Cra sUppoRt contInuUM

D5.1 - Plan and early activities 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	D5.1 - Plan and early activities on Dissemination, Exploitation, Standardisation & Sustainability.		
Work Package	WP5		
Contractual due date	30.06.2025	**Actual submission date**	27.06.2025
Nature	R — Document, report	**Dissemination Level**	PU - Public
Lead Beneficiary	p-NET		
Responsible Author	Didoe Prevedourou		
Contributions from	All partners		

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

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Revision history (including peer reviewing & quality control)

Version	Date	Author	Notes
0.1	04/04/2025	p-NET	ToC
0.2	11/06/2025	p-NET	First complete draft
0.3	18/06/2025	p-NET	Prefinal for review
0.4	24/06/2025	p-NET	Prefinal w. review comments by DSA
0.5	25/06/2025	p-NET	Prefinal w. review comments by SPH
0.6	26/06/2025	p-NET	Prefinal w. integrated review comments
1.0	27/06/2025	p-NET	Final, QC, reviewed by co-ordinator and submitted

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Description
AI	Artificial Intelligence
CAC	Conformity Assessment and Compliance Service
CC	Common Criteria
CISOs	Chief Information Security Officers
CMS	Content Management System
CRA	Cyber Resilience Act
CyReA	Cyber Resilience Assessment Service
D&C	Dissemination & Communication
DPMA	Digital Product Maturity Assessment
DPRA	Digital Product Risk Management
EC	European Commission
ECC	European Cybersecurity Competence Centre
ENISA	European Union Agency for Cybersecurity
ERs	Exploitable Results
EU	European Union
EUCC	European Union Common Criteria
G2M	Go-to-Market
GA	Grant Agreement
IPR	Intellectual Property Rights
IT	Information Technology
KERs	Key Exploitable Results
KPI	Key Performance Indicators
MS	EU Member State
NCCs	Network of National Coordination Centres
NGO	Non-Governmental Organization
NRLA	National, Regional and Local Authorities
OES	Operators of Essential Services
QR code	Quick Response code
R&I	Research and Innovation

SDO	Standards Developing Organization
SME	Small and Medium-sized Enterprise
SOC	Security Operations Center
TRL	Technology Readiness Level
UI	User Interface
UX	User Experience
WCAG	Web Content Accessibility Guidelines

1. Executive Summary

Deliverable 5.1 is a public document of the CURIUM project, created as part of the Work Package 5 (WP5) "Dissemination, Exploitation, Communication and Outreach Activities" and addresses all three Tasks of the WP, namely Task 5.1 'Communication & Dissemination Activities', Task 5.2 'Impact creation, Exploitation & Standardization Activities', and Task 5.3 'Stakeholder, EC, and National Authorities Engagement'. CURIUM envisions a secure, resilient digital environment by strengthening the security, privacy, and accountability of hardware and software with digital elements. The core of CURIUM's approach is the Compliance Continuum, a set of tools and services designed to streamline compliance with the CRA. By simplifying and automating compliance processes, CURIUM empowers European SMEs to conduct self-assessments, prepare for third-party certification, and reduce costs, while accelerating time to market. The aim of the Dissemination, Exploitation, Communication and Outreach Activities within the project is to inform as many people as possible about the existence, the activities, the objectives and the results of the project. For this purpose, various communication actions are undertaken to promote the visibility of the project and its impact. The document provides a comprehensive overview of the project's Dissemination and Communication strategy, relevant project rules and procedures, planned and already implemented activities. It also addresses exploitation aspects of the project by a./ Presenting individual partners' exploitation strategies and plans vis-à-vis expected project results, and b./ Introducing the project's methodology towards defining joint Go-to-Market roadmaps for the project's Key Exploitable Results. Project Plans and methodologies regarding networking, clustering and establishing strategic collaborations are documented and the deliverable concludes with the project's planning and implementation of standardization efforts.

2. Introduction

2.1 Scope and Purpose

Deliverable D5.1 is the first outcome of WP5, titled Dissemination, Exploitation, Communication and Outreach Activities. The WP is designed to guarantee that the project's outcomes are effectively distributed throughout the European research, industrial and state authorities sectors. It further ensures that all crucial stakeholders are specifically targeted, and that continuous communication is maintained between the project partners on one side, and on the other, the general public, the scientific community, technicians, experts, media representatives, policymakers, various industries, and end-users. As such, WP5 aims to address the following objectives:

O5.1. Plan and carry out a Dissemination and Communication (D&C) strategy customized to CURIUM by taking preparatory steps to launch project dissemination activities, by creating the project web site, design templates, initial printed materials, etc. The strategy will also specify the consortium's approach to address scientific and SME end-user communities, the private and public sector and the wider public.

O5.2. Plan for maximizing exploitation. Create and follow a plan that handles IPR and establish the uptake of CURIUM results after the project's end. The plan includes revealing different market channels, a compilation of already known exploitation opportunities, conducting an iterative monitoring of actual market needs, and guidelines driving project workflow to meet them in a timely manner.

O5.3. Design and launch a coherent and organized project outreach and collaboration plan. Such plan will be implemented by coordinating the network of contacts of each entity, by participating in various events and meetings, by organizing our events and scientific workshops, as well as engaging with our national and international links.

The WP is organized in three Tasks each designed to address one of the objectives above.

The present deliverable provides an overview of the work performed in all three Tasks during the first six months of the project.

2.2 Content Organization

Following the Executive Summary and the Introduction, the document is structured in three main chapters, each devoted to the work performed in a specific Task of WP5: Chapter 3 corresponds to Task 5.1, Chapter 4 to Task 5.2 and Chapter 5 to Task 5.3. In more specific terms,

- Chapter 3 presents the development of a comprehensive dissemination and communication plan, which precisely delineates the strategies and specific tools purposed for use throughout the project's duration. The dissemination strategy, which includes the definition of internal procedures, identifying the target audience, and establishing timelines, and the communication strategy, detailing the means, methods, and tools employed to engage the designated target audience throughout the project's entire lifecycle. All communication and dissemination activities that are carried out are meticulously recorded in the CURIUM "D&C Tool" .xlsx file.

- Chapter 4 presents the partners' individual exploitation plans based on anticipated project results, as perceived in the first six months of the project's work. For those Expected Results (ERs) the IP and Ownership status is also defined. The chapter also introduces the project's methodology towards defining joint exploitation plans of the project's Key Exploitable Results (KERs) and Go-to-Market (G2M) Strategy and Roadmaps.
- Chapter 5 is devoted to networking and clustering, strategic collaborations and standardization. For networking and clustering, the objectives of the activity and the methodology to be followed are presented together with an initial (to be continuously enriched) list of candidate projects to cluster and network with for the design and implementation of joint activities. Strategic collaborators are also identified together with possible channels of communication-collaboration, expected impacts and assessment frameworks. Plans related to standardization monitoring and active engagement are also presented together with concrete standardization efforts that have been contributed by the project in the first six months.
- Chapter 6 is the Conclusions chapter which summarizes key take aways of the deliverable and future plans.

3. Dissemination & Communication Plan and Activities

3.1 D&C Strategy

As part of the CURIUM project, a dissemination and communication strategy has been carefully designed to ensure that the project's results, insights, and achievements are effectively communicated to a wide range of stakeholders, including policymakers, researchers, business and industry professionals, and the general public.

3.1.1 Objectives

The dissemination and communication strategy aims to maximize the impact of the project and to that end promotes active engagement with relevant stakeholders and ensures wide dissemination of the knowledge generated.

Steps and Phases:

1. The first step is to identify the target audiences, D&C tools and channels. Based on this, an effective D&C plan can be created to maximize the impact of the project results.
2. The second step is to design a comprehensive set of communication materials that facilitate easy recognition of the project and increase exposure to its goals, activities, and achievements.
3. The third step involves utilizing both internal and external dissemination channels, organizing project events, and participating in workshops, conferences, and international/EC meetings to ensure widespread knowledge of the project and its results.
4. The last step is to sustain the visibility of the project activities and outcomes over the long term, by continuously updating communication materials, engaging with stakeholders to maintain their interest and support, influencing standards and policy making and establishing strategic collaborations.

The **main objectives** of the dissemination and communication plan are to:

1. **Raise Awareness:** The first objective is to increase awareness of the project among key stakeholders and the general public. By sharing information about the project's goals, activities, and outcomes, the project aims to create a better understanding of the challenges faced by the targeted stakeholders and the need for sustainable and innovative solutions.
2. **Disseminate Knowledge:** The second objective is to ensure that the knowledge generated by the project is widely disseminated to relevant stakeholders. This includes sharing research findings, insights, and best practices.
3. **Promote Collaboration:** The third objective is to foster collaboration among stakeholders. The project aims to create opportunities for networking, knowledge-sharing, and strategic collaboration.
4. **Create Impact:** The final objective is to create long lasting impact contributing to the vision of a secure and resilient digital environment.

3.1.2 Target Stakeholders

The table below captures the target groups and how CURIUM envisions they will uptake the project's results to achieve the expected impacts. Understanding the targeted groups profiles in the addressed value chain is an essential component of the D&C Strategy.

Table 0-1: Target Stakeholders Profile

Target Group	Expected Benefits	Pathway Goal	Impact
SMEs	Availability of tools, services and processes for cyber security assurance, cyber resilience, and certification	Extensive evaluation and demonstration of results, Impact assessment and analysis	Increased cyber-resilience; Compliance with regulations; More secured services to end customers; Risk mitigation and business continuity; Increased awareness
Industry Associations	Regulation compliance; broad access to validated tools	Results demonstration, Impact analysis	Efficient testing of end services; Mitigation action planning
Security services/tools Providers	Optimize security challenges; certify tools/models/processes	Self-assessing capabilities; assess effectiveness of controls	Strengthening innovation; Increased resilience and compliance
Open-source communities	Validation of security assurance of open-source components	Encouraging community participation and infusion of cyber security in open-source solutions	Enhanced inclusion of open-source solutions in cyber security policies and improvement of their security posture
Scientific Community	Validated methods, tools, models, and reference architecture	Diffuse knowledge through publications, scientific events etc.	New domain knowledge, increased capacity for new research
Cyber Insurance Companies	Automated or semi-automated risk assessment. Reduce the information asymmetry between insurers and clients	Testing and evaluation of insurance policies that are based on evidence-based risk assessment and analysis in real world scenarios.	Availability of tools for SME compliance Increased awareness
Policymakers	Better insight into policy deficiencies and gaps; availability of conformity-related information	Report actionable knowledge	Definition of future research and EU innovation directions
Consumer Associations & General Public	Secured and resilient services, tools, and processes	Increase general awareness through communication strategy	Increased awareness about security assurance, certification, and cyber resilience value in consumed services

3.1.3 Dissemination Tools, Activities and KPIs

The present paragraph outlines the dissemination tools and activities that the consortium has developed to achieve effective dissemination of the project's results and maximize their impact. The various tools and activities have been carefully planned to ensure the project's promotion to the wide range of targeted stakeholders, and include:

- Scientific Publications: The consortium plans to disseminate the project's findings through a variety of scientific publications that target both the scientific community and industry. By targeting these publications, the consortium aims to ensure that its research is widely recognized and adopted by relevant stakeholders.
- Workshops, webinars, trainings, joint events with other projects/initiatives: To facilitate knowledge transfer and promote sustainability, the CURIUM partners will organize technical workshops, training sessions, and webinars both virtual and physical. Additionally, as part of clustering activities, joint events will be co-organized with existing cybersecurity projects in which consortium members participate, as well as with relevant initiatives.
- Push results to communities, associations, and establish strategic collaborations: The consortium will collaborate with relevant communities, associations, innovation hubs, and EU-funded projects in which consortium partners are active members to jointly disseminate CURIUM results.
- Industrial exhibitions, trade fairs: The consortium partners will participate in various well-known symposia, events, industrial exhibitions, and trade fairs with the aim to actively engage with multiple stakeholders and disseminate the outcomes of CURIUM through presentations, talks, brochures, and personal interactions.
- Standards & policy contributions: To ensure that the impact of CURIUM is far-reaching and long-lasting, the project aims to influence policymaking and standards development. This involves obtaining recognition and approval for the project's proposed innovations and contributions and subsequently integrating them into production environments. To achieve this, the consortium partners plan to provide recommendations for policymaking and standardisation.
- Showcases & demos: CURIUM will include in its dissemination plan, showcase activities to demonstrate the feasibility of its proposed capabilities and incentivise wide adoption.

Relevant Key Performance Indicators (KPIs) are summarized in the Table below.

Table 0-2: Dissemination KPIs

No	KPI Description	Target Value	Current values
1	Presentations	≥5 conference/ scientific events/ industrial	3
2	Participation in industrial exhibitions, open days & networking events	>=3 by the end of the project;	5
3	Publications	≥3 publications in int'l referred journals & conferences; ≥3 publications in int'l magazines; ≥5 conference/ scientific events/ industrial for presentations	1
4	Organization of business & exploitation-driven event	≥1 events; ≥50 attendees; ≥ 20% of participants engaged for further exploitation	-

5	Number of scientific workshops organized by CURIUM project	2	-
6	Number of workshops, training sessions, and events that facilitate interaction and CRA compliance among European SMEs	>=3; 25-100 participants each; ≥40% of the participants in each event attracted and registered as contacts	-
7	Number of training courses provided by CURIUM (external, from consortium members or developed inside the project)	>10	2
8	Number of information days organized by CURIUM project	2	-
9	Raise awareness activities organized, targeting SMEs, SMEs associations and general public	>5	1
10	Internal Trainings to build staff capacity	≥10 internal trainees for becoming familiar with the CURIUM training tools and program	-
11	Number of EU and international security and networking bodies, agencies and organizations to connect with	>10	>10 identified
12	Clustering activity	>5 similarly themed projects and initiatives identified; >2 jointly organized workshops	>5 identified
13	Number of standardization groups to participate and if possible, contribute	>2	>2 identified
14	Policy-making contributions	engagement of ≥3 policy making bodies	1
15	Impact Max. Update Reports	3 (1 per semester)	1
16	Business Opportunities	≥3 partnerships formed with key business/open-source communities in the field by the end of the project.	-

3.1.4 Communication Tools, Activities and KPIs

Effective communication is a critical aspect of any successful project. Clear and strategic communication will maximize the impact and reach of the project's objectives, results, and achievements. Communication efforts include providing accessible information about the project's objectives, expected outcomes, and important aspects, as well as providing regular updates on events and project outputs. Relevant tools and activities are summarized in the bullet list below followed by a Table of relevant KPIs.

- **Project Website:** A project website that serves as the primary source of information on the goals and activities of the project and enables quick retrieval of key action data with a few clicks. The website was developed in M03 and will be constantly updated and maintained for three years after the project is completed. p-NET is responsible for this activity in task T5.1.
- **Social Media:** CURIUM has established and maintains its online presence across a number of social media platforms, using LinkedIn and X to interact with research and innovation communities and disseminate new publications, and YouTube and Podcasts to engage a large audience.
- **e-Newsletters:** aim to provide a snapshot of the main activities and successes of CURIUM, and gauge engagement, especially when promoting events and outcomes across different domains. To automate the distribution across contact points, expert marketing platforms (like Brevo and

Mailchimp) will be employed. The first Newsletter is under preparation and will be circulated in July 2025.

- **Promotional material:** Flyers, rollup banners, and any other printed paper-based resources, are used when participating in events. Most of the information will be accessible as electronic documents, with printing as needed.
- **Multimedia:** Utilizing the available distribution channels for promotion (such as YouTube and Vimeo), CURIUM will create multimedia content (video-clips) with a self-explanatory and appealing presentation of its scope and results.

Table 0-3: Communication KPIs

No	KPI Description	Target Value	Achieved
1	Website	Visits >= 500 on avg annually; Downloads >=300; or >= 20 monthly on average	From 27/05/ - 25/06/2025: 166 Sessions 317 Pageviews No deliverables yet uploaded
2	Social Media	Push announcements >= 10 monthly; new followers >=5 monthly; retweets >=20 annually; LinkedIn posts >=30 annually	Push announcement: 0 New followers LinkedIn: 125 Retweets X: 0 LinkedIn posts: 7
3	Project accounts	LinkedIn & ResearchGate	LinkedIn & X
4	e-Newsletters	>=3; receivers >= 500	-
5	LinkedIn Discussions	>=20	-
6	Electronic brochures	≥200 downloads	Not yet uploaded
7	Brochures (hard copies)	≥120 hard copies distributed in ≥3 events	≥50 hard copies distributed in 3 events
8	Videoclips	≥ 4 video demonstrators of CURIUM	-
9	Videoclips views	≥1000 views of 5-min videos in You-Tube by the end of the project	-

3.1.5 Rules & Procedures

Internal Communication: Smooth collaboration and efficient operation of any consortium heavily relies on internal communication. A well-functioning communication flow implies that information is precise, unambiguous, and disseminated in a timely manner to everyone concerned. Concurrently, it demands striking an appropriate balance between scarce and excessive information. For the CURIUM project, the main aims of internal communication include:

a./ seamless information exchange among participating partners;

b./ proper and continuous updating of all parties on the project's progress;

c./ alignment of partner activities and resolution of any existing interdependencies;

d./ timely detection and mitigation of potential risks and problems;

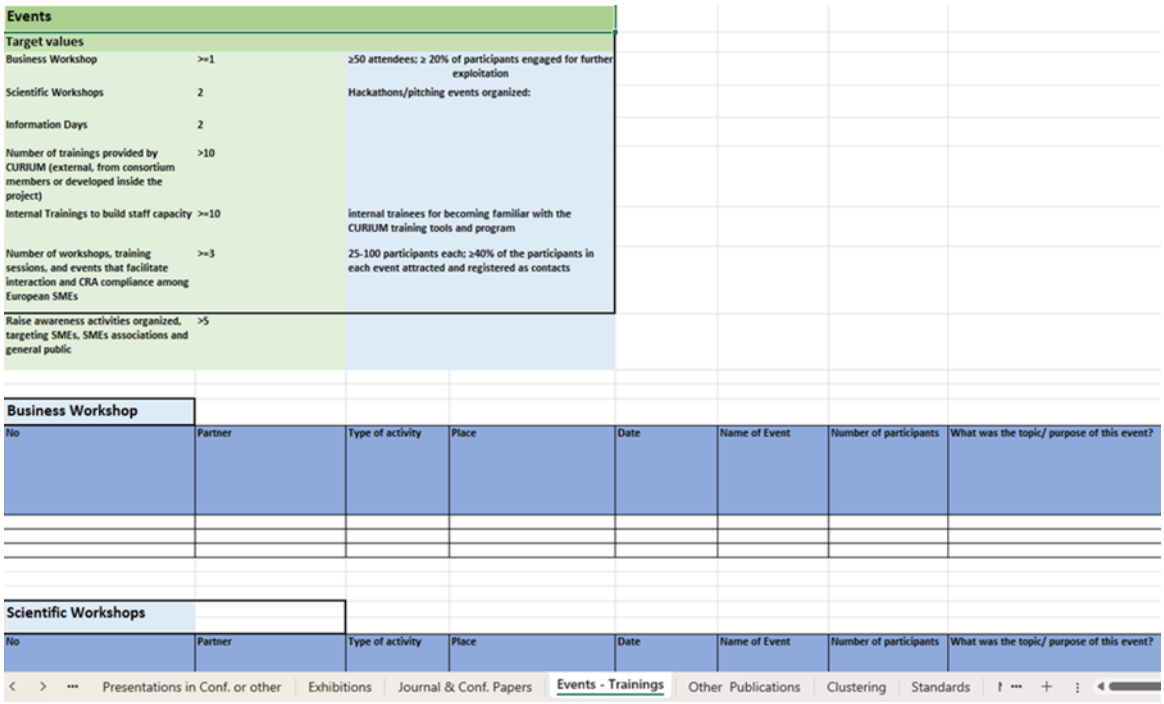
e./ informed decision making.

CURIUM partners engage in communication through the following structured methods: physical or online meetings, e-mails exchange and use of various collaboration tools. For streamlining the internal sharing of information and documents, a SharePoint platform is leveraged with CYS responsible for its management. This way all partners can readily retrieve the latest information, documents, and templates available on the platform.

External Communication: To facilitate the planning, tracking, execution, and oversight of all planned communication and dissemination activities, the Task maintains continuous interaction with all WPs' activities to ensure that project outcomes and results are communicated and disseminated promptly. Regarding external communication, it is crucial to acknowledge that the dissemination of the project's achievements must never jeopardize the potential protection of any generated intellectual property, such as patents or product designs, or impede further industrial application. Consequently, prior to undertaking any dissemination activity, including publications or presentations, strict rules requiring advance notification to all partners will be rigorously applied, consistent with the Grant and Consortium Agreements. All project outcomes will explicitly acknowledge the support received from EU and the ECCC, as mandated by Article 17, titled "Communication, Dissemination and Visibility," and its corresponding Annex 5, "Communication, Dissemination, Open Science and Visibility," both part of the CURIUM Grant Agreement. It is a requirement that the EU emblem, along with a funding statement, always appears in publications. Additionally, dissemination materials should contain the following acknowledgement: "The project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre ('granting authority'), under the powers delegated by the European Commission ('European Commission'), under the Grant Agreement No. 101190372. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC. Neither the European Union nor the granting authority can be held responsible for them". To maintain high standards, processes are in place for the quality control of all dissemination material, covering both its content and its presentation. These processes are designed to check: (i) the messages being shared outside of the consortium, including their appropriateness for the target audience and highlighting their advantages and industrial relevance when relevant; (ii) the technical specifics, to ensure the excellence of the scientific and research goals achieved; (iii) proper reference to the project and the funding authorities; and (iv) the quality of the layout and overall suitability.

Guidelines for partners: Partners are requested and encouraged to report on all planned and implemented project communication and dissemination activities, encompassing publications, participation in events, and contributions to the press and media in the D&C Tool. The D&C Tool is an Excel file that was created at the very beginning of the project, consists of multiple sheets, including events, publications, exhibitions, clustering, standards, as dispayed in the screenshot below. Detailed information about every communication and dissemination action implemented within the project is expected to be reported in the corresponding worksheet-table. The dissemination recording file furthermore enumerates the type, objective, status, and targeted audience of each activity, specifying the methods employed, such as attendance, abstract submission, poster presentations, distribution of materials like fact sheets, oral presentations, demo/video displays, and having a stand or booth. The

communication tracking component offers data on the target audience, publication specifics, the communication channel used, the partner responsible, and the results achieved. Consistent and continuous update of the D&C Tools enables progress tracking against KPIs.



Events		
Target values		
Business Workshop	>=1	≥50 attendees; ≥ 20% of participants engaged for further exploitation
Scientific Workshops	2	Hackathons/pitching events organized:
Information Days	2	
Number of trainings provided by CURIUM (external, from consortium members or developed inside the project)	>10	
Internal Trainings to build staff capacity	>=10	internal trainees for becoming familiar with the CURIUM training tools and program
Number of workshops, training sessions, and events that facilitate interaction and CRA compliance among European SMEs	>=3	25-100 participants each; ≥40% of the participants in each event attracted and registered as contacts
Raise awareness activities organized, targeting SMEs, SMEs associations and general public	>5	

Business Workshop

No	Partner	Type of activity	Place	Date	Name of Event	Number of participants	What was the topic/ purpose of this event?

Scientific Workshops

No	Partner	Type of activity	Place	Date	Name of Event	Number of participants	What was the topic/ purpose of this event?

Presentations in Conf. or other | Exhibitions | Journal & Conf. Papers | Events - Trainings | Other Publications | Clustering | Standards

Publication Policy and Open Access: Partners have committed to depositing peer-reviewed articles generated by the project into a repository, such as Zenodo. They also pledge to make their best efforts to ensure open access to these articles no later than the time of publication. This open access will align with the provisions of Article 17 and Annex 5 of the Grant Agreement. Depending on the consortium's strategy for a specific peer-reviewed scientific publication, either the "green" (self-archiving) or "gold" (open access publishing) model will be utilized. The CURIUM website will feature information about and links to the Open Access Documents for all scientific publications produced by the project.

3.2 Dissemination Activities Performed

As part of the CURIUM Project's comprehensive dissemination strategy, a wide range of activities were conducted to promote project objectives, foster stakeholder engagement, and enhance awareness of the Cyber Resilience Act (CRA) across Europe. These efforts spanned high-profile conference participations, targeted business workshops, interactive exhibitions, and hands-on training sessions. Project partners actively contributed to discussions on emerging cybersecurity legislation, showcased the project, and gathered valuable feedback to inform ongoing work. Through these activities, CURIUM has strengthened its visibility, fostered collaboration among EU-funded initiatives, and laid the groundwork for future capacity-building efforts aimed at enhancing digital resilience.

3.2.1 Conference Participation and Presentations given

Dr. Athanasios Staveris-Polykalas, Senior Cybersecurity Specialist at **p-NET**, participated in the **EU Cyber Acts Conference** held in Brussels from 25 to 27 March 2025. The event gathered over 1,000 stakeholders from 27 countries, including policymakers, industry leaders, product developers, and certification bodies, to explore the strategic impact of the EU's cybersecurity legislation - most notably the newly approved CRA.

Dr. Staveris-Polykalas contributed to key discussions on integrating cybersecurity into digital product development and emphasized the importance of harmonized standards and cross-border coordination. His engagement in the conference has brought valuable insights into the CURIUM consortium, particularly regarding the practical implementation of the CRA and its implications for enhancing digital product resilience across the EU.

Figure 1: Participation in EU Cyber Acts Conference, Brussels

Cyber-security, d.o.o. (CYS) participated in the National Coordination Center Croatia (NKS) conference titled **"Cyber-security: New Challenges and New Opportunities"**, held on 28–29 May 2025 in Zagreb, Croatia. During the event, the CRA and CURIUM projects were presented.

The conference was organized with the support of **ENISA**, **EUCC**, **Croatian NKS**, and **CARNet**, and was aimed at a wide audience, including SMEs, industry professionals, academia, and the IT sector.

Figure 2: Participation in National Coordination Center Croatia (NKS) Conference, Zagreb

The accepted scientific paper titled:" *Towards Automated Certification Framework of Composite Systems: A SWRL-Based Approach*", was presented on **IEEE ICE – 31st International Conference on Engineering, Technology and Innovation**, held from 16 to 19 June 2025 in Valencia, Spain. As part of this high-level academic and industry-focused event, presented scientific paper addressed the intersection of the CRA, Common Criteria (CC), and ontologies for automation.

This contribution highlights research from two projects (CUSTODES – DEKRA and APIROPlus Solution and CURIUM – APIROPlus Solution) on applying semantic technologies to enhance cybersecurity certification processes and compliance automation under the CRA framework. Participation in IEEE ICE 2025 provides an opportunity to engage with leading experts in engineering and innovation, disseminate key results, and gather feedback to further advance the CURIUM project objectives. More information about the conference is available at https://ice-conference.org.

Figure 3 Attending on ICE25 ICEEE Conference

Argiro Chatzopoulou, representing **APIROPLUS Solutions**, participated online in the **CYBERSTAND.eu Annual Event 2025**, titled *"Navigating CRA Compliance – Support Initiatives and Resources,"* held on June 19th, 2025 in Brussels.

Many of the projects showcased during the event focused on the Cyber Resilience Act (CRA) and were funded under the same call.

In a brief, high-level presentation, the free tools and services that make up the CURIUM Continuum were presented, along with the CURIUM Project's broader strategy concerning:

- Risk assessment
- System composition
- Contributions to standardization

The session concluded with a reaffirmation of supporting ongoing standardization efforts and providing constructive feedback to **policy makers** involved in the implementation of the CRA.

Figure 4 Participating on CYBERSTAND Annual Event

3.2.2 Exhibitions

EIT Digital participated in the **Forum InCyber – Europe (FIC2025),** held from 1 to 3 April 2025 in Lille, France. Recognized as one of Europe's leading events dedicated to digital security, the Forum serves as a key platform for discussing cybersecurity trends, regulatory developments, and emerging challenges. It attracted a diverse range of stakeholders, including cybersecurity experts, policymakers, researchers, CISOs, technology providers, startups, investors, and law enforcement agencies.

At the event, EIT Digital promoted the CURIUM project through a dedicated booth and a presentation slot, increasing its visibility among SMEs, industry leaders, and public sector representatives. Booth visitors received detailed insights into CURIUM's mission, objectives, and current activities. In addition, responses to the WP2 questionnaire were gathered, providing valuable input on stakeholder awareness of the CRA and their training needs. These insights will directly support the development of CURIUM's capacity-building strategy.

Figure 5: Participation in Forum InCyber Europe (FIC 2025), Lille, France

APIRO participated in **BEYOND Expo**, held in Athens, Greece from 4 to 6 April 2025, at a booth hosted by the Digital Security Authority of Cyprus. BEYOND Expo is a prominent international technology exhibition that brings together global innovators, industry leaders, researchers, startups, and policymakers to showcase and explore developments across various tech sectors. During the event, APIRO engaged with over 30 stakeholders, including cybersecurity experts, technology providers, students, investors, and public sector representatives. APIRO presented the CURIUM project, distributed printed flyers, shared the stakeholder questionnaire, and held informative discussions with visitors, raising awareness and generating interest in the project's goals and activities.

Figure 6: Participation in BEYOND Expo, Athens, Greece

p-NET hosted an interactive information booth at **TEDxPatras 2025**, where attendees could ask questions and learn more about EU-funded initiatives aimed at improving cybersecurity. This outreach activity helped increase the visibility of the CURIUM project and reinforced its role within the broader European cybersecurity landscape. Approximately 30 CURIUM flyers were distributed to interested participants. Collaboration with the CUSTODES and SAND5G projects was also featured, highlighting strong cooperation among EU-funded initiatives to promote cybersecurity awareness and digital resilience.

Figure 7: Participation in TEDx Patras 2025, Patras, Greece

EIT Digital hosted a booth at the **South Summit** event held from June 4th to 6th, 2025 in Madrid, Spain, showcasing CURIUM and other EU-funded projects in which it participates. The team engaged with start-ups by discussing product security and emphasizing EIT Digital's mission to advance European innovation and ensure compliance with key EU regulations, such as the CRA.

EIT Digital also announced CURIUM's upcoming webinar in July, designed to present the project and outline its capacity-building activities, including startups and SMEs to join these initiatives.

The booth attracted considerable attention from SMEs, highlighting EIT Digital's role as a European Commission-supported entity that assists start-ups at all stages of development.

Furthermore, EIT Digital networked with innovation hubs such as Andalucia Emprende, Asturias, and Euskadi, with plans to collaborate on activities such as cybersecurity talks focused on the CRA. These partnerships aim to enhance CURIUM's visibility and foster strategic collaborations with the European innovation ecosystem.

Figure 8: Participation in South Summit 2025, Madrid, Spain

3.2.3 Business Meetings

EIT Digital participated in a series of business meetings during the **Forum InCyber Europe (FIC2025)**, held in Lille, France on 1–2 April 2025. As part of these meetings, EIT Digital presented the CURIUM project to a targeted audience of industry professionals, cybersecurity experts, and policymakers. The sessions provided an opportunity to highlight the project's objectives, relevance to the CRA, and its potential impact on strengthening cybersecurity capabilities across Europe. In addition to the presentation, EIT Digital actively disseminated the WP2 stakeholder questionnaire to gather input on awareness of the CRA and related training needs. The feedback collected will directly contribute to CURIUM's capacity-building and stakeholder engagement strategies.

Figure 9: Participation in Business Meetings at Forum InCyber Europe (FIC2025), Lille, France

On 5 May 2025, the CURIUM project was presented at the event **"Cyber Resilience Act: Building a Cybersecure Future,"** held in Nicosia, Cyprus at the ICT Academy (Office of the Commissioner of Communications). Co-organized by the Digital Security Authority of Cyprus and the Cyprus Organization for Standardization, the event gathered around 80 participants, including representatives from EU-funded projects, the standardization community, ENISA, and other key cybersecurity stakeholders.

APIRO took the lead in presenting the CURIUM project, emphasizing its alignment with the objectives of the CRA and its contribution to enabling a secure digital transformation across Europe. The presentation highlighted how CURIUM supports CRA implementation by addressing capacity-building needs and enhancing cybersecurity awareness.

The event served as a valuable platform for raising the project's visibility, fostering collaboration among stakeholders, and reinforcing CURIUM's role within broader European cybersecurity and standardization efforts.

Figure 10: Participation in the "Cyber Resilience Act" event, Nicosia, Cyprus

3.2.4 Training

The CURIUM project supported the interactive cybersecurity workshop titled "Think Before You Click! To Hackers, the Easiest Target is You!", held on 17th May 2025 at the University of Patras Conference Center. The workshop was organized by project partner **p-NET** as part of **TEDxPatras 2025** and was conducted in collaboration with the SAND5G and CUSTODES projects - demonstrating strong cooperation among EU-funded initiatives to promote cybersecurity awareness and digital resilience.

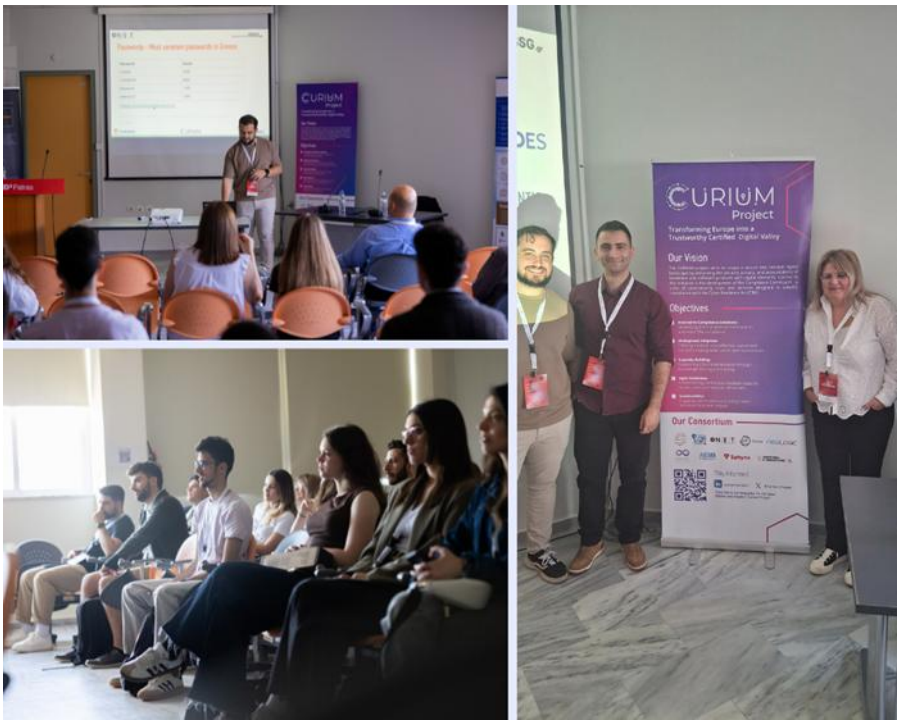
Targeted at youth, the workshop was delivered by Cybersecurity Research Associates George Daniil and Nikolas Filippatos from the University of Patras. The session featured a series of hands-on activities designed to engage participants in real-world cybersecurity scenarios. The training emphasized practical strategies for identifying and mitigating common digital threats, with a special focus on simple, actionable steps individuals can take to improve their online security.

The workshop effectively conveyed key messages of the CURIUM project, and its commitment to raising cybersecurity awareness and strengthening digital resilience among citizens and SMEs. The Workshop had approximately 45 attendees.

In parallel, **p-NET** hosted an interactive information booth where attendees could engage with project representatives, as described under the section “Exhibitions” above.

The event attracted a diverse audience and was considered highly successful in terms of engagement and impact. It constitutes a valuable contribution to the project’s training, communication, and dissemination objectives, as outlined in the CURIUM dissemination plan.

Figure 11: Cybersecurity Training Workshop at TEDx Patras 2025, Patras, Greece



3.3 Communication Activities Performed

The CURIUM Project has developed a cohesive visual identity to effectively communicate its core values of cybersecurity, innovation, and trust. While the project logo plays a key role in establishing a professional and modern brand, equal importance has been placed on building a strong online presence. The project website serves as the central hub for information, offering accessible, user-friendly content aligned with the project's goals. In addition, CURIUM’s social media accounts on LinkedIn and X support ongoing communication, stakeholder engagement, and visibility within the research and policy communities. Together, these platforms enhance the project’s outreach efforts, ensure consistent branding, and foster collaboration across relevant networks and EU-funded initiatives.

3.3.1 Logo

The CURIUM logo was designed to embody the core values of the project: cybersecurity, resilience, protection, and the reliability of digital solutions.

Two versions of the CURIUM logo were presented to all partners, with the first option, shown in Figure 10 below, being the preferred choice of the majority.

Figure 12: CURIUM's Logo

Every design element of the logo was meticulously chosen to integrate technological aesthetics with a modern and trustworthy identity. The balance between a modern, clean typeface and advanced technological motifs creates a visual identity that conveys professionalism and dynamism.

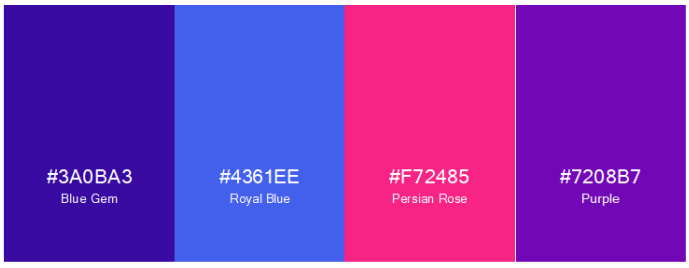
To effectively communicate this message visually, three key elements were required:

- A carefully selected colour palette.
- Appropriate typography.
- A dominant leading element.

The colour scheme of the logo as illustrated in Figure 11 was based on shades of purple and blue, strategically selected to convey reliability, innovation, and technological advancement. Purple is associated with knowledge, creativity, and futuristic thinking - qualities that align perfectly with the vision of the CURIUM project.

Blue enhances the feeling of security, trust, and stability - essential attributes in cybersecurity. The combination of these shades creates a modern, dynamic, and technologically advanced visual identity that fully aligns with the mission of the CURIUM Project.

Figure 13: CURIUM Project's Colour Pallet



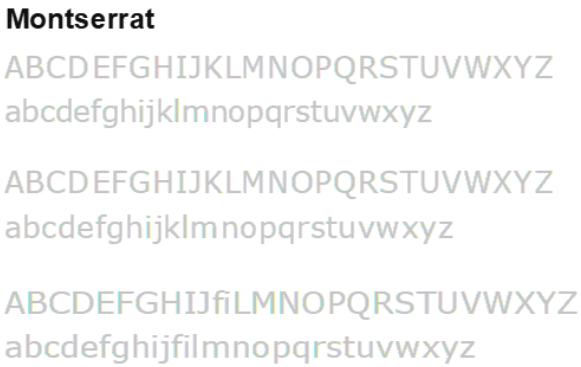
Typography

The Montserrat typeface shown in figure 12 was carefully chosen as most suitable for the logo due to its modern, highly legible, and professional character. Its geometric structure conveys stability and precision, while its clean lines make it ideal for applications related to technology and security.

Montserrat furthermore maintains a contemporary and user-friendly aesthetic while preserving the level of seriousness required in a field such as cybersecurity.

Pairing this typeface with the technological elements of the logo achieves a perfect balance between innovation and trustworthiness, resulting in a professional and dynamic visual identity.

Figure 14: CURIUM Logo's Typography



Dominant Element

The central design feature of the logo is the letter C, which serves as the visual focal point of the design.

As shown in figure 13 the letter "C" is surrounded by circular technological patterns, reminiscent of digital circuits and data flow, symbolizing interconnectivity, information, and cybersecurity. Additionally, the second "U" is designed to resemble a lock.

This approach highlights resilience and scientific precision, positioning CURIUM as a pioneering research project with a strong emphasis on cybersecurity.

Figure 15: CURIUM's Logo's Dominant Element

The logo is a cornerstone of all communication materials and has been used in all promotional material of the CURIUM Project, including the website, banner, flyers and social media.

3.3.2 Website

The logo design of the CURIUM Project served as the foundation for the website's visual identity, ensuring consistency and recognisability across all project communications and materials. The website was developed to reflect the project's core values - innovation, collaboration, and accessibility - while maintaining a professional and intuitive user interface.

The website is accessible at: www.curium-project.eu.

Its visual layout, colour scheme, and typography are directly inspired by the official project logo, which was selected by partner consensus. This branding coherence reinforces the CURIUM identity and improves visibility across platforms.

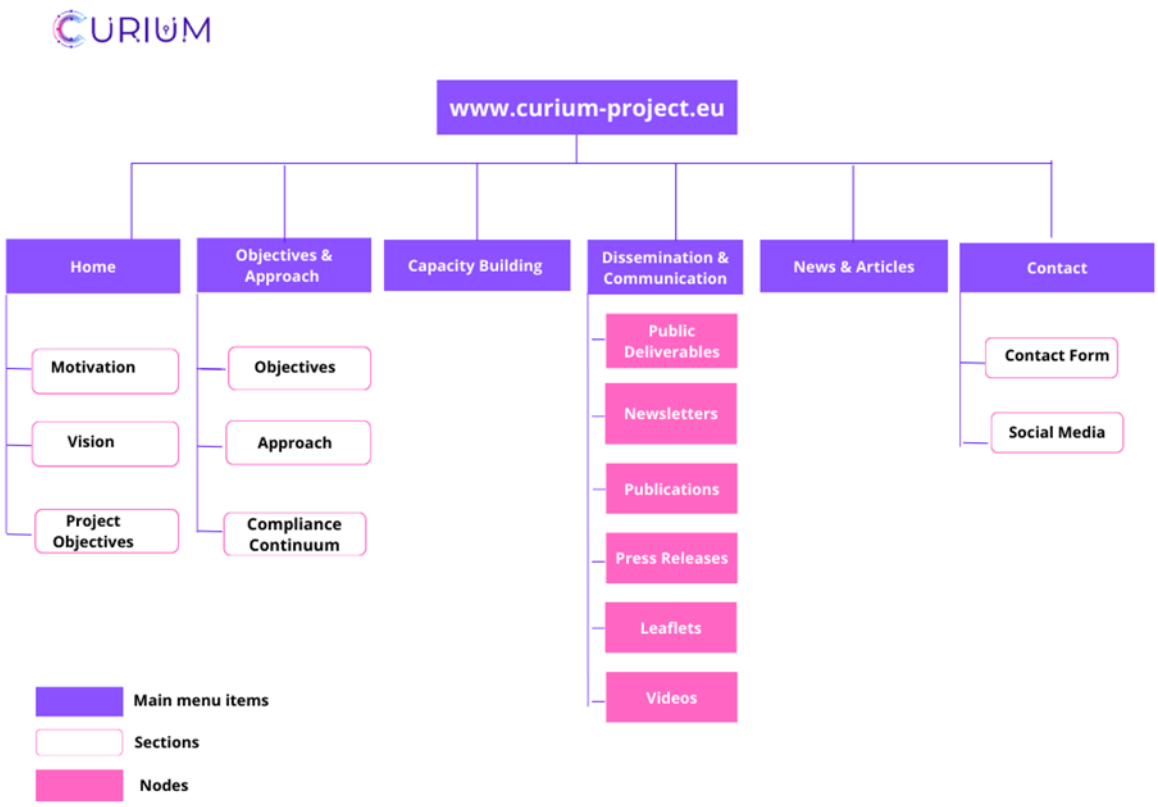
Functionally, the website serves as the central hub of information for the CURIUM Project. It plays a key role in communication efforts, reaching both the general public and relevant stakeholders who may benefit from the project or wish to engage in its activities. The design prioritises practicality and user engagement, offering structured, relevant content across its various pages.

Figure 14 outlines the website sitemap highlighting its key features, including:

- An overview of the project's motivation, vision, and objectives.
- A dedicated section on capacity building.
- A Deliverables section under Dissemination & Communication.
- A regularly updated News & Articles section, with subpages for newsletters, publications, press releases, and public engagement activities.
- Links to the project's social media channels.
- A Contact page where interested parties can reach out to learn more or participate in project activities.

To maximise accessibility and usability, the website was developed using a responsive design, ensuring seamless performance across desktop and mobile devices. It was also built in accordance with the Web Content Accessibility Guidelines (WCAG), supporting users with varying levels of ability.

Figure 16: Website Sitemap



3.3.2.1 *Website Development and Design Methodology*

The CURIUM Project website was developed using the WordPress Content Management System (CMS) - a flexible, scalable platform that allows for efficient content updates and long-term maintenance. WordPress was chosen for its user-friendly backend, which enables the project team to manage content autonomously throughout the project lifecycle.

During the design and implementation of the website, emphasis was placed on both User Interface (UI) and User Experience (UX) principles. The site was intentionally built to be content-rich, easy to navigate, and visually aligned with the CURIUM brand.

To ensure a high-quality user experience, the following design principles were applied:

Aesthetically Pleasing Visual Design

- Clean, modern layout consistent with the project's branding.
- Logical grouping and alignment of content.
- Effective and purposeful use of graphics and colour.

Comprehensibility

- Intuitive and easily understood interface.
- Clear navigation paths that help users quickly locate information.

User Control

- All actions are user-initiated.
- Interactions are responsive and reversible.
- The system avoids disruptive error messages.

Simplicity

- Streamlined interface with minimal complexity.
- Common actions are readily accessible.
- Prominent placement of key functions.
- Consistent design patterns across all pages.

Efficiency

- Reduced cognitive load through minimal eye and hand movement.
- Smooth transitions between sections.
- Optimised navigation paths.

Clarity

- Clear content and icons.
- Visually and conceptually coherent interface.

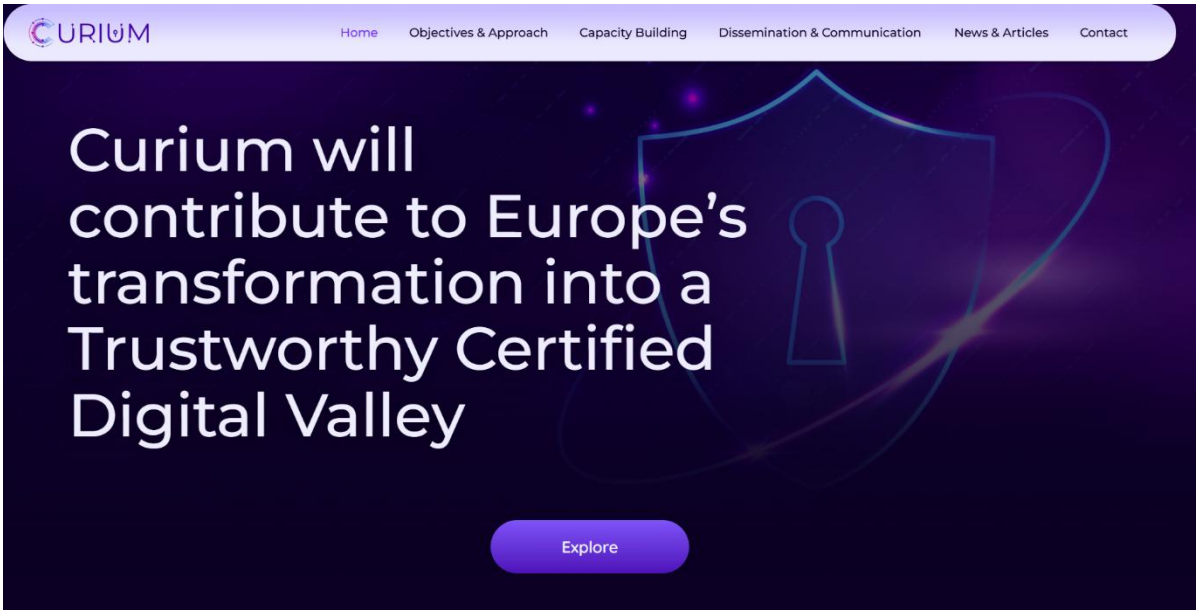
Consistency

- Uniform appearance and functionality across all pages.
- Repeated actions produce consistent results.
- Core navigation and structural elements maintain fixed positions.

The structure and design of the CURIUM website reflect the project's strong commitment to accessibility, clarity, and effective communication. As a dynamic communication tool, it plays a crucial role in stakeholder engagement, the promotion of project results, and the delivery of transparent updates to a broad audience, including researchers, policy makers, and the general public.

The website will be actively maintained and updated throughout the duration of the project to ensure timely sharing of progress, resources, and results. It is operated by p-NET, a partner committed to operate the site beyond the project lifetime.

Figure 17: Website homepage

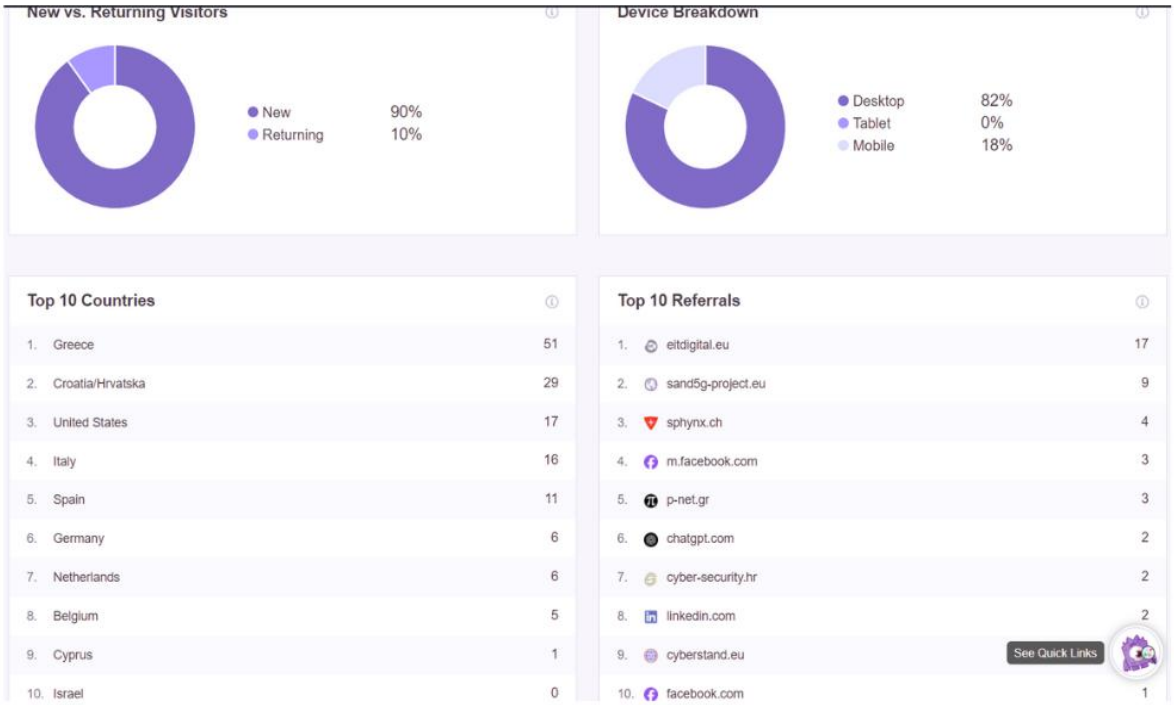


3.3.2.2 Website Administration

The administration site of the CURIUM website has been developed with the use of WordPress, a web-based software that professionals use to design a website, with additional focus on security, accessibility, performance and user-friendly features which are regularly maintained throughout the project.

The D&C Leader has access to the website analytics, through Monster Insights, aiming to observe and report on the website's traffic and results. This tool assists the project consortium in tracking activities within the website. The analytics will be tracked by the D&C Leader of the project, and updated statistics will be periodically provided to the project consortium.

Figure 18: Website statistics: New vs. Returning Visitors & Devices breakdown (as of 18/06/25)



3.3.3 Social Media

To support its communication and outreach efforts, the CURIUM Project has established social media accounts on LinkedIn and X (Twitter), serving as dynamic platforms for communication, visibility, and stakeholder engagement. These platforms play a key role in CURIUM's broader D&C Plan, helping to promote project activities, share progress, and foster collaboration with relevant organisations, networks, and other EU-funded initiatives.

The project's social media accounts are:

LinkedIn: www.linkedin.com/company/curium-project

X (Twitter): @Curium_Project

These accounts were created in month three of the project and shared with all project partners, who were encouraged to follow, share, and promote them within their professional networks. This collaborative approach supports both early audience growth and sustained engagement with broader research, policy, and educational communities.

Content shared through these channels will include:

- Project updates and milestones
- Public deliverables and key outputs

- Announcements of events, workshops, and training activities
- Press releases
- Opportunities for collaboration or public engagement

Social media activities are aligned with the project's D&C Plan, and are coordinated by the D&C Leader, with contributions from all partners. Regular updates are shared to maintain visibility and provide timely information to followers.

The CURIUM Social Media Strategy is built around the following core principles:

- *Channel Selection*
  Choosing platforms based on their popularity, suitability, and effectiveness for reaching the project's target audiences.

- *Audience Targeting*
  Identifying and focusing on specific stakeholder groups aligned with the Grant Agreement (GA) and the project's impact goals.

- *Content Promotion*
  Highlighting project outcomes consistently, ensuring that results and activities are clearly communicated and accessible.

- *Use of Diverse Tools and Formats*
  Employing a variety of communication methods, such as social media posts, press releases, articles, and videos, to maximise visibility and engagement.

- *Performance Monitoring and Adaptation*
  Designing a monitoring framework to track social media performance and adapt the strategy based on data insights. This ensures flexibility in addressing underperforming areas or adjusting focus on specific groups as needed.

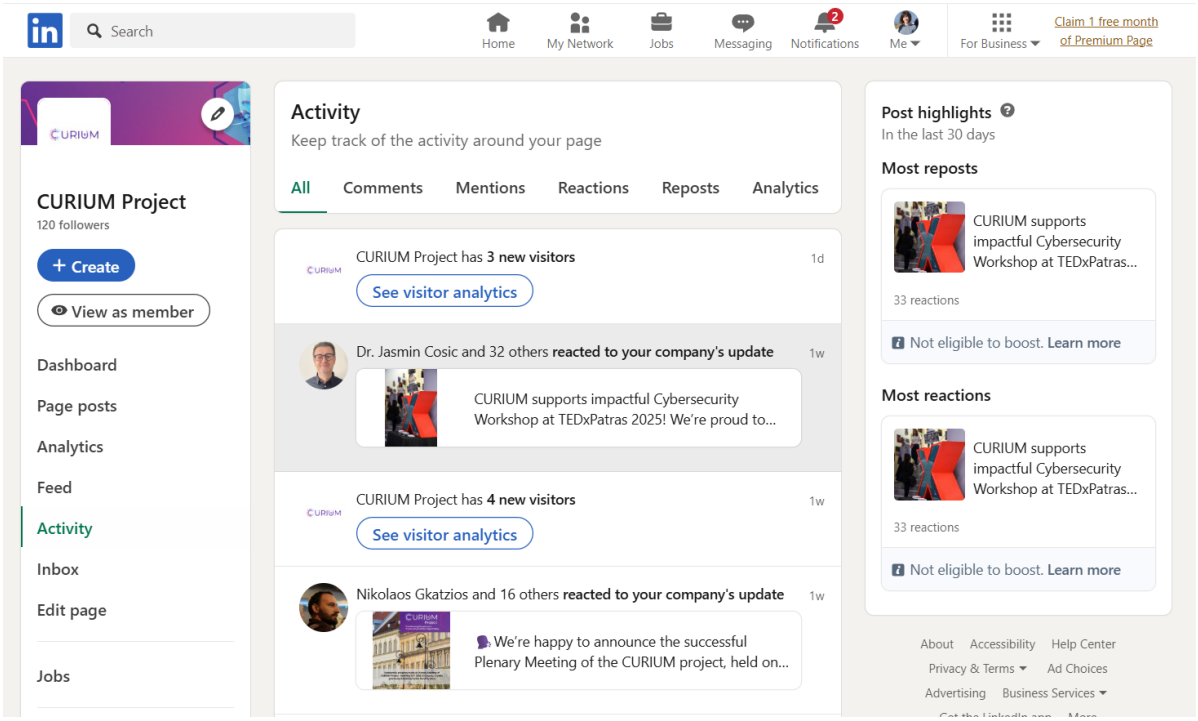
Overall, CURIUM's use of social media complements its broader communication objectives, creating an accessible, timely, and responsive channel for engaging stakeholders and sharing the project's mission and results with diverse audiences across Europe and beyond.

3.3.3.1 Social media metrics

Social media metrics, such as follower growth, impressions and engagements are regularly monitored. These analytics inform the communication and communication strategy, enabling adjustments where needed to enhance effectiveness and ensure that target audiences are reached.

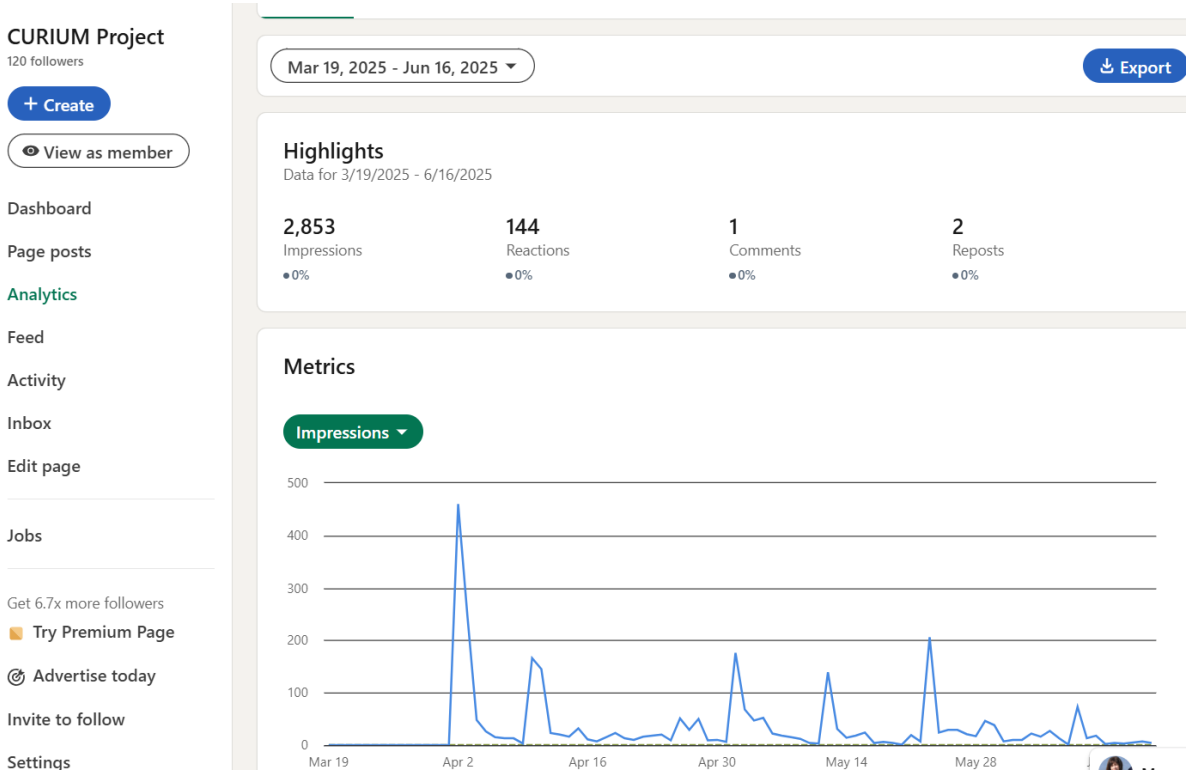
As shown in Figure 17, the LinkedIn account currently has 120 followers as of Month 6 of the project.

Figure 19: Screenshot of CURIUM's LinkedIn Account



The following figure depicts the total number of impressions, reactions and reposts on CURIUM's LinkedIn page from 19/03/25 to 16/06/2025.

Figure 20: LinkedIn Statistics from 19/03 – 16/06/2025



As shown in figure 19 below, the followers on X currently amount to 6 followers, as of month 6 of the project.

Figure 21: CURIUM Project's X (previous Twitter) Account

3.3.4 Flyers / Banners

As part of its communication and outreach efforts, the CURIUM Project has developed a suite of promotional materials, including flyers and a banner, designed to support both digital and physical communication activities. These materials are key tools for raising awareness, enhancing visibility, and engaging stakeholders at events, conferences, and workshops.

The official CURIUM flyer presents a clear and engaging overview of the project's vision, objectives, methodology and capacity building. It is designed to be visually aligned with the project's branding, incorporating the logo, typography, and colour scheme. The flyer includes:

- A concise summary of the project's objectives and rationale.
- Approach, which includes the key actors in ensuring a comprehensive, industry-driven framework for cybersecurity resilience and compliance.
- Project partners' logos.
- Links to the project website and social media platforms.

A printable version of the flyer has been uploaded onto the project's SharePoint, which may be printed and distributed at partner institutions, stakeholder meetings, and public events. A digital version is also

available for download via the CURIUM website and can be shared through mailing lists and social media.

Figure 22: CURIUM's flyer

To support the visual presence of the project at public-facing events, a roll-up banner has been designed in line with the CURIUM visual identity. The banner may be used at:

- Project meetings
- Training workshops
- Academic conferences
- Community outreach events.

The banner features the CURIUM logo, a concise summary of the project's vision and scope, and the logos of all project partners. Its layout is designed to ensure quick readability and strong brand recognition, while maintaining a professional and visually appealing appearance. A QR code is also included, allowing interested individuals to easily access the CURIUM project website by scanning it with their mobile devices.

Both flyers and banners have been created with flexibility in mind, allowing for updates or new versions as the project progresses and milestones are reached. All materials adhere to the EU visibility guidelines, including proper acknowledgment of funding through the display of the EU emblem and the support of the European Cybersecurity Competence Centre (ECCC).

These promotional tools are essential to CURIUM's wider communication strategy, helping the consortium communicate effectively with target audiences and ensuring consistent messaging across different formats and settings.

Figure 23: CURIUM's roll-up banner at TEDx Workshop, Patras, Greece

4. Exploitation Strategy and Plan

Task 5.2. of the project aims to support (amongst others) impact creation and exploitation planning. As part of this task, the project plans to conduct market-oriented analysis and planning to pave the way for identifying (firstly) and paving the way for fulfilling (at a later stage) the project's market potential. To be able to effectively implement this process and extract the desired results, the project partners have created an Exploitation and Market analysis strategy.

4.1 Exploitation and Market analysis strategy

Based on the information of the European Commission on Research and Innovation[1], exploitation is the use of results in developing, creating and marketing or improving a product or process, or in creating and providing a service in standardisation activities or shaping a policy.

Exploitation can be commercial, societal, political, or aimed at improving public knowledge and action. It also includes recommendations for policy making through feedback to policy project partners or facilitating uptake by others e.g. through making results available under open licences.

Exploitation focuses on the actual use of the results, translating research concepts into concrete solutions that have a positive impact on the public's quality of life.

The focus of the dissemination and exploitation activities is on the results, i.e. all output generated by the project during its implementation.

The Exploitation and Market analysis strategy of the CURIUM project, consists of the following steps:

- **Identification of the exploitable results of the project.** One cannot speak about the concept of exploitation without first clarifying the term project results and how this is interpreted within the CURIUM project. Based on the definition provided by the Horizon 2020 programme manual[2], project results are defined as "any tangible or intangible output of the action, such as data, knowledge and information whatever their form or nature, whether or not they can be protected, which are generated in the action as well as any attached rights, including intellectual property rights". In simpler terms, the project results are outcomes of the project which can be used by the project partners or external (to the project) stakeholders during and after the end of the project. Such outcomes could be used to support internal activities of the partners, to become concrete products or services provided to external or internal customers, to be become part of products or services, to lay the foundations of further research or even to improve the understanding of a partner on a subject. These results will be called throughout the rest of the document as Exploitable Results (ERs).
- **Identification of IP protection issues**. The ERs could be subject to Intellectual Property protection as defined also within the Grant Agreement. During this stage, each participant, who brings in

[1] https://research-and-innovation.ec.europa.eu/strategy/dissemination-and-exploitation-research-results_en

[2] Dissemination & Exploitation - Open Access - H2020 Online Manual

Intellectual Property Rights (IPR) into the project or has developed IPR within the project, shall clearly identify and document these rights against the Exploitable Results. These issues will be taken into consideration in the creation of the individual or any joint exploitation plans of the CURIUM project ERs.

- **Identification of ownership of the ERs.** The ownership of each ER will be identified. Results may be owned exclusively by one partner or may be jointly owned by one or more partners. These cases shall be identified and – in the cases of joint ownership – specific provisions shall be made for the management of exploitation activities.
- **Identification of stakeholders and market potential**. The key audience for each ER shall be identified, along with the market's and customer's needs and wants. During this part of the process, the potential users/stakeholders of the ERs shall be identified and answers to the following questions shall be sought: Which are the potential users/stakeholders needs and demands? - What are the user's gains? What are their gains from your solution? - What are the potential markets? - Who is the competition and what solutions exist already? - What is the unique selling proposition of your expected outputs, and why is it "better"? To support this analysis the CANVAS Model shall be used.
- **Creation of exploitation plans**. Taking into consideration the exploitation interests of the project partners, the possible exploitation routes as well as the results of all the previous steps, the project partners shall define initial exploitation plans at an individual level and for the jointly owned ERs. Within these plans, effort will be invested in the identification of different exploitation measures to ensure that results will meet real needs during the project lifetime and beyond. This project has a lifetime limited to 18 months, so the focus will be beyond the project lifetime rather than during.

4.2 Identification of the Exploitable Results of the Project

As defined in the methodology, the first step of the process is to provide a structured way for the partners to identify exploitable results. To this effect, a suitable form was created and provided to the partners after a workshop / demonstration.

Each result is described in terms of what it is, which partner(s) developed it, and what purpose it serves. This includes both tangible and intangible outputs, such as software tools, methodologies, guidelines, services or knowledge resources.

The document consists of the following sections:

- **Basic Information.** Requesting information on the partner, the name of the Exploitable result, the type of the result, its main functionalities, the expected project month of completion and the possible exploitation path.
- **Assistance.** Requesting information on the type of assistance needed by the partner to achieve the effective exploitation of the result.
- **Technical maturity.** Requesting information on the technical maturity of the result based on the TRL scale.
- **Market demand.** Requesting information on the market demand and readiness level of the market.
- **Value proposition canvas.** Requesting information on the fit of the result for the market following the Value Proposition Canvas initially developed by Dr Alexander Osterwalder.

The template document used is presented in Annex I of this document.

Results of the data collection:

The following table depicts the Exploitable Results identified by the project partners during the first iteration of the exploitation results data collection process. More than 10 Exploitable Results were identified during this first iteration of exploitable results data collection.

Table 0-4: List of Identified Exploitable Results

Exploitable Result (ER)	Type of ER	TRL (M0)	TRL (M18)
CURIUM Continuum	Portal	0	7
Penetration Self-Testing and Vulnerability Assessment Services and tools (PSTVA)	Software	7	8
Cyber Resilience Assessment service (CyReA)	Software	7	8
Digital Product Risk management (DPRA)	Software	7	8
Conformity Assessment and Compliance service (CAC)	Software	6	8
Digital Product Maturity Assessment (DPMA)	Software	7	8
CURIUM Compliance Continuum Blueprint Design	Design	7	8
CURIUM capacity building plan	Plan	N/A	N/A
Training material for the CRA	Training material	N/A	N/A
End Users' Needs in Relation to the Cyber Resilience Act	Information / Knowledge	N/A	N/A
Capacity Building Services	Service	N/A	N/A
Policy recommendations	Information / Knowledge	N/A	N/A
Contributions to standards	Information / Knowledge	N/A	N/A

4.3 Identification of IP protection issues

The Grant Agreement recognizes in Article 16 the existence of background identified as needed for the implementation of the action. The term "background" means any data, know-how or information — whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights — that is:

(a) held by the beneficiaries before they acceded to the Agreement and

(b) needed to implement the action or exploit the results.

During the grant agreement process, the project partners have already identified and declared in writing the background, as specified above.

During the Consortium Agreement process of the project, the various partners have already declared their background and the following provisions regarding ownership apply:

Joint ownership is governed by Grant Agreement Article 16.4 and its Annex 5, Section Ownership of results, with the following additions:

- each of the joint owners shall be entitled to use their jointly owned Results for non-commercial research and teaching activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s).
- each of the joint owners shall be entitled to otherwise Exploit the jointly owned Results and to grant non-exclusive licenses to third parties (without any right to sub-license), if the other joint owners are given: (a) at least 45 calendar days advance notice; and (b) fair and reasonable compensation.

The joint owners shall agree on all protection measures and the division of related cost in advance.

As for the exclusively owned or developed results, these are and remain within the exclusive ownership of the identified owner.

To further support this step of the strategy, as well as the next ones, and ultimately the drafting of the exploitation plans, a suitable form was created and provided to the partners after a workshop / demonstration.

This form (Individual Exploitation Design) requires the following information for each of the Exploitable Results:

1. Partner / Owner
2. Relevant Exploitable Result(s)
3. Exploitation Goal
4. Exploitation Method
5. Target Stakeholders or Customers
6. Short-Term Actions and Benefits (during project or soon after)
7. Long-Term Perspective
8. IPR Status or Support Needs

The following table depicts IP related information identified by the project partners during the first iteration of the individual exploitation design analysis.

Table 0-5: Exploitable Results

Exploitable Result (ER)	Exploitation Goal	IPR Status or Support Needs
CURIUM Continuum	The CURIUM Compliance Continuum constitutes a comprehensive ecosystem designed to function as a unified platform for small and medium-sized enterprises (SMEs) that manufacture or own ICT products. This modular solution aims to provide systematic guidance throughout the CE marking compliance process, with specific alignment to the requirements established under the Cyber Security Act framework.	Developed by CURIUM project partners.
Penetration Self-Testing and Vulnerability Assessment Services and tools (PSTVA)	The main objective is to offer a security assessment tool that helps customers to firstly identify and secondly mitigate vulnerabilities within their products/infrastructure. The tool aims to help businesses secure their IT infrastructure, web services, and user management systems efficiently and accurately	Developed by AEGIS Several tools are involved * e.g. Nmap – License: Nmap Public Source License (based on GNU GPLv2), Nikto – License: GNU GPL v2 etc.
Cyber Resilience Assessment service (CyReA)	The tool enables SMEs with various roles and responsibilities in the supply chain to determine the category to which their ICT products with digital elements belong according to the Cyber Resilience Act (CRA). It aims to ensure that the manufacturer/owner has verified that the ICT products have been assessed and comply with certain essential requirements related to the Cyber Resilience Act (CRA) of the incorporated digital elements.	Developed by NLG
Digital Product Risk management (DPRA)	The tool supports the dynamic assessment of risk based on the temporal parameters of the ICT product with digital element such as vulnerability exploitation and asset dependencies. It provides capabilities to the organisations for managing their security risks in a holistic and cost-	Developed by NLG

	effective manner by assessing both individual and cascading risk.	
Conformity Assessment and Compliance service (CAC)	The main objective of the developing the tool is to offer a security solution that helps customers to firstly check their possible compliance/non-compliance with CRA, identify the gaps. Second the tool will provide a few functionalities regarding technical documentation management, post-market analysis, legal intelligence, etc.	Developed by CYS
Digital Product Maturity Assessment (DPMA)	The Security Assessment Tool combines multiple sources (standards and other international publications) and proposes a series of risk treatment actions depicted against a maturity scale and cross referenced to the controls of ISO 27001.	Developed by APSS
CURIUM capacity building plan & services	The project's capacity-building plan is designed to support SMEs in navigating cybersecurity regulations, fostering a culture of security, and enabling a smoother digital transformation within the European innovation ecosystem. The aim is to empower SMEs across Europe with cybersecurity competencies and CRA compliance. Planned services involve: 1. Training and Education, 2. Experimentation and Testing, 3. Consulting and Support Services, 4. Awareness and Knowledge Transfer, 5. Collaboration and Sustainability.	Developed by EITD & p-NET

** A detailed Excel file has been created and will be retained and updated throughout the lifetime of the project of the specific tools comprising this service. For each one of the tools, the licence governing the usage and operation has been depicted.*

4.4 Identification of ownership of the ERs

Table 0-6: List of the ownership status of the Identified Exploitable Results

Exploitable Result (ER)	Type of ER	Owner
CURIUM Continuum	Portal	Joint ownership
Penetration Self-Testing and Vulnerability Assessment Services and tools (PSTVA)	Software	AEGIS
Cyber Resilience Assessment service (CyReA)	Software	NLG

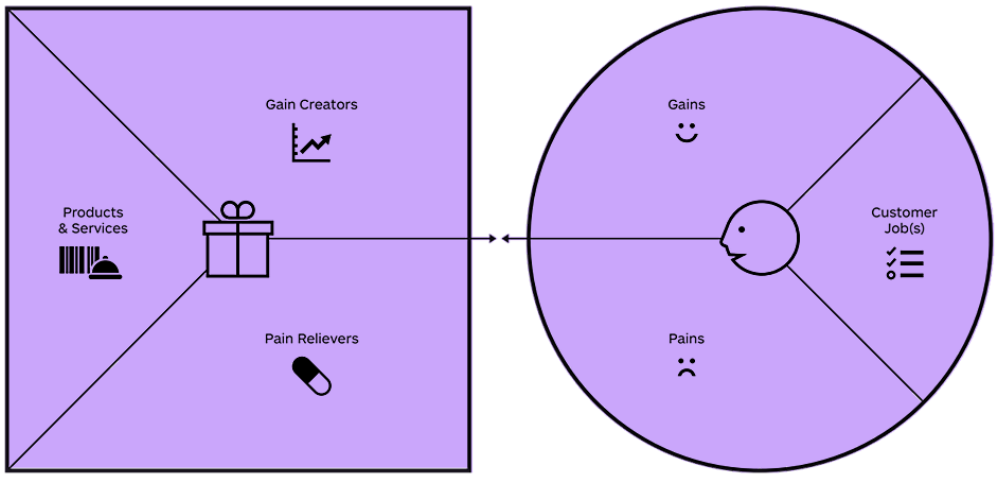
Digital Product Risk management (DPRA)	Software	NLG
Conformity Assessment and Compliance service (CAC)	Software	CYS
Digital Product Maturity Assessment (DPMA)	Software	APSS
CURIUM capacity building plan	Plan	EITD, p-NET
Training material of CRA	Training material	Joint ownership
End Users' Needs in Relation to the CRA	Information / Knowledge	Joint ownership
Capacity Building Services	Service	Joint ownership
Policy recommendations	Information / Knowledge	Joint ownership
Contributions to standards	Information / Knowledge	Joint ownership

4.5 Identification of Stakeholders and Market Potential

For the identification of the stakeholders and the market potential, the project utilizes the Value Proposition Canvas. The Value Proposition Canvas, developed by Dr. Alexander Osterwalder, is a framework that helps ensure a strong fit between a solution and the market. It focuses on two key elements of a business model: the customer segments and the value propositions. In this context, it is used to identify the targeted customers for the ERs of the CURIUM project and to better understand their needs. Each ER may have its own canvas, or one may be developed for the main output of the CURIUM project (The CURIUM Continuum).

The following figure shows the structure of the Value Proposition Canvas, which supports the alignment between customer needs and project outcomes.

Table 0-7: Value Proposition Canvas (adapted from Strategyzer)



For each one of the identified ERs, the canvas will be used to guide the collection and analysis of needed information. This exercise has been initiated and will be developed at full scale in the next months. Relevant results will be reported in Deliverable D5.2 - Final report on Dissemination, Exploitation, Standardisation & Sustainability, due in Month 18. In the present deliverable, an illustrative example is included. It relates to

Penetration Self-Testing and Vulnerability Assessment Services and tools (PSTVA)

Name:	Penetration Self-Testing and Vulnerability Assessment Services and tools (PSTVA)
Description of ER:	It is a tool which integrates a collection of automated and semi-automated penetration testing tool suites and frameworks, managed through a central dashboard).
Scope:	This includes the evaluation of the added value the ER delivers through its core functionality: Network vulnerability assessment and Web service vulnerability assessment. The analysis will examine the way the tool addresses specific customer pains and gains across various industries.
Stakeholders: & their needs	SMEs developing or deploying digital products. Identify and assess vulnerabilities in networks and web services as part of risk management and CRA compliance. Conduct internal security audits and produce vulnerability reports that align with CRA requirements. Demonstrate due diligence to clients, partners, or regulators. Feel confident in facing external audits. Get insights and support for decision-making on risk management.
Gains:	Automated and semi-automated vulnerability scanning reduces manual effort in assessments. Produces technical outputs that can be used as audit evidence (e.g., vulnerability scan results). Stakeholders gain clarity on actual risks and vulnerabilities. Central dashboard allows orchestration of multiple tools, fitting into varied IT

	environments. Saves internal staff time through automation and centralized management.
Pains:	SMEs have issue to interpret how CRA applies to their products or systems (High Severity, High Frequency) Vulnerability assessments often rely on disconnected tools with different interfaces, output formats, and learning curves. (High Severity, High Frequency) In SMEs, there may not be dedicated cybersecurity staff to conduct or interpret assessments. (Medium-High Severity, Medium Frequency) Generating clear, auditable reports that align with CRA is not trivial (Medium Severity, Medium Frequency) Non-compliance can result in significant financial and reputational consequences. (High Severity, Medium Frequency)
Gain creators:	By integrating various penetration testing and vulnerability assessment tools and frameworks into a single centralized dashboard, the tool significantly improves operational efficiency. The modular nature of the tool allows it to be easily adapted for different products, teams, or environments. Automations of the tool allow personnel with limited cybersecurity expertise to perform assessments and gain basic knowledge of their company's cybersecurity posture.
Pain relievers:	The tool eliminates the need for compiling results from various tools manually. This reduces the time spent preparing for compliance assessments and ensures that no data was left out while minimizing duplication in the documentation process. The tool reduces the need for expensive external penetration testing or consultancy services by enabling internal security teams to conduct vulnerability assessments themselves.
Prod. & Services:	The software tool enables the automated scanning of networks and web services for vulnerabilities. Generates standardised reports that can be directly used for CRA compliance, internal documentation, and audits. These reports include vulnerability findings, risk assessments, and suggested remediation actions. The tool can be used on a recurring basis, allowing organisations to conduct continuous vulnerability assessments to stay compliant with CRA.

4.6. Creation of Exploitation Plans

The final step of the Exploitation strategy of the project is the creation of the exploitation plans. The exploitation plans are divided into two categories, individual exploitation plans (one for each partner) and common exploitation plan for the jointly owned CURIUM Continuum. In the present deliverable Individual Exploitation Plans of all beneficiaries are defined and reported. Common exploitation plans will be reported in Deliverable D5.2.

4.6.1 Individual Exploitation Plans

An individual exploitation plan focuses on how to best utilize the results of a project for the benefit of specific individuals, particularly those involved in its development or who will be impacted by it. It outlines the activities needed to ensure the project's continuation and maximize its impact, including how to share the results with relevant stakeholders and involve them in the project's development.

This section provides an overview (high level) of the individual exploitation plans of each partner of the CURIUM project.

CYS

Cyber-security, d.o.o. is currently engaged on the tool development and the plan is to have first Beta version ready in M9 (TLR:8 will be reached). After obtaining the feedback from the partners and SME which will be engaged in evaluation, the plan is to have FR ready in M12. The plan is to use CAC tool to support SME in compliance check and conformity assessment with CRA. Also, the training materials delivered in this project will be used to support SME and customers to fulfil CRA requirements. The main objective of developing the tool is to offer a security solution that helps customers to firstly check their possible compliance/non-compliance with CRA, identify the gaps. Second the tool will provide a few functionalities regarding technical documentation management, post-market analysis, legal intelligence, etc. The tool aims to help SME to have their product secure and resilient. Target customers include medium to large enterprises across multiple sectors: IT & Cybersecurity, Healthcare, Financial Services & Banking, Energy, Retail, and E-commerce.

SPHYNX

As the lead beneficiary of Work Package 2 and responsible for Task 2.3 concerning CURIUM Compliance Continuum Design and technical specifications, SPHYNX will acquire significant technical knowledge and specialized expertise in automated regulatory compliance processes, specifically aligned with the Cyber Resilience Act requirements.

SPHYNX develops and maintains a comprehensive product suite designed to enable enterprises to establish, continuously monitor, assess, and manage security and privacy risks across their organizational assets and business operations. This solution encompasses ICT infrastructures, applications, data assets, and business processes, providing both technical risk assessment capabilities and business/economic impact analysis. The company's participation in CURIUM project delivers substantial exploitable outcomes through two primary channels:

Enhanced Product Development and Validation: The project enables SPHYNX to further validate and refine its existing service offerings, including third-party security assessment services and cyber-range training solutions. The technical insights and regulatory expertise gained through the project activities will directly enhance the quality, accuracy, and market relevance of these products.

Strategic Market Positioning: The specialized knowledge and demonstrated expertise in Cyber Resilience Act compliance automation positions SPHYNX advantageously for participation in future

relevant EU-funded projects and commercial opportunities within the evolving cybersecurity regulatory landscape.

p-NET

The p-NET Competence Centre empowers organizations in the field of Emerging Smart Networks and Services. We achieve this by facilitating knowledge and technology transfer through various services. Businesses and public authorities can benefit from our research and innovation on tailored solutions, access to our cutting-edge labs for experimentation and pilot testing, and specialized training to upskill and reskill their workforce in telecoms and smart network advancements. We also provide strategic consulting and startup mentoring, fostering innovation and growth. The planned CURIUM Capacity Building Services underpin all our offerings.

p-NET's strategy for growth and impact is comprehensive and multi-faceted. We're actively working to:

- Deepen our expertise in critical areas like cybersecurity and cyber-resilience.
- Significantly expand our experimental and testing capabilities for secure Beyond 5G and 6G systems.
- Drive collaborative research and innovation activities, specifically engaging with CURIUM partners to develop follow-up proposals and secure further R&I funding.
- Enrich our capacity-building efforts by creating new training content and designing and delivering webinars.
- Cultivate robust partnerships with strong potential for joint business development.

DSA

The Digital Security Authority (DSA) has designed and distributed a targeted questionnaire to gather insights from a wide spectrum of stakeholders - including manufacturers, importers, distributors, authorized representatives, national authorities, and end-users of products with digital elements. The analysis of the results will offer a comprehensive understanding of the practical challenges and knowledge gaps that organizations face in complying with the Cyber Resilience Act (CRA). These findings will be instrumental in developing actionable guidelines, recommendations, and educational materials to support broad CRA adoption, particularly among SMEs and micro-enterprises. To operationalize this strategy, the DSA will implement a multi-channel approach that includes workshops, training sessions, and awareness events, alongside digital communication tools such as newsletters. Additionally, the DSA plans to pilot funding support schemes to reduce the financial burden of CRA compliance. These efforts aim to improve CRA literacy, increase institutional readiness, foster stakeholder engagement, and contribute to a more secure and resilient digital product ecosystem across the EU.

AEGIS

AEGIS has developed a security assessment tool (TRL:7 at the start of the project) that will be further refined and validated within CURIUM, with the objective of reaching TRL:8 by the end of the project

timeline. The tool is designed to support organisations in identifying and mitigating vulnerabilities across IT infrastructure, web services, and user management systems.

During the project, the tool will be pilot tested with selected early adopters from various key sectors. The feedback gathered during pilot testing will be used to enhance the tool's detection accuracy, usability, and feature set. This phase will also serve to validate its functionality in real-world conditions and ensure it addresses current security needs. The insights gained through this process will directly inform the further development of the tool and its positioning in the cybersecurity market.

AEGIS will use the training materials co-developed in the project to offer targeted training and awareness sessions for customers and partners. This will support broader adoption of the tool and help organisations understand how to use it effectively within their security operations. Furthermore, the outcomes of CURIUM will be exploited to strengthen AEGIS's research and innovation efforts. In the long term, the tool will evolve to support advanced use cases, offering a scalable and effective security solution for medium to large enterprises seeking to enhance their cyber resilience.

NLG

Nealogic's goal is to improve the development of its software for operations services, data management and financial flows management to make them compliant with CRA regulations, using the tools developed by CURIUM.
The implementation of these tools will consist of new business opportunities in the ICT, manufacturing and Public Administration sectors, strengthening NeaLogic's positioning as a reliable technological partner for European regulatory compliance.

NCSA

NCSA intends to exploit and utilize the project's results, in further innovation and deployment activities other than those covered by the action concerned. This includes, among other things, research and knowledge exploitation efforts, such as supporting standardisation activities. To this end, the present plan includes revealing a compilation of already known initial exploitation strategies, including potential opportunities and guidelines driving project workflow to meet them promptly. Through its involvement in the CURIUM project, NCSA aims to expand its research activities and explore joint exploitation and innovation opportunities in cybersecurity.

As far as the NCSA individual exploitation plan is concerned, the National Authority already enhances a multidisciplinary set of cybersecurity competences and resources focusing mainly on the Regulatory Issues on Cybersecurity, Certification Processes and Standardization, as well as training, knowledge, as well as capacity building.

Focusing on this role, NCSA targets to increase the knowledge and know-how in designing a continuum that will offer impactful solutions and can help the implementation of the CRA and National strategies for securing digital assets inside the EU. Moreover, NCSA aims to gain knowledge from the contributions

on the definitions and processes of cybersecurity frameworks. In addition, through CURIUM, NCSA will gain expertise on CURIUM' services and end-solutions, through expanding our research activities and potential participation in R&I projects. Through our collaboration with CURIUM partners, we also focus on identifying joint exploitation opportunities and future synergies for R&I opportunities in the cybersecurity domain.

APIRO

APIRO has already developed a tool (TRL:7 at the start of the project) and will invest in developing it further and in launching and testing this tool within the CURIUM Continuum (reaching TRL:8 at the end of the project timeline). APIRO will gain useful insights on issues that could be remedied and improvements that could be implemented to make its use more effective and efficient. It is the plan of APIRO to further use this tool to support its customers in various compliance related consulting and testing activities. APIRO will use the training material jointly created by the project to provide training and awareness services to customers and other stakeholders. Finally, APIRO will exploit the outcomes, and the know-how gained from the CURIUM project to further advance research activities and support standardization efforts.

EIT DIGITAL

The overall objective is to enhance EIT Digital's educational and innovation ecosystem by integrating and validating CURIUM's capacity-building outputs and validated technologies into its digital transformation programs. We aim to extract value by scaling these resources to empower SMEs across Europe with cybersecurity competencies and CRA compliance, while strengthening our position as a leader in digital education and innovation. The value targets SMEs, academic partners, and policy makers seeking practical cybersecurity solutions, ultimately expanding EIT Digital's ecosystem by attracting new members through enhanced reputation and impactful offerings. EIT Digital aims at integrating and adapting CURIUM training materials into its Professional School curriculum to enhance existing cybersecurity courses or as part of a broader digital transformation program. It also aims to leverage validation results to inform policy recommendations for the European Commission and National Authorities on SME cybersecurity needs.

5. Collaboration and Standardisation

5.1 Networking and Clustering Plan

5.1.1 Introduction

The present section aims to provide a description of the planning and the framework of the CURIUM project with regards to the networking and clustering activities with sister projects as well as other partners, projects with similar interests and focus, and relevant initiatives. To fully cover the objectives of this dedicated Task 5.3, within the WP5, the comprehensive plan of core networking and broader collaboration activities is complemented with the definition of the assessment process that will evaluate the effectiveness and impact of these activities.

This Networking and Clustering Plan defines the project's targeted outreach strategy to directly involve specific stakeholders for networking, co-organisation of common actions and activities to align efforts to maximize impact. This part of the strategy includes identified stakeholders and initiatives, as well as other EU-funded projects by R&I programmes, especially those funded under the same or similar calls and relevant projects in the CURIUM thematics.

5.1.2 CURIUM Networking and Clustering objectives

Networking and clustering within the context of EU Projects involves related projects and initiatives with similar focus and inter-dependent research and D&C activities getting together in common actions, events, webinars, workshops or virtual meetings and share concepts, ideas, best practices, and challenges.

In this context, CURIUM 's objectives of the clustering activities focus on collaboration with other stakeholders and projects funded under the same project calls and other Horizon Europe related projects, Digital Europe projects and ECCC projects, as well as other projects and initiatives identified by the project partners, particularly national and regional ones, aligned to CURIUM goals and objectives.

Based on the CURIUM project's goals and related EU cybersecurity policy context, CURIUM project operates within a rapidly evolving digital landscape shaped by initiatives such as the EU Cybersecurity Act (EU CSA) and the Cyber Resilience Act (CRA). These regulations create new demands for compliance, resilience, and trust in digital products and services. Within this framework, networking and clustering activities serve the following core objectives:

1. Support the implementation of the CRA through coordinated dissemination of CURIUM tools, services, and compliance pathways among peer projects, stakeholders, and regulatory actors.
2. Foster knowledge exchange among EU-funded cybersecurity initiatives focusing on resilience, testing, and certification schemes.
3. Establish strategic alliances with key clusters in digital innovation, cybersecurity testing, and compliance, to amplify impact and speed up market uptake.
4. Enhance exploitation and sustainability through collaboration with SMEs, large enterprises, SDOs, regulators and national authorities[1].

5. Promote harmonization of cybersecurity compliance across Member States by engaging in policy dialogues, shared pilot evaluations, and collaborative events.

5.1.3 CURIUM Networking and Clustering Methodology

CURIUM's strategy is shaped by best practices and the experience of the consortium applying a structured, multi-stakeholder clustering model, focusing on the involvement of academia, research communities, industrial stakeholders, governmental bodies, and civil society communities to co-design cybersecurity resilience initiatives. These stakeholders collaborate closely in order to maximise the overall impact, through vertical integration and a collaborative approach with digital platforms, initiatives and ecosystems that represent common potential use cases for CURIUM's solutions.

In addition, networking aims to improve technical synergies, stakeholder engagement, and dissemination of project results, focusing on the strategic collaborations plan, described in Section 5.2, that follows.

More specifically, the project aims to liaise and engage with consultation and policy events involving policy makers and relevant Working Groups for closely monitoring and presenting its results. The project and its results will be also presented in open national and international networking events in order to boost reciprocal relationships between the stakeholders focusing on crucial advance training of digital skills.

As far as the typology of the clustering is concerned, CURIUM will use the following typologies for effective networking:

- common thematic activities on cybersecurity and resilience
- compliance-focused Horizon Europe and Digital Europe Programme projects,
- joint activities in certification readiness, security testing methodologies, and trustworthy-by-design tools
- policy clustering for the active and continuous interaction with EU and national cybersecurity regulators, ENISA, and CRA implementation taskforces,

Clustering activities involve direct outreach to project coordinators, involvement in EU forums, and use of platforms like the European Cluster Collaboration Platform or from other projects as well. Joint activities involve publication of papers, white papers, technical reports, co-organization and/or participation in joint workshops, webinars, standardization co-development meetings and workshops, and technical achievements.

The following Table will be used to collect relevant material and will be updated on a constant basis, along with the core KPIs of the D&C tool.

Table 0-8: Projects and Initiatives within the Focus of CURIUM

	Project/ Initiative	Scope & Description	Link	Forms of collaboration	Resp. Partner	Progress Made
	Phoeni2x	The project aims to design, develop and deliver a Cyber Resilience Framework providing Artificial Intelligence (AI) – assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange, tailored to the needs of Operators of Essential Services (OES) and of the EU Member State (MS) National Authorities entrusted with cybersecurity.	https://phoeni2x.eu/	NCSA is a project partner and can support the interaction between the 2 projects for either commonly organized events or for knowledge transfer between the 2 projects.	NCSA	
	SecAwarenessTruss	SecAwarenessTruss will deliver a customized federated cybersecurity range platform that will offer systematic and innovative training programs targeting Critical Infrastructure organisations to develop a skilled workforce for cyber defence and collaborative response. The project will include cross sector complex scenarios, gamification-based exercise and knowledge sharing capability aiming for hands-on and interactive learning facility.	https://secawarenesstruss.eu/	NCSA is a project partner and can support the interaction between the 2 projects for either commonly organized events or for knowledge transfer between the 2 projects.		
	EL-SOC	The project aims to deploy a national hub for sectoral SOCs. In particular, the project aims to develop EL-SOC's cyber threat detection and analysis capabilities by leveraging disruptive technologies to increase		NCSA is the project coordinator and can support the interaction between the 2 projects for either commonly organized events or		

		situational awareness and strengthen national-level capabilities.		for knowledge transfer between the 2 projects.		
	OCCTET	The OCCTET project (Open-Source Compliance Comprehensive Tools and Resources) is an EU-funded initiative aimed at improving cybersecurity and compliance with the Cyber Resilience Act (CRA) for Small and Medium Enterprises (SMEs).	https://occtet.eu/	The project's approach is very similar to CURIUM. It is based on Open-Source Tools. Exchange of best practices is considered mutually beneficial.		
	CADMUS	CADMUS aims to address the cybersecurity expertise shortage in Europe by developing targeted training opportunities based on approaches including cyber range projects, games, hackathons, bootcamps, and traineeships. These interventions aim to upskill educators, trainers, SME and startup employees, civil servants as well as graduate students who target cybersecurity careers through hands-on experiences and theoretical background building.	https://cadmus-project.eu/	NCSA is the project coordinator and can support the interaction between the 2 projects for either commonly organized events or for knowledge transfer between the 2 projects.		
	ATHENA	The project aims to deliver ATHENA, a europeAn THreat intelligence, rEspoNse and prepAredness platform, encompassing the national cybersecurity authorities of Cyprus, Greece, Bulgaria, and Malta. ATHENA will adopt a Cyber Security Operations Centers (CSOCs) Blueprint for cross border- cross-organizational, and cross-functional cooperation,		NCSA is a project partner and can support the interaction between the 2 projects for either commonly organized events or for knowledge transfer between the 2 projects.		

		collaboration, and coordination, and creating a model Coordinated Response Cluster for EU member states and other eligible entities.				
	AKADIMOS	The AKADIMOS project aims to support the creation and initial operation of the European Cybersecurity Skills Academy (henceforth "the Cyber Skills Academy" or "the Academy") which, as specified in the relevant EC Communication aims at a single point of entry that establishes synergies for cybersecurity training initiatives along with funding opportunities regarding the development of cybersecurity skills and thus contributing towards closing the skills gap of cybersecurity professionals across EU.		NCSA is the project coordinator and can support the interaction between the 2 projects for either commonly organized events or for knowledge transfer.		
	ERMIS	The project aims to deliver cyber security assurance and insurance as a service, by integrating mechanisms, services, and tools in an innovative marketplace platform. The marketplace will support the adoption of market-ready innovative cybersecurity solutions and tools to provide end-to-end support for cyber risk assessment, security certification, and cyber insurance processes.		NCSA is a project partner and can support the interaction between the 2 projects for either commonly organized events or for knowledge transfer.		
	GR-SME-SOC	GR-SME-SOC aims to create a sectoral SOC supporting the Greek SME community. It will operate independently,		NCSA is a project partner and can support the interaction		

		under the aegis of the Greek National Cyber Security Authority (NCSA). The consortium will contribute a rich set of easy-to-deploy, ready-to-use, and high-maturity tools for high performance real-time monitoring, threat detection, prediction and recommendations, as well as reporting, alerting and coordinated response capabilities.		between the 2 projects for either commonly organized events or for knowledge transfer.		
	CUSTODES	CUSTODES is a system comprised of a variety of components with the aim to provide trustworthy, cost effective, agile and portable conformity assessment capabilities, to a variety of interested parties, covering multiple Assurance levels of Composite ICT products or ICT services.	https://custodes-project.eu/	Common partners will ensure exchange of best practices, and collaboration on engagement, knowledge transfer and capacity building.	APSS, p-NET, EITD	
	SAND5G	SAND5G will deliver a risk and impact assessment platform for 5G to support 5G stakeholders secure their systems and services and National Authorities and MS Regulators overview the security status and applied measures that implement national cybersecurity strategies and legislation, in line with European 5G cybersecurity policies and EU toolbox for 5G security.	https://sand5g-project.eu/	Common partners will ensure exchange of best practices, and collaboration on engagement, knowledge transfer and capacity building.	NCSA, p-NET, SPH	

[1] The groups of focus include, but are not limited to, policy makers (national ministries, government officials, councils, EU, National, Regional and Local Authorities (NRLA), Regulatory Agencies, Standardisation Organisations such as ETSI, CEN, ISO), EU Institutions and agencies (e.g. DG CNECT, DG EMPL, ENISA, JRC, ECSO).

5.2 Strategic Collaborations Plan

The Strategic Collaboration Plan within the CURIUM project serves as a structured approach to identifying, engaging, and managing relationships with external stakeholders that can contribute to the project's success. It outlines the strategies and mechanisms the project will use to foster partnerships, encourage knowledge exchange, and create synergies with relevant organizations, networks, and initiatives to facilitate the effective implementation of the CRA and the uptake of the novel Compliance Continuum framework across Europe. The plan's objectives are to enhance the reach and relevance of project outcomes, ensure alignment with wider policy and regulatory frameworks, and support the long-term sustainability and adoption of results. It also establishes criteria for selecting collaborators and defines the types of joint activities that will maximize mutual benefit and collective impact.

5.2.1 Strategic Objectives of Collaboration

The main objectives of collaboration within the CURIUM project include:

- Knowledge exchange between research, industry, regulatory communities to foster innovation and improve understanding of cybersecurity and compliance challenges.
- Policy alignment to ensure that the novel Compliance Continuum framework reflects current CRA requirements and regulatory expectations.
- Technology adoption by promoting the use of the CURIUM services and tools among SMEs and micro-enterprises to enhance cybersecurity and simplify compliance processes.
- Market access and scaling through partnerships can facilitate the promotion and wider uptake of CURIUM solution across Europe.
- Enhanced impact through cross-sector synergies by connecting different stakeholder groups and promoting cooperation for shared cybersecurity objectives.
- Support alignment of CURIUM's tools and services with national CRA implementation roadmaps.
- Co-develop and deliver CRA-focused capacity building, training, and awareness activities.
- Ensure practical input into the novel Compliance Continuum from experienced regulatory and training actors.
- Establish feedback loops for continuous improvement (through advisory roles or co-validation activities).

5.2.2 Strategic Partners and Target Collaborators

The partners involved in the CURIUM project intend to establish contact with key working groups, including consortia from similarly themed projects, cybersecurity initiatives, European Commission institutions, and ENISA, to explore collaboration opportunities and identify ways to enhance the project's impact. CURIUM project aims to engage a diverse range of stakeholders including:

- Government
- Policymakers and regulators
- Industry companies
- NGOs (non-governmental organizations)

- Non-profit organizations
- SMEs
- Research and academic institutions
- Certification and Standardisation experts
- National and EU Regulators

An initial list of identified target collaborators include:

- Participants, project partners, and relevant stakeholders engaged in the following projects and initiatives related to cybersecurity digital skills.
  - Horizon EU/CEF/ENISA/
  - Erasmus+
  - COSME
  - DG EMPL
  - DGCNECT

The objective is to foster synergies and establish collaborations aimed at promoting project outcomes, co-organising events, and formulating an enhanced educational agenda that can be aligned to external agendas (e.g. the EU agenda).

5.2.3 Communication channels

Channels used during the project to communicate either with external or internal stakeholders include, but are not limited to:

External Communication Channels:

- The project's website
- Consortium partners' websites
- Consortium partners' social media channels (Twitter, Facebook, LinkedIn, etc.)
- Presentations at external events
- Meetings with targeted audiences (liaison or networking)
- Partners' events
- Partners' communication channels

Internal Communication Channels:

- Emails
- Meetings
- Workshops, seminars, and trainings
- Annual reports (e.g., KPI reports)
- Presentations at consortium partners' internal events and initiatives

5.2.4 Planned Collaboration Activities

The CURIUM project will promote collaboration through various mechanisms, including:

- Organization of joint workshops and events with external stakeholders to present project progress and gather feedback.
- Bilateral and multilateral meetings and Memoranda of Understanding (MoUs) to formalize collaborations with strategic partners.
- Co-authored publications and white papers to communicate project findings and recommendations.
- Shared dissemination and communication efforts to maximize visibility of the project's results through events, social media, and stakeholder networks.
- Exchange of technology or data where appropriate to support joint testing and validation activities and encourage real-world adoption of the CURIUM's novel compliance continuum platform.

- Input to Policymaking.

  The CURIUM project actively participated in the European Commission's public feedback exercise on the technical description of important and critical product categories listed in Annex III and IV of the Cyber Resilience Act (CRA). Given the project's relevance to the CRA and its development of tools to assist stakeholders in determining CRA scope, the consortium collaboratively submitted feedback. The input included technical suggestions aimed at clarifying product categorization criteria and ensuring alignment with practical implementation needs. The CURIUM team emphasized the importance of precision in defining critical product classes, particularly regarding the implications for conformity assessment under Article 32.

5.2.5 Monitoring and Evaluation

Progress in collaboration efforts will be tracked and measured against key performance indicators (KPIs), including:

- Number of trainings provided by CURIUM (external, from consortium members or developed inside the project)
- Number of scientific workshops organized by CURIUM project
- Number of information days organized by CURIUM project
- Number of CRA compliance use-cases and best practices
- Number of open-source components made available
- Number of jointly organized workshops
- Number of participants in each event attracted and registered as contacts
- Number of small and large-scale events participated by the end of the project
- Number of collaborations established with external organizations and initiatives.
- Joint activities conducted, including training, workshops, publications, and events.
- External uptake or impact of project outcomes, measured by stakeholder participation, feedback received, and application of CURIUM tools and services beyond the core consortium.

5.2.6 Market Impact and Sustainability of CURIUM project

Market Impact: The primary targeted users of CURIUM are European SMEs, particularly micro and small enterprises. However, the proposed solutions and planned activities of the project can support all industries to a certain extent and at the same time promote EU policies and regulations towards a more secure and resilient EU digital space. Inside this large ecosystem, CURIUM will actively pursue the creation of communication channels between the project partners, external industry stakeholders and EU organizations. It will organize meetings and workshops to demonstrate project innovations and actively receive valuable feedback that can help the consortium make necessary adjustments towards the development of solutions with significant societal and market impact. In addition, CURIUM will focus on identifying new business opportunities and facilitating business development between projects' partners and with external stakeholders, as well as establishing strategic collaborations to ensure the continued exploitation of project results after the project's conclusion.

Sustainability of CURIUM project:

The following are some of the collaboration activities between project partners and external stakeholders that can be undertaken to ensure the continued relevance and long-term sustainability of the CURIUM solution beyond the project's completion:

- participation of EIT in multiple EDIHs (European Digital Innovation Hubs) and the wider EU network of SMEs and startups.
- collaboration with ENISA and engagement with Cybersecurity Standardization activities.
- collaboration through the National Authorities with the European Cybersecurity Competence Centre (ECCC) and Network of National Coordination Centres (NCCs) which aims to increase Europe's cybersecurity capacities and competitiveness etc.

Furthermore, activities related to raising awareness and visibility are key factors to the success and long-term sustainability of CURIUM, as they will engage stakeholders and contribute to knowledge exchange between actors from different sectors (e.g., government, policymakers, academia, industry, companies, NGO's, etc.), maximizing its benefit to the European economy and society. They will aim to promote scientific excellence and innovation, explore and generate market demand for the technologies, products and services developed and strengthen their uptake, foster public awareness, engagement and understanding of science and technology energy-sustainability related, as well as draw the attention of national governments, policymakers, and regional authorities.

5.3 Standardisation Plan

5.3.1. What is standardisation?

A standard is a document that sets out the technical requirements of a product, service or process and its use. Standards are adopted by recognised standardisation bodies (such as ISO, CEN, CENELEC, ETSI, and many more). In these organisations, representatives from industry, research, governments and civil society, discuss and agree on what should be a standard. Once a standard is published, its use is normally voluntary but, in some cases, certain specific standards can be made mandatory by law. In other words, standards form a common language that allows researchers, people, public institutions

and industry to communicate, produce and commercialise products and services in a harmonised manner. This is especially important in the European single market.

Standards play an important role in the valorisation of research & innovation results[3]:

- They help researchers bring their innovation to the market and spread technological advances by making their results transparent. In spreading the diffusion of new technologies, standards provide both economic opportunities, facilitate the realisation of SDGs and give confidence to consumers that an innovative technology is safe. They codify the technology requirements and inform both manufacturers and consumers on what to expect.
- They allow technologies and materials to be interoperable: since a standard provides details on the use and content of a technology or a material, it is much easier to know when and how it can be used in combination with other technologies.
- In other words, by codifying information on the state of the art of a particular technology, standards enable dissemination of knowledge (both within and outside the relevant industry community). Moreover, standards bridge the gap between research and products or services allowing the diffusion of technology in the market and increasing the probabilities of its take-up. Standardisation facilitates the deployment of new technologies, interoperability between new products and services. Innovations can more easily gain market acceptance and consumer trust if they comply with existing standards for safety, quality, performance and sustainability.

5.3.2. The CURIUM standardization strategy

The CURIUM project has devised a stepped approach in relation to standardization. This approach comprises of the following steps, implemented from the beginning of the project to the end of the project duration.

- Identification of topics covered / related to the project
- Identification of standards that can be of use to the project as incoming knowledge or adopted and built upon and
- Identification of possible standardization efforts where the project could provide useful contribution.

RESULTS - Topics

During the first steps of the project implementation, the project team derived the main topic as follows:

- The CRA
- Cyber resilience
- Vulnerability management
- Vulnerability reporting
- Risk Assessment
- Cybersecurity measures
- Cybersecurity testing, evaluation and conformity assessment
- Training and capacity building

RESULTS - Standards

[3] https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/eu-valorisation-policy_en

To be able to identify the main standards related to the topics of the CURIUM project, the project first identified the key players related to European Standardization, as mentioned in Deliverable D2.1. :

- **CEN**: European Committee for Standardisation[4]
- **CENELEC**: European Committee for Electrotechnical Standardization[5]
- **ETSI**: European Telecommunications Standard Institute[6]
- **ISO**: International Organization for Standardization[7]
- **IEC**: International Electrotechnical Commission[8]
- **ITU**: International Telecommunication Union[9]

Additionally, and specifically for the parts related to risk assessment and risk treatment (proposal of cybersecurity controls) the following Standards Developing organizations are also relevant:

- **NIST[10, 11]**
- **MITRE CWE[12]**
- **MITRE CAPEC[13]**
- **MITRE ATT&CK[14]**
- **MITRE D3FEND[15]**
- **Open-Source Vulnerabilities (OSV)[16]**

Using existing resources on standardization (e.g. the draft standardization request[17], the Joint Analysis on the Cyber Resilience Act Requirements Standards Mapping by the Joint Research Centre and ENISA[18]) and the portals of the Standards Developing Organizations (SDOs), a list of relevant standards was devised. Examples of these standards are included in Tables 5-1 and 5-2 of deliverable D2.1 and are not repeated here.

This list (which is a live document of the project) contains more than 50 standards from the above-mentioned SDOs. The project partners shall take these standards into consideration and in case they are utilized in any way with the project implementation, relevant references will be provided in the respective deliverables.

Results – On-going standardization activities

[4] About CEN - CEN-CENELEC

[5] About CENELEC - CEN-CENELEC

[6] ETSI - Welcome to the World of Standards!

[7] ISO - International Organization for Standardization

[8] IEC homepage

[9] ITU: Committed to connecting the world

[10] https://nvd.nist.gov/search

[11] https://csrc.nist.gov/news/2014/nist-sp-800-53-on-line-database-updated-to-revisio

[12] https://cwe.mitre.org/

[13] https://capec.mitre.org/

[14] https://attack.mitre.org/

[15] https://d3fend.mitre.org/

[16] https://osv.dev/

[17] https://ec.europa.eu/docsroom/documents/58974

[18] https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

The project shall invest effort into providing feedback from the project results to relevant standardization activities. For this reason, relevant ongoing standardization efforts have been identified, are monitored, and feedback is being provided.

Within the first 6 months of the project lifetime, we are happy to report the following contributions to standardization activities:

CEN/CLC/JTC 13/WG 9 "Special Working Group on Cyber Resilience Act"

CEN/CLC/JTC 13/WG 9 "Special Working Group on Cyber Resilience Act" is a special working group created under CEN/CLC/JTC 13.

The purpose of the working group is to provide information and complement activities related to the Cyber Resilience Act (CRA).

APIRO and DSA, both partners of the CURIUM project, are active members of this working group and work on providing feedback on relevant requests and assignments.

Table 5-3 of D2.1 provides an overview of the current projects of the WG9.

ISO/IEC JTC 1/SC 27/WG1

The subject of WG1 of ISO/IEC JTC 1/SC 27 covers standards related to Information Security Management Systems.

APIRO, a partner of the CURIUM project, is a member of this working group and works on providing feedback on the relevant requests and assignments.

ETSI Cyber Security Technical Committee (TC CYBER)

ETSI TC CYBER is recognized as a major trusted centre of expertise offering market-driven cybersecurity standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. It works closely with stakeholders to develop standards that increase privacy and security for organizations and citizens across Europe and worldwide. TC CYBER is the most security-focused technical committee in ETSI, and has many strands of work. Its roadmap describes each of TC CYBER's key areas where standardisation can help on the journey to better security.

p-NET has been involved in ETSI's standardization activities and participated in some of its specification's groups e.g. ETSI ISG INS.

6. Conclusion

Deliverable D5.1 contributes to the accurate planning and effective execution of all necessary activities to achieve the identified impact maximization objectives. These objectives include implementing communication activities specifically tailored for diverse stakeholders, producing various promotional materials for the project's outputs, increasing awareness and attracting interested stakeholders and potential clients, and facilitating the continuous involvement of the broader community across all phases of the project. Key objectives for this plan also involve active participation in conferences, workshops, exhibitions, and courses, active monitoring and contributions to standards, alongside cultivating relationships with other framework projects and initiatives through networking and clustering activities.

The deliverable comprehensively outlines the strategy for disseminating the outcomes of CURIUM and details the various activities planned to enhance the project's visibility. It reports on activities already implemented and the impact achieved. The document defines the target audience along with their corresponding D&C channels. It also presents a collection of CURIUM promotional material that has been created and will undergo regular updates. This material is used to raise awareness and inform the public and various designated target audiences about the project and its ongoing developments. Additionally, it will be widely utilized by CURIUM partners whenever they give presentations at conferences, attend exhibitions, organize workshops, and engage in other relevant activities. The D&C Tool that has been created to meticulously record each partner’s contribution to the collective D&C activities is also presented. This information collector the comprehensive assembly of data and allow keeping track with the project’s commitments and KPIs. Partners are supplied with dissemination guidelines including reference to the European Commission’s Open Access policy. Additionally, partners are encouraged to showcase CURIUM at national or international events or conferences that may offer suitable platforms for presenting the project’s results.

The initial exploitation efforts undertaken are also presented, including a preliminary listing of Expected Results (ERs) of the project as perceived by the partners. For each ER, the IP and ownership status are defined. A Canvas-based methodology to perform Market and Value proposition analysis of each ER is proposed to be applied at full-scale in the following months. Partners’ individual exploitation plans are reported while joint exploitation plans remain to be discussed and defined. They will be reported in Deliverable D5.2.

The objectives and methodology for networking and clustering are defined together with a list of candidate projects which has been compiled according to the clustering methodology. The effort is driven by the aim of joining forces to minimize resource use, increase scale, and maximize impact. The framework for establishing strategic collaborations to achieve sustained impact is also outlined. It involves the identification of targeted collaborators, areas and means of collaboration, expected benefits and evaluation measures. In the first six months, the project has already engaged with standardization and has contributed to policymaking. Relevant standardization bodies and areas have been identified for the project to actively engage with, contribute to, monitor and/or ensure compliance with.

The reported activities will continue until the end of the project and updated achievements will be reported in Deliverable D5.2 - Final report on Dissemination, Exploitation, Standardisation & Sustainability, due in Month 18.

Annex I

Cra sUppoRt contInuUM

ERs Identification

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	D5.1 - Plan and early activities on Dissemination, Exploitation, Standardisation & Sustainability.		
Work Package	WP5		
Contractual due date	30.06.2025	**Actual submission date**	
Nature	R — Document, Questionnaire	**Dissemination Level**	PU - Public
Lead Beneficiary			
Responsible Author			
Contributions from			

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

1. Introduction to Exploitable Results

In accordance with EU definitions on project results and exploitation:

A **result** refers to any tangible or intangible output of the project — such as data, knowledge, methodologies, software, or services — generated during its implementation. These results may be subject to intellectual property rights and may have potential for further use beyond the scope and duration of the project.

An **Exploitable Result (ER)** is any result — whether technical, organisational, or knowledge-based — that can be used for additional value creation. This may include use in commercial offerings, service development, policy formulation, research activities, or standardisation initiatives.

A **Key Exploitable Result (KER)** is a result with particularly high potential for uptake, adoption, or impact. These are prioritised for detailed exploitation planning, including business modelling and potential protection.

As a first step in the exploitation planning process, all partners are invited to identify the Exploitable Results they are involved in — as owners, co-owners, or main contributors. One form should be completed per ER.

1.1. Basic Information

Partner / Owner	
Contact Information	
Name and description of the Exploitable Result	
Type of result (product, process, software, service, etc.)	
Main functionalities (Top 3–5 in bullets)	
Expected project month of first deliverable of ER (e.g., M12)	
Exploitation Path of ER (internal use, commercial, open source, etc.)	

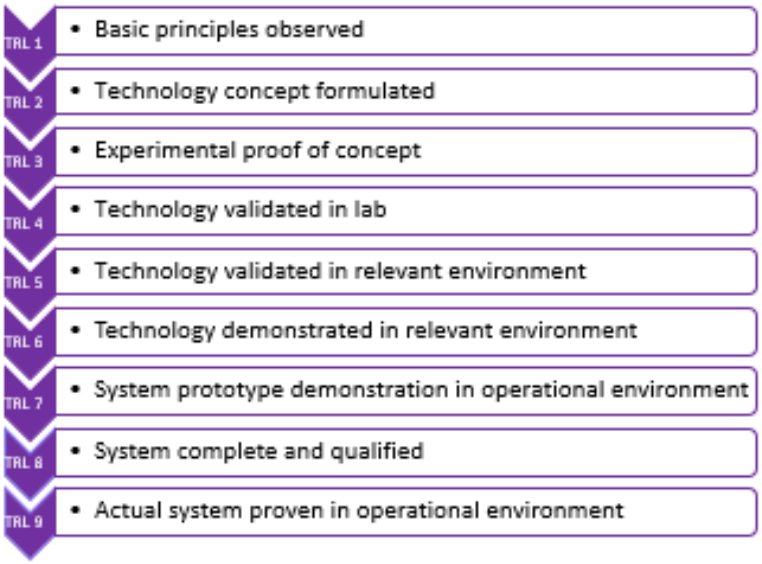
1.2. Assistance

Do you require help for promotion / dissemination / communication from WP5?

Do you need additional support from WP5 for Public relations or visibility, IP protection, Business model design, Licensing or legal advice?

1.3. Technical Maturity

Where a topic description refers to a TRL (Technology readiness levels), the following definitions apply, unless otherwise specified:



Note: The TRL scale is used to assess the technological maturity of software-based or tool-based results in the context of CURIUM. For non-technical outputs (e.g. process frameworks), alternative readiness scales may be used where relevant.

According to the above-mentioned definitions, please filled in the table below.

Technical maturity of the ER at the start of the project	
Current technical maturity of the ER	
Envisioned technical maturity of the ER at the end of the project	

1.4. Market demand or readiness level

What is the current contribution to or positioning in the market?

Which industrial sector does the ER target or is relevant with?

1.5. Value Proposition Canvas

The Value Proposition Canvas, developed by Dr Alexander Osterwalder, is a framework that helps ensure a strong fit between a solution and the market. It focuses on two key elements of a business model: the customer segments and the value propositions. In this context, it is used to identify the targeted customers for the ERs of the CURIUM project and to better understand their needs. Each ER may have its own canvas, or a single one may be developed for the main system/output of the CURIUM project.

The following figure shows the structure of the Value Proposition Canvas, which supports the alignment between customer needs and project outcomes.

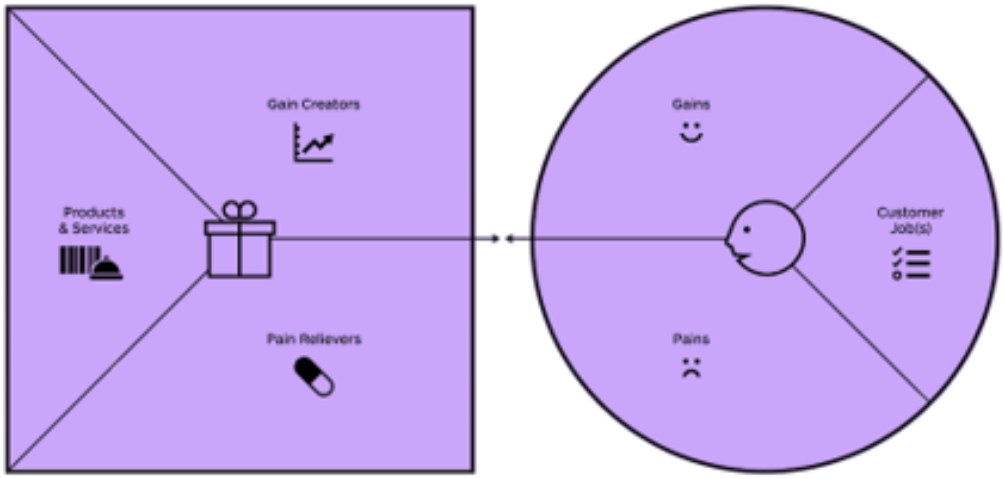


Figure 1 Value Proposition Canvas (adapted from Strategyzer)

1.5.1. Step 1: Scope

Indicate the scope of this analysis (e.g., ER description, entire solution):

1.5.2. Step 2: Customer Segment Analysis

1.5.2.1. Customer Jobs

Customer Jobs refer to the tasks that your target stakeholder (e.g. SME, consultant, public authority) is trying to accomplish. These may include:

- **Functional jobs**: understanding which CRA obligations apply, preparing compliance documentation, managing internal audits.
- **Social jobs**: gaining trust as a supplier, building a reputation for secure products, aligning with EU regulatory expectations.
- **Emotional jobs**: feeling confident in product security, reducing anxiety about regulatory non-compliance.
- **Basic needs**: ensuring communication with assessors, accessing reliable tools, having timely support for decisions.

Describe the tasks your target stakeholder (e.g. SME, public authority, consultant) is trying to accomplish in the context of CRA compliance. Include both operational activities and higher-level objectives they aim to fulfil. Consider the abovementioned categories.

-
-
-
-
-
-

1.5.2.2. Gains

Gains refer to all the positive outcomes that your target stakeholder expects, desires, or would be positively surprised by when using your solution. These may be functional, emotional, social, or strategic. Consider:

- What **improvements** would make their compliance process easier or faster? (e.g. reduced documentation time, automation of CRA mappings)
- What kind of **results** do they expect or value? (e.g. higher confidence in conformity, audit-readiness, completeness of evidence)
- What would exceed their **expectations**? (e.g. self-assessment support, modular use, integration into existing tools)
- What could **reduce** their **costs** or **effort**? (e.g. fewer external consultations, less staff time, clear processes)
- What increases the **credibility** or **reputation** of their organization? (e.g. better preparedness, CRA-aligned tools, support for national guidance)
- What makes the **adoption** of your **solution** easier? (e.g. intuitive interface, modular architecture, freemium option)

Describe the main expected or desired benefits of your targeted stakeholder when using this Exploitable Result. Consider both obvious and unexpected gains — functional, strategic, emotional, or reputational. You may list and rank them by relevance and frequency. Reflect on how your ER helps users save time or effort, reduce complexity, increase confidence, or improve their ability to comply with CRA requirements.

-
-
-
-
-
-
-
-

1.5.2.3. Pains

Pains refer to the negative experiences, obstacles, and risks that your target stakeholder faces in trying to achieve CRA compliance or support others in doing so. These may include technical limitations, lack of expertise, high effort or costs, unclear obligations, or fear of non-conformity.

Consider the following when identifying pains:

- What aspects of CRA compliance are difficult, time-consuming, or unclear?
- What current tools or processes are frustrating, slow, or insufficient?
- What are the main risks or fears (e.g. failing an audit, incomplete documentation, financial penalties)?
- What makes adoption or implementation of compliance solutions hard? (e.g. lack of staff, resistance, training needs)
- Are there emotional or reputational consequences of poor compliance or uncertainty?

List the challenges and obstacles that your stakeholder experiences when attempting to comply with CRA or support others in doing so. Consider functional, financial, technical, or psychological pains. Specify how severe and how frequent these pains are. This will help identify where your solution offers the most value.

-
-
-
-
-
-
-

1.5.3. Step 3: Value Proposition

1.5.3.1. Gain Creators

Gain creators describe how your Exploitable Result (ER) delivers value by enabling or amplifying the expected gains of your stakeholder. This can include functional, efficiency-related, reputational, or strategic advantages.

- Consider the following questions when describing your gain creators:
- Does your ER reduce the time or effort needed to assess CRA obligations?
- Does it improve the accuracy, consistency, or clarity of compliance documentation?
- Does it outperform existing manual or improvised processes?
- Does it help the stakeholder feel more confident or audit-ready?
- Does it support internal alignment and process repeatability?
- Does it increase the stakeholder's ability to demonstrate CRA conformity externally (e.g. to CABs, customers, authorities)?
- Does it make it easier to scale compliance across multiple products or teams?

Describe how your Exploitable Result creates value by enabling or increasing the gains your stakeholder expects. Focus on benefits such as increased efficiency, reduced compliance costs, better internal alignment, higher audit readiness, or improved usability compared to current practices. You may also explain how your ER helps users feel more confident, prepared, or credible in demonstrating CRA conformity.

-
-
-
-
-

1.5.3.2. Pain Relievers

Pain relievers describe how your Exploitable Result (ER) helps reduce or eliminate the obstacles, burdens, or risks faced by your stakeholder in their effort to comply with the CRA.

Consider the following questions:

- Does your ER simplify complex regulatory requirements or reduce misinterpretation risk?
- Does it reduce manual effort, redundant documentation, or duplicate assessments?
- Does it address skill or knowledge gaps in small teams?
- Does it help avoid typical errors in CRA conformity assessments?
- Does it lower financial or time-related costs for compliance?1.5.3.3 Products and Services

Describe how your ER alleviates the pains and challenges experienced by your stakeholder. Focus on how it reduces effort, risk, uncertainty, or complexity in the context of CRA compliance. Where possible, indicate which pains are most critical and how your ER specifically addresses them.

-
-
-
-
-
-

1.5.3.3. Products & Services

Products and Services refer to the concrete outputs you are offering through this ER. These can include tools, components, services, frameworks, guidelines, or data sets that support stakeholders in achieving CRA compliance or enabling others to do so.

Consider the following:

- What exactly is being delivered (e.g. software tool, training material, conformity mapping template)?
- Is the offering digital, physical, methodological, or advisory?
- Is it a standalone service or part of a larger support system?
- How frequently is it expected to be used (e.g. one-off, per product, recurring)?
- Who are the intended users or beneficiaries of the result?

List the specific deliverables associated with this ER and describe how each contributes to helping stakeholders achieve CRA-related goals. Clarify the form of each product or service (e.g. digital tool, method, training) and how central or recurring its use is expected to be.

-
-
-
-
-
-

Annex II

Cra sUppoRt contInuUM

D5.1 - Plan and early activities 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	D5.1 - Plan and early activities on Dissemination, Exploitation, Standardisation & Sustainability.		
Work Package	WP5		
Contractual due date	30.06.2025	**Actual submission date**	27.06.2025
Nature	R — Document, report	**Dissemination Level**	PU - Public
Lead Beneficiary	p-NET		
Responsible Author	Didoe Prevedourou		
Contributions from	All partners		

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

Co-funded by the European Union

ECCC

Individual Exploitation Design

This template is intended to collect input from each CURIUM partner regarding their individual exploitation intentions. Each partner is invited to complete this template for the Exploitable Results (ERs) they are primarily involved in. The information provided will support the definition of individual and joint exploitation strategies, the identification of Key Exploitable Results (KERs), and the alignment of exploitation planning with regulatory and market opportunities.

Partner / Owner	<Please specify the organisation and contact person responsible for this plan>
Relevant Exploitable Result(s)	<Please indicate which ER(s) this exploitation plan refers to>
Exploitation Goal	<Describe your overall objective regarding the use or commercialisation of the result. What value do you aim to extract from the result, and for whom?>
Exploitation Method	<Explain how you plan to exploit the result. For example, internal use, commercial offering, integration into services, licensing, policy use, training, open source dissemination, etc.>
Target Stakeholders or Customers	<Specify the target audiences, markets, or user groups you intend to reach. Include relevant sector(s), geography, or profile (e.g. SMEs, CABs, authorities)>
Short-Term Actions and Benefits (during project or soon after)	<What steps will you take in the next 6–12 months to support the use or adoption of the result? What are the expected benefits during this period?>
Long-Term Perspective	<Describe your long-term vision for the exploitation of the result. How will it be sustained or expanded after the project ends?>
IPR Status or Support Needs (optional)	<Do you foresee any IPR protection, licensing, or business support needs? Would you benefit from assistance in business planning, market analysis, or regulatory positioning?>