanced cybersecurity projects determine an assessment clause

cannot be automated due to vague wording, this provides actionable feedback to the ESOs before final publication.

- Produce a validated "Tooling Catalogue" that SMEs can confidently use to achieve CRA conformity.

To ensure high-quality validation and successful workshop outcomes, the initiative will initially be implemented in pilot mode, focusing on five representative vertical standards.

Proposed pilot standards are, as following:

1. Operating Systems
2. Network Interfaces
3. PKI Certificate Issuance Software
4. Smart Home Security Products
5. Virtualization/Containers

The importance of these workshops stems from the fact that, although the standards define the technical and assessment requirements necessary for compliance, many European SMEs lack the engineering capacity required to manually meet the associated testing and evidentiary requirements.

5.4 Other activities

- Participation in a panel discussion on the 6th edition of Joining Forces for Blockchain Standardisation, topic Chat Control & Data Privacy: Balancing Security, Encryption & Fundamental Rights (Argyro Chatzopoulou – APIRO), 18 March 2026 (<https://inatba.org/events/joining-forces-for-blockchain-standardisation-2026/>)

- Attendance to the 10th Cybersecurity Standardisation Conference, organized by the European Standardisation Organisations CEN, CENELEC and ETSI, and ENISA, the EU Agency for Cybersecurity, on the 12th of March 2026 (https://www.enisa.europa.eu/cybersecurity_standardisation_2026)

- Participation in a panel discussion to the Conference: Building CRA Compliance through Horizontal Cybersecurity Standards, organized by the Cyprus Organization for Standardization (CYS) with the support of the Digital Security Authority (DSA). Topic: "Ask the National Authority" (Xenia Kyriakidou – DSA), 21 September 2026 (<https://conference.cys.org.cy/>)

6. Collaboration Activities

6.1. Introduction & Scope

The present section aims to provide an overview of the collaboration, networking and clustering activities, illustrated and constituted, during the lifetime of the CURIUM project. Overall, clustering and broad collaboration constitutes an important horizontal dimension of the CURIUM project, since it is considered strategically essential for the maximization of the relevance, uptake and longer-term impact of CURIUM results and their sustainability, in the long run and also after for potential exploitation opportunities after the lifetime of the project.

Within the CURIUM clustering framework established during the first iteration of the deliverable D5.1, the project partners follow a structured, multi-stakeholder collaboration approach aimed at connecting the project with relevant EU and national initiatives, EU-funded research and innovation projects, national cybersecurity authorities and regulators, industrial players, SMEs and micro-enterprises, standardisation communities and clusters, RTOs and other stakeholders involved in the implementation of the CRA.

The clustering activities took place under the scope of Task 5.3 lead by NCSA, with the extensive collaboration of all partners. As presented in the plan and the interim review, the project leverages on both its institutional role in the cybersecurity ecosystem and its participation or coordination role in a number of complementary EU and national cybersecurity projects. This positioning provides CURIUM with an important bridge towards innovative initiatives, dealing with cyber resilience, security testing, certification and conformity assessment, cybersecurity operations, skills and capacity building, threat intelligence and CRA implementation. In addition, as it was established in the planning phase described in D5.1, the overall purpose of the collaboration framework is not limited to dissemination of CURIUM results, rather, to generate a continuous two-way knowledge exchange, through which external expertise, operational experience, regulatory developments, methodologies and technological results can inform CURIUM, while CURIUM's Continuum, tools, services and implementation experience can be shared with the wider EU cybersecurity ecosystem.

The project's dedicated objectives follow directly from the collaboration strategy defined during the first iteration, which identifies knowledge exchange, policy alignment, technology adoption, market access and scaling, cross-sector synergies, CRA-focused capacity building, practical regulatory input and continuous feedback loops as the main strategic purposes of CURIUM collaboration.

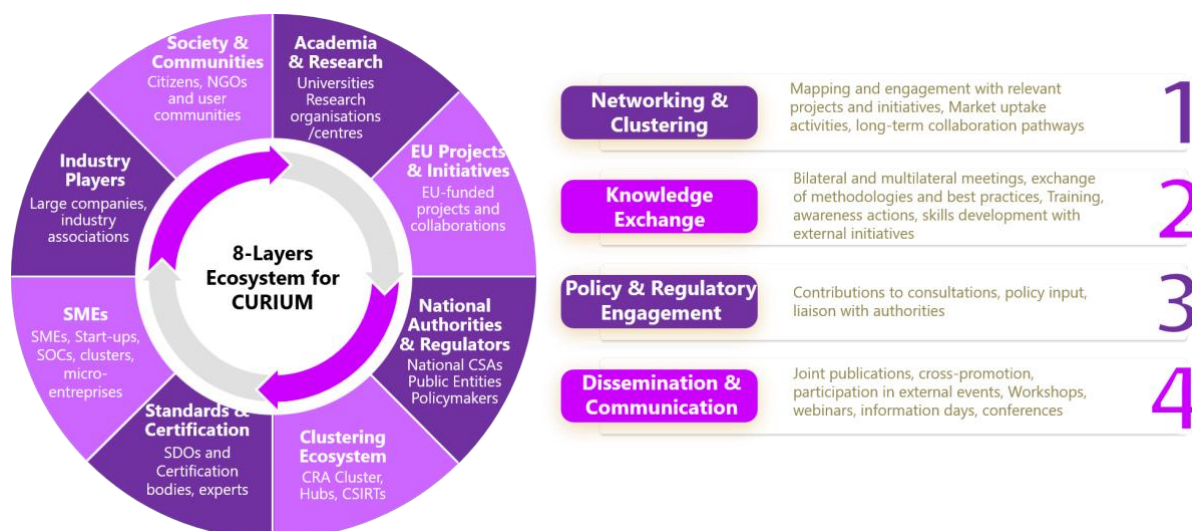


Figure 26: CURIUM Clustering and Collaboration Framework

CURIUM's collaboration activities are designed to reinforce the project's role within the wider European cybersecurity and regulatory ecosystem while directly supporting implementation of the CRA, aiming to disseminate, demonstrate and validate practical compliance pathways, tools and services that can help stakeholders interpret and operationalise CRA requirements. In parallel, CURIUM sought to facilitate systematic knowledge and experience exchange with EU projects and initiatives addressing cybersecurity resilience, security assessment, conformity assessment, certification, security testing and trustworthy-by-design technologies. This exchange is complemented by the establishment of knowledge exchange synergies with projects developing collaboration for the common communication and exploitation of the results and solutions. This systematic exchange, led to reducing duplication and enabling mutual learning.

Collaboration strategy also managed to strengthen policy and regulatory alignment through structured interaction with national and European authorities, mainly with ENISA especially through dissemination activities and events, ensuring that CURIUM remains responsive to the evolving regulatory landscape, following during the whole life-time the regulatory and compliance evolution, and refining the solutions, based on the feedback and discussions took place in physical and virtual events.

In addition, particular attention was placed on the uptake of CURIUM results by SMEs and micro-enterprises, especially the last months of the project and the extension period, after the completion of the development process and the reach out with the SMEs ecosystem, which often face disproportionate barriers to compliance and therefore require simplified, practical and cost-effective CRA support. The collaboration framework additionally creates opportunities for joint validation, allowing external projects, stakeholders and experts to provide feedback on CURIUM methodologies,

services and the novel Compliance Continuum, while also enabling the project to test the relevance, usability and transferability of its results in realistic settings.

Beyond these technical and regulatory dimensions, CURIUM collaboration positioning intended to generate a wider networking effect through coordinated dissemination, awareness raising, capacity building, standardisation, exploitation and sustainability actions. The project was active in series of common workshops, webinars, training activities, information days, joint publications and participation in relevant external events, using these mechanisms both to share results and to engage external communities in dialogue, supported standardisation readiness and helped to alignment CURIUM solutions with recognised practices and emerging requirements. All those activities also managed to increase the project's visibility, strengthen exploitation pathways and facilitate broader market access and scaling of its results and solutions, targeting also to the sustainability after the project's lifetime.

Collectively, the CURIUM clustering and collaborations objectives directly reflect targeted the achievement of knowledge exchange, policy alignment, technology adoption, market access and scaling, cross-sector synergies, CRA-focused capacity building, practical regulatory input and continuous feedback loops were identified as the principal strategic purposes of CURIUM collaboration.

6.2. Collaboration Activities Performed

During the period covered by the deliverable, CURIUM has progressed from the definition of its initial networking and clustering framework towards the establishment of a structured basis for external collaboration. Activities performed so far can be grouped into:

- (i) ecosystem and project mapping
- (ii) establishment of collaboration pathways through NCSA and all partners
- (iii) CRA policy engagement
- (iv) preparation of technical and knowledge-based synergies/collaborations

One of the main activities in the collaboration process is tracking for the identification and documenting of the projects and initiatives presenting concrete thematic and operational synergies with CURIUM. For each relevant initiative and EU project, CURIUM considered its thematic focus related to the CRA, relationship to CURIUM's objectives, possible forms of collaboration, responsible consortium partners, and opportunities for follow-up activities. The corresponding register is designed as a living instrument that can be progressively updated as collaborations mature.

As part of the clustering activities and joint events and the project-to-project continuous interaction and exchanges, CURIUM at the near end of its lifetime, managed also to formalise selected strategic relationships and collaborations with three projects, through the co-signing of Memoranda of Understanding (MoUs). More specifically, three principal cooperation arrangements are evidenced: with COcyber, AKADIMOS and CyberHubs. MoUs include a provision to remain in force for three years, providing a structured basis for technology and use-case exchange, common policy contributions, and participation in the ecosystem, as part of the exploitation activities, after the project's end. The collaborations include knowledge exchange, joint dissemination and exploitation activities, capacity building, and cybersecurity-skills development, and are designed to continue until the end of AKADIMOS. Specifically, for CyberHubs the relationship formalises CURIUM's participation as an Associated Project and provides a framework for cybersecurity-skills intelligence, knowledge exchange, education–industry cooperation, awareness, capacity building and joint ecosystem activities, including cooperation that may continue beyond the CyberHubs project lifetime. Collectively, the MoUs transforms clustering contacts into structured and potentially durable cooperation mechanisms, supporting the continued dissemination, uptake and exploitation of CURIUM results beyond the project's funded implementation period.

To this end, the CURIUM Project signed MoUs (**Error! Reference source not found.**) with the following projects:

- AKADIMOS
- COcyber
- CyberHUBS

The MoUs establishes a structured collaboration framework between CURUM and other synergetic projects, based on their complementary objectives and shared ambition to strengthen EU cybersecurity resilience, foster innovation, and contribute to a secure and trustworthy digital ecosystem. These collaborations are tightly linked with the main CURIUM target audience that mainly supports SMEs in implementing the CRA through its Compliance Continuum of cybersecurity tools and services for security testing, regulatory compliance and risk mitigation. In addition, the MoUs therefore create a formal basis for cooperation, information sharing and strategic alignment between the two projects, with the aim of generating greater collective impact than could be achieved through isolated activities. Actually, such type of collaborations foreseen several concrete forms like the exchange technologies, use cases and project results; joint events and workshops, discussion forums, networking and clustering events. Moreover, the coordinators of the projects had several meetings for activities.

CURIUM has established a collaboration link with CyberHubs – the European Network of Cybersecurity Skills Hubs, participating as an Associated Project and thereby extending its clustering activities towards the European cybersecurity skills and capacity-building ecosystem. CyberHubs is a three-year Erasmus+ initiative coordinated by DIGITALEUROPE, bringing together seven national Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia and Spain. The Hubs connect industry, academia, policymakers and training providers and have identified country-specific cybersecurity skills needs and developed corresponding national strategies. This collaboration is particularly relevant to CURIUM because effective implementation of the CRA and the uptake of the CURIUM Compliance Continuum also depend on the availability of adequately skilled professionals and on stronger links between technical, regulatory and training communities. Through its Associated Project status, CURIUM has already supported the mutual exchange of expertise on CRA, promoted relevant skills-development and awareness activities to SMEs and experts, as well as to partners of other EU projects, as presented in the table below, and managed in a short-time period to amplify the project's results and real-world solutions to the respective SMEs ecosystem, across wider European networks and EU-funded projects, contributing to knowledge sharing and CRA awareness. The interaction with CyberHubs therefore reinforces CURIUM's broader clustering strategy by linking CRA-oriented compliance, cybersecurity tools and SME support with complementary actions addressing cybersecurity skills shortages and workforce development.

Moreover, a complete overview of the interactions of CURIUM with other EU projects, initiatives and organisations, have been included in Table 16 below. The table includes all collaboration activities with (a) Structured Clusters & Networks, (b) Strategic Project-to-Project Collaborations, (c) CRA Cluster and other synergetic projects interactions and (d) Institutional, SDOs and Innovation Ecosystem.

Cluster / EU Project / Initiative	Type / Status	Collaboration and activities evidenced in CURIUM news
CyberHubs – European Network of Cybersecurity Skills Hubs	Structured collaboration – CURIUM Associated Project	CURIUM joined CyberHubs as an Associated Project. The Erasmus+ initiative, coordinated by DIGITALEUROPE, connects seven national Cybersecurity Skills Hubs. Cooperation focuses on expertise exchange, cybersecurity skills development, amplification of results,

		knowledge sharing and strengthening the European cybersecurity community.
CRA Cluster / CYBERSTAND.eu	Active cluster membership	CURIUM participates in all three CRA Cluster core groups: Technical Interoperability, Standardisation, and Outreach & Training. Activities include mapping CRA coverage and gaps, developing data-exchange approaches for SMEs, providing standardisation feedback, contributing use cases, and aligning SME outreach and training.
CYBERSTAND.eu	Standardisation and CRA implementation collaboration	Beyond cluster membership, CURIUM participated in the CYBERSTAND.eu Annual Event and several CRA Standards Unlocked – EU Tour activities, using them to present the Compliance Continuum, exchange with CRA projects, contribute to standardisation discussions and provide feedback relevant to CRA implementation.
STAN4CRA.eu	CRA standardisation ecosystem	Together with CYBERSTAND.eu, STAN4CRA organised the Barcelona CRA Standards Unlocked event. The interaction connected CURIUM with projects developing SME-oriented standards, guidance and CRA compliance tools and supported its engagement with the wider CRA Cluster.
CUSTODES	Major recurring project-to-project synergy	Collaboration spans joint research, validation, dissemination, capacity building and CRA conformity-assessment activities. CURIUM and CUSTODES produced a joint scientific paper on automated cybersecurity certification; jointly engaged French SMEs through a validation pathway linking CURIUM's scope assessment to the CUSTODES Pilot Programme; were jointly represented in CRA Cluster

		events; and jointly supported awareness and regulatory-readiness activities.
CUSTODES – Paris SME validation	Joint validation / SME engagement	The two projects jointly organised an in-person stakeholder activity with French SMEs. CURIUM provided an initial CRA-scope assessment while interested SMEs could progress to the CUSTODES Pilot Programme, creating a complementary pathway for validation, expert mentoring, cybersecurity tooling and capacity building.
CUSTODES – joint scientific work	Joint R&I output	A scientific paper developed as a joint CURIUM–CUSTODES outcome investigated the use of ontologies and semantic technologies for cybersecurity certification and CRA compliance automation and was presented at IEEE ICE 2025.
SAND5G	Recurring EU-project collaboration	CURIUM and SAND5G jointly organised the Risk Assessment & Incident Response workshop at the University of Patras, combining organisational cyber-risk and incident-response practices with security issues surrounding next-generation 5G networks.
CURIUM + SAND5G + CUSTODES	Joint awareness and capacity building	The three projects jointly supported cybersecurity awareness at TEDxPatras and subsequently supported the Patras IQ session on CRA/CSA requirements. These interactions created a recurring collaboration around awareness, risk management, regulatory preparedness and SME cybersecurity.
COcyber	European project-clustering / concertation cooperation	CURIUM joined the first COcyber Concertation Workshop, which gathered ten EU cybersecurity projects. Cooperation was organised around five pillars: networking and communication, policy alignment, knowledge and

		technology transfer, research and innovation, and skills and training. Identified follow-up outputs included joint policy briefs, co-hosted events, coordinated skills activities and shared technology assets.
OCCTET	CRA Cluster project interaction	CURIUM connected with OCCTET at the Zagreb CRA Standards Unlocked event and again shared the CRA Cluster platform with it in Barcelona. The common thematic focus concerns practical and SME-oriented CRA compliance tools and support.
CRACoWi	CRA-project networking	Identified by CURIUM as one of the EU co-funded CRA initiatives with which it connected and engaged during the Zagreb CRA Standards Unlocked event.
CONFIRMATE	CRA-project networking	Interaction took place within the CRA Standards Unlocked / CRA-compliance project ecosystem in Zagreb, providing a basis for mutual visibility and knowledge exchange between complementary CRA initiatives.
OSCRAT	CRA-project networking	CURIUM connected with OSCRAAT during the Zagreb event and shared the wider CRA Cluster environment oriented towards practical CRA-compliance tools and SME support.
Secure4SME	SME-focused CRA-project interaction	CURIUM engaged with Secure4SME in Zagreb as part of the group of EU-funded projects addressing innovative approaches to CRA compliance and SME support.
CRACY – CRA made Easy	CRA Cluster interaction	CURIUM and CRACY participated in the Barcelona CRA Cluster session, exchanging visibility around tools, guidance and SME-oriented approaches for operationalising CRA requirements.

TrustBoost	CRA Cluster interaction	TrustBoost and CURIUM contributed to the same Barcelona CRA Cluster session, creating an interaction channel within the wider community of projects developing CRA-compliance support.
NERO Cybersecurity	CRA Cluster interaction	NERO and CURIUM were represented within the dedicated CRA Cluster session at the Barcelona event, supporting cross-project exchange on cybersecurity and CRA implementation.
CYNERGY	Innovation / digital-resilience ecosystem interaction	At Bucharest Tech Week 2026, CYNERGY convened industry, researchers, policymakers and technology providers. Within this setting, CURIUM and CUSTODES jointly showcased complementary tools, methodologies and expertise supporting cybersecurity resilience and compliance readiness.
Vigilance and CyberAid	EU-project ecosystem interaction	CURIUM participated in the AI Enables Cybersecurity event organised in the context of the Vigilance and CyberAid kick-off meetings. The interaction provided a platform for presenting the Compliance Continuum and engaging participants on CURIUM Tools.
ENISA	European institutional / CRA implementation interaction	CURIUM amplified ENISA's SME CRA readiness survey, aimed at informing ENISA and the Commission about SMEs' awareness, maturity and support needs. It also promoted ENISA's survey on Software Bill of Materials adoption, linked to European Commission work on CRA implementation.
Andalucía Emprende, Asturias and Euskadi innovation hubs	Innovation-ecosystem collaboration pathway	Through CURIUM partner EIT Digital, contacts were developed at South Summit Madrid with these innovation hubs, with plans for collaborative cybersecurity activities and CRA-

		focused talks, supporting CURIUM visibility and access to European startup and innovation communities.
Digital Security Authority of Cyprus / Cyprus Organisation for Standardisation	National authority & standardisation interaction	CURIUM was presented at the jointly organised Cyber Resilience Act: Building a Cybersecure Future event, which brought together EU projects, ENISA, standardisation actors and cybersecurity stakeholders. The activity strengthened CURIUM's links with regulatory and standardisation communities.
Digital Security Authority / Office of the Commissioner of Communications – Cyprus	Skills and cybersecurity ecosystem	CURIUM participated in the Nicosia Cybersecurity Career Fair organised within the European Cybersecurity Month context, using the initiative to promote capacity building, training and cyber-resilience innovation.
Croatian National Coordination Centre (NKS), ENISA, EUCC and CARNet	National/EU cybersecurity ecosystem interaction	CURIUM was presented at the Croatian NKS conference supported by ENISA, EUCC and CARNet, reaching SMEs, industry, academia and IT stakeholders and strengthening links with national coordination and European cybersecurity communities.

Table 16: Overview of CURIUM Collaboration and Networking Interactions

Overall, CURIUM has progressively embedded itself in several structured EU cybersecurity collaboration mechanisms that provide continuity. A particularly significant development is CURIUM's participation in CyberHubs – the European Network of Cybersecurity Skills Hubs as an Associated Project, so that CURIUM can exchange expertise, promote skills-development initiatives, disseminate project results through established national communities and connect CRA implementation with the wider challenge of cybersecurity workforce readiness. In addition, CURIUM is also actively involved in the CRA Cluster, coordinated through CYBERSTAND.eu, participating across its Technical Interoperability, Standardisation, and Outreach & Training groups. This provided CURIUM with a structured mechanism for exchanging experience with other CRA-oriented projects, identifying technical and regulatory gaps, discussing interoperability and data-exchange requirements, contributing use cases and

supporting coordinated SME outreach and trainings/events/activities. The relationship therefore extends beyond visibility and establishes a recurring environment for collective CRA implementation activities. Finally, CURIUM has participated in the COcyber concertation ecosystem, where European cybersecurity projects collaborate across five areas: networking and communication, policy alignment, knowledge and technology transfer, research and innovation, and skills and training. This interaction has created opportunities for joint policy briefs, co-hosted events, coordinated capacity-building activities and sharing of technological assets and expertise.

Moreover, the elaboration with the other EU projects, also led to joint outputs, shared validation activities, SME access, complementary technical expertise, joint dissemination and stronger pathways from CRA readiness towards practical conformity assessment and cybersecurity implementation. The strong relationship with CUSTODES, created multiple opportunities, such as joint scientific research, conformity assessment, SME validation, dissemination and capacity building. From this collaboration, a joint CURIUM–CUSTODES scientific paper investigated the use of ontologies and semantic technologies to support automation of cybersecurity certification and CRA compliance.

The interactions and clustering with EU projects, which also have collaborations directly with SMEs, created several opportunities for validation activities across EU Member States, CURIUM provided an initial assessment of CRA applicability and scope, while interested companies could subsequently engage with the CUSTODES Pilot Programme for further validation, cybersecurity tooling and expert mentoring. This created a complementary pathway from CRA scoping and readiness assessment towards conformity-assessment support and practical validation. Furthermore, CURIUM and SAND5G jointly organised a workshop on Risk Assessment & Incident Response, combining organisational cyber-risk and incident-response perspectives with cybersecurity challenges affecting next-generation network infrastructures. The collaboration was further reinforced through activities involving CURIUM, CUSTODES and SAND5G, including cybersecurity awareness and regulatory-readiness actions associated with TEDxPatras and Patras IQ.

6.3 Section Summary

CURIUM has established a solid framework for positioning the project as an active contributor to the wider European cybersecurity, CRA compliance and cyber-resilience ecosystem. Building on the Networking and Clustering Plan and Strategic Collaboration Plan, the project has defined a structured approach for stakeholder engagement, collaboration, communication and monitoring, involving EU and national authorities,

regulators, cybersecurity projects, industry, SMEs, research organisations, certification and standardisation experts, and cybersecurity skills initiatives. Particular added value derives from consortium's extensive links with complementary cybersecurity projects and initiatives, creating concrete channels for knowledge exchange, stakeholder engagement and joint activities. This is complemented by collaboration opportunities identified through other consortium partners and with projects addressing cyber resilience, conformity assessment, assurance, open-source tools, risk assessment, SOC operations, threat intelligence, training and SME support.

A series of notable contributions of the CURIUM's achievements have been documented in the respective table, along with the feedback process on the definitions of important and critical product categories under the CRA, demonstrating the project's capacity to contribute practical technical expertise to the evolving regulatory environment. All the identified collaboration opportunities have indeed provided valuable feedback to the project and the respective solutions, providing measurable outcomes, prioritising technical validation, CRA relevance, SME uptake, standardisation and certification readiness, capacity building, exploitation and sustainability. Collaboration effectiveness is monitored through two main indicators covering established partnerships, joint activities and stakeholder out-reach. Overall, the framework provides CURIUM with the mechanisms needed to strengthen its technical quality, regulatory alignment, EU visibility and the long-term adoption and sustainability of the Compliance Continuum.

7. Conclusion

7.1. General remarks

This deliverable has reported on the dissemination, exploitation, standardisation and collaboration activities carried out throughout the CURIUM project, consolidating the results of Tasks T5.1, T5.2 and T5.3 into a final account of the project's Work Package 5 activities.

The dissemination and communication activities described in [Section 3](#) achieved broad engagement with SME, industry, policy and cybersecurity communities, with the cumulative KPI assessment confirming that the majority of the targets defined in the Grant Agreement were met or exceeded, particularly in relation to website traffic, social media growth, publications, newsletters, video production and stakeholder events. These results confirm that the dissemination strategy defined in D5.1 was effectively implemented and adapted as the project's tools and results became progressively available.

The exploitation plans presented in [Section 4](#) provide an initial basis for the future uptake of CURIUM's seven Key Exploitable Results. For each KER, the deliverable has defined target stakeholders, value propositions, exploitation and adoption approaches, ownership and IPR arrangements, indicative cost and revenue considerations thereby paving the way for future plans.

The standardisation activities reported in [Section 5](#) demonstrate CURIUM's active and continuous contribution to the European standardisation landscape relevant to the Cyber Resilience Act, through the monitoring of related standards, the provision of technical feedback to European draft standards, the participation in Standards Developing Organisations' working groups, and contributions to EU regulatory consultations. The collaboration and clustering activities presented in [Section 6](#) further reinforced CURIUM's positioning within the wider European cybersecurity and CRA compliance ecosystem, notably through its active participation in the CRA Cluster and its structured engagement with complementary EU-funded projects, national cybersecurity authorities and standardisation bodies.

Taken together, the results presented in this deliverable demonstrate that CURIUM has successfully conveyed its technical achievements a range of stakeholders, has provided meaningful contributions to standardisation, and established collaborative relationships across the European cybersecurity ecosystem. Section 7.2. provides an overview in relation to the sustainability of the project results.

7.2. Sustainability Outlook

Options related to the sustainability and long-term evolution of each one of the KERs of the CURIUM project, are presented in the Key Exploitable Result (KER) exploitation plan in [Section 4](#). These options are specific to each one of the KERs, since the tools provided by the CURIUM project, are individually developed and owned.

This fact presents advantages and disadvantages:



The operation of the CURIUM Continuum Portal does not depend on the availability of any one individual tool. So, even if a tool owner (CURIUM project partner) decided to stop supporting the tool, this could easily be removed from the CURIUM Continuum Portal, while the rest would remain operational.



On the other hand, the specific evolution plan, marketing strategy and investment made for each tool is entirely dependent on the tool owner (CURIUM project partner). This means that a tool owner may decide to invest heavily in a short period of time, and advance their tool, whereas another may decide on a slower pace.



The tools included within the CURIUM Continuum Portal, address different needs of the interested parties, covering the entire compliance lifecycle. This in turn leads to different audiences and different adoption rates.



The modular nature of the CURIUM Continuum Portal allows the addition of further services and tools based on the needs of the interested parties and the plans of the project partners. For example, at any time, the capacity building material and services can be updated, increased and offered through the platform to the interested parties without the need for substantial alterations.

The CURIUM project partners have committed to maintain the CURIUM Continuum Portal and to continue providing the included tools, for 18 months after the end of the project. Within this duration, the project partners will continue to gauge the needs of the interested parties and evaluate the paths for further exploitation and development of the tools, aiming to support their sustainable provision.

Within this period, the consortium partners intend to explore the establishment of a coordinated operational governance mechanism for the CURIUM Compliance Continuum, covering platform hosting, maintenance, integration management, user support and the evolution of the ecosystem after the end of the support period. The exact form of this mechanism (e.g. distributed ownership by individual partners, a lead-

partner model, or a jointly governed structure) remains to be agreed by the consortium and is not yet formally established.

Table 17 summarises, for each KER, the partner primarily responsible for its continued exploitation and the intended pathway for its use, maintenance and evolution after project completion. Full details on target stakeholders, value proposition, ownership, cost/revenue considerations and adoption logic for each KER are provided in the corresponding subsections of Section 4.4.

KER	Responsible Partner	Partner(s)
KER1 – CURIUM Continuum	All partners Leading Partner: AEGIS	Continued operation as the orchestration layer consolidating the access to the other KERs.
KER2 – PSTVA	AEGIS	Continued development and commercial/service-oriented exploitation as a standalone or integrated security-testing offering
KER3 – CyReA	NLG	Continued exploitation as a CRA scoping and classification service, with NLG leading commercialisation and maintenance
KER4 – DPRA	NLG	Continued exploitation as a risk-management service, integrated with or complementary to CyReA
KER5 – CAC	CYS	Continued exploitation as a conformity assessment and compliance support service
KER6 – DPMA	APIRO	Continued exploitation as a maturity assessment service or implemented within other tools or services
KER7 – Capacity Building Plan and Services	Consortium (multiple partners)	Continued delivery of training and knowledge-transfer materials through partner networks

Table 17 Summary of KER responsibility and possible pathways.

Beyond the individual KERs, CURIUM's sustainability is reinforced by the institutional relationships and collaborative structures established during the project, described in detail in [Section 6](#):

- **CRA Cluster membership**, through which CURIUM continues to contribute to and benefit from coordinated EU-level work on CRA implementation, technical interoperability and standardisation, independently of the project's own funding cycle.
- **Associated Project status with CyberHubs**, providing an ongoing channel for skills-development, awareness-raising and knowledge-sharing activities linked to the CRA and cybersecurity workforce development.
- **Signed Memoranda of Understanding with AKADIMOS, COcyber and CyberHubs**, establishing a formal basis for continued cooperation, information-sharing and joint activities.