□

Cra sUppoRt contInuUM

CURIUM Compliance Continuum blueprint, knowledge capacity and validation plan

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	D2.2: CURIUM Compliance Continuum blueprint, knowledge capacity and validation plan		
Work Package	Work Package 2: Analysis of Requirements and Knowledge/Capacity building plan for CURIUM Compliance Continuum		
Contractual due date	30/06/2025	**Actual submission date**	30/06/2025
Type	R	**Dissemination Level**	PU
Lead Beneficiary	p-NET		
Responsible Author	P-NET		
Contributions from	All partners		

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
0.1	04.04.25	5	Initial Table of Contents and assignment of activities and sections to partners	p-NET, SPH
0.2	07.05.25	60	Initial contributions to sections	ALL
0.3	14.05.25	80	Second round of contributions	ALL
0.4	30.05.25	100	Final round of contributions and refinements	ALL
0.5	06.06.25	100	Ready for review (Reviewers' version)	p-NET
0.6	16.06.25	100	Internal Review	AEGIS, NLG
1.0	20.06.25	100	Review comments addressed	p-NET
1.1	30.06.25	100	Quality Assurance performed	CYS

Disclaimer

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

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

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

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

Copyright message

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 This Deliverable contains original unpublished work except where clearly indicated otherwise.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

Table of Contents

1. Executive Summary 7
2. Introduction 8
2.1. Mapping Deliverable Contents to Related CURIUM GA outputs 8
2.2. Deliverable Overview and Report Structure 9
3. End user's needs 10
3.1. Introduction 10
3.2. Survey results 10
3.2.1. Role of respondents within their organizations / entity 10
3.2.2. Existing knowledge of CRA 10
3.2.3. Existing knowledge and challenges for SMEs 12
3.2.4. Kind of support to understand and comply with CRA Requirements 21
3.2.5. Preference on type of training 22
3.2.6. Preferred host for training 24
4. State of the Art 25
4.1. Risk Assessment and Cyber Resilience 25
4.1.1. Risk Management Methodologies and Tools 26
4.1.2. AI enabled Cybersecurity Risk Management 28
4.2. Maturity Assessment for Controls 28
4.3. Maturity Assessment of Digital Products 32
4.4. Vulnerability Assessment and Penetration Testing 32
4.5. Relevant Research Projects 34
5. CURIUM Technical Tools and Services 36
5.1. Objectives of the Tools and Services 36
5.2. Tools-Specific Description 36
5.2.1. DPRA, Digital Product Risk Management / Risk Management Suite 36
5.2.2. CyReA, Cyber Resilience Assessment / Governance, Risk and Compliance tool 38
5.2.3. PSTVA, Penetration Self-Testing and Vulnerability Assessment Services and Tools 39
5.2.4. CAC, Conformity Assessment and Compliance Tool 41
5.2.5. DPMA, Digital Product Maturity Assessment service 43
5.3. Requirements 43
6. Knowledge and Capacity Services 61
6.1. Key pillars of the Capacity Building strategy 61
6.2. Capacity Building implementation plan 63
6.3. Expected Outcomes 65
7. CURIUM Compliance Continuum Blueprint Design 66
7.1. Systematic Guidance for CE Marking Compliance 66
7.2. The Blueprint Design 66

7.3. Open-Source Indicative Tools 68
8. CURIUM validation plan 73
8.1. Validation methodology 73
8.2. System validation 73
8.3. Performance monitoring 74
8.4. Time plan 75
8.5. Assessment methodologies for KPIs 76
9. Conclusions 78

Table of Figures

Figure 1: Knowledge level of CRA 12
Figure 2: Knowledge of CRA 13
Figure 3: Average value in challenges in organizational assessment / readiness 18
Figure 4: Average value in challenges in knowledge 19
Figure 5: Average value in challenges in access to tools 19
Figure 6: Average value in challenges in expert advice / support 20
Figure 7: Average value in challenges in funding / cost 20
Figure 8: Average value in challenges in training 21
Figure 9: Preferred Types of Support by Organization Type 22
Figure 10: Training Preferences by Organization/entity 23
Figure 11: Preferred host for training 24
Figure 12: Risk Management suite, High Level Architecture. 38
Figure 13: High Level Architecture of the Governance, Risk and Compliance tool 39
Figure 14: High Level Architecture of the Penetration Self-Testing and Vulnerability Assessment Module. 41
Figure 15: High Level Architecture of the CAC - Conformity Assessment and Compliance Module 42
Figure 16: Curium Continuum supporting the european SMEs and industry: preliminary schematic 67
Figure 17: Curium compliance Continuum Blueprint Design 67
Figure 18: Cyber-resilience conformity assessment borrowed from the eu-cra 68
Figure 19: Validation plan time line 75

List of Tables

Table 1: Adherence to CURIUM GA Deliverable & Tasks Descriptions 8
Table 2: Role within the organization 10
Table 3: Average values of all questions 12
Table 4: Average value in challenges 15
Table 5: Training Preferences 22
Table 6: PSTVA Vulnerability Identification and Prioritisation 41
Table 7: Curium Requirements 45
Table 8: Training Activity Catalogue Template 61
Table 9: Collaboration Table Template 63
Table 10: Indicative open-source tools with capability descriptions. 69
Table 11: System requirements template 74
Table 12: Performance Monitoring template 75
Table 13: performance monitoring of process KPIs 76

1. Executive Summary

Deliverable D2.2 “CURIUM Compliance Continuum blueprint, knowledge capacity and validation plan” aims to exhibit the tools and services deployed under CURIUM along with their technical, functional and non-functional requirements.

It also provides a comprehensive analysis of end-user needs, additional to what was reported in D2.1. Moreover, state-of-the-art risk assessment practices, and stakeholder input are outlined, showcasing a modular ecosystem that supports conformity assessment, documentation, vulnerability management, and audit readiness.

This report also provides details about the project’s knowledge and capacity-building strategy to enhance SMEs’ cybersecurity competence. By focusing on training, consulting, and awareness, CURIUM empowers European SMEs, particularly micro and small enterprises, to build cybersecurity competence and confidently pursue certification.

Additionally, it describes the blueprint design for the CURIUM compliance continuum, which consists of the modular interplay of all the CURIUM tools and services. By integrating five technical tools within a centralised user interface and supporting them with capacity-building resources, the Continuum enables systematic risk-based self-assessment, vulnerability management, and regulatory alignment for digital products.

Finally, it introduces the validation plan, which incorporates agile, user-driven testing cycles to ensure its tools meet cybersecurity needs and CRA compliance by leveraging stakeholder engagement, agile validation cycles, and iterative feedback.

This document is linked to milestones MS4 & MS5 and tasks T2.2, T2.3 & T2.4.

2. Introduction

2.1. Mapping Deliverable Contents to Related CURIUM GA outputs

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

TABLE 1: ADHERENCE TO CURIUM GA DELIVERABLE & TASKS DESCRIPTIONS

CURIUM GA Component Title	CURIUM GA Component Outline	Related Objectives
TASKS		
Task 2.2	*End users' requirements including regulatory aspects* *This task focuses on collection of the end-users' requirements taking into consideration technical, operational, regulatory, legal etc. aspects of end users, with a special focus on SMEs and micro enterprises. It will also examine relevant processes, guidelines and responsibilities for all stakeholders to ensure that proposed solutions address the targeted clients' needs and are aligned with EU and national policies and/or regulatory obligations.*	*O2.2. Definition of data flow for the architecture operations taking into consideration relevant legal and ethical aspects.* *O2.3. Detailed description of end users' requirements, with a focus on SMEs and micro enterprises.*
Task 2.3	*CURIUM Compliance Continuum design and technical specifications* *This task will create the reference blueprint of CURIUM including a) the basic technical components for supporting the services, b) the security tools and solutions needed for performing activities like security testing etc. and c) the knowledge and capacity services. The architecture will be designed to be model-driven and modular (dynamically inserting services and security tools) flexible for allowing integration additional sources, and interoperable for connecting with possible external systems. It will also include open APIs and data representations aligned with existing interoperability standards and accessible User Interfaces which follow the principles for usable, inclusive, intuitive, also considering their diverse backgrounds of its users.*	*O2.5. Detailed design and technical specifications for the "blueprint" of the CURIUM Compliance Continuum.*
Task 2.4	*CURIUM knowledge, and capacity building and validation plan* *Inside the context of this task, CURIUM will formulate the plan for knowledge and capacity building for CRA, as well the Cybersecurity Act and other relevant EU policies for the security and digital transformation of EU. It will identify key stakeholders and users, and define processes and tools for skills' upscaling, training and awareness, mentoring, partnership/cooperation building at different levels (technical, administrative, operational etc.) etc. In this task the validation plan with its concrete phases will also be*	*O2.4. Definition of the knowledge and capacity building plan that will drive these activities throughout the duration of the project.*

	defined to allow for fast engagement, solutions' releases and feedback collection.	

DELIVERABLE

D2.2. CURIUM Compliance Continuum blueprint, knowledge capacity and validation plan.

This deliverable will provide the technical, functional and operational requirements and the final design for the CURIUM Compliance Continuum. It will also describe the plan for validation and also capacity and knowledge building. This deliverable will reflect the outcomes of T2.2, T2.3 and T2.4.

2.2. Deliverable Overview and Report Structure

This deliverable aims to complement D2.1 on End User's needs, showcasing all the CURIUM tools and services along with their requirements. It also provides the reference blueprint of the project, the validation plan and the plan for knowledge and capacity building.

It is structured as follows:

Section 1: Executive summary of the document.

Section 2: Serves as a link between the GA and this document and showcases its overview.

Section 3: Showcases survey results, complementary to D2.1 inputs.

Section 4: Provides state-of-the-art information on risk assessment methodologies, maturity assessments of controls and digital products, vulnerability assessments and penetration testing and relevant research projects.

Section 5: Outlines the tools and services of the project and their respective requirements, structured as technical, functional and non-functional.

Section 6: Describes the capacity building strategy, its implementation plan and the expected outcomes of the operation.

Section 7: Presents the blueprint design of the project and some open-source indicative tools.

Section 8: Describes the validation plan, consisting of the evaluation methodology to be used, a time plan and an initial assessment of the project's KPIs.

Section 9: Concluded the document.

3. End user's needs

3.1. Introduction

The primary objective of the survey was to gain a deep understanding of stakeholders' needs, challenges and expectations in order to equip them with the necessary tools and services for conducting effective self-assessment processes or preparing their products with digital elements for third-party assessments. These tools seek to reduce costs and time required for certification while ensuring compliance with the obligations set out by the Cyber Resilience Act (CRA).

To achieve this, the CURIUM partners developed a structured survey aimed at capturing diverse perspectives and practical insights from stakeholders. The survey was organized into four key sections: Demographics, Existing Knowledge of the CRA, Challenges, and Offerings, a total of 27 questions. These sections aimed to collect comprehensive data from a wide range of stakeholders across various industry sectors and EU Member States. The ultimate goal was to ensure that the findings collected accurately reflect the realities and expectations of different organizational profiles, thereby guiding the development of targeted compliance and capacity-building solutions under the CURIUM Compliance Continuum.

As mentioned in **Deliverable D2.1 – CRA and EU Certification Analysis Towards a European Trustworthy Certified Digital Valley, Section 7.3**., the stakeholder questionnaire was conducted via the EU Survey platform and collected 91 completed responses from a broad range of participants, including manufacturers, developers, regulators, national authorities, and academic institutions.

This section focuses only on the additional results and insights, not previously reported in **Deliverable 2.1**.

3.2. Survey results

3.2.1. Role of respondents within their organizations / entity

TABLE 2 below presents the distribution of respondents based on their role within their respective organizations.

TABLE 2: ROLE WITHIN THE ORGANIZATION

Role	Total Number
Management (Non - IT/ IS)	11/ 91
Management (IT/IS)	34/ 91
Member of the IT / IS team	12/ 91
Member of the product design / development / implementation team	13/ 91
Compliance Officer	2/ 91
Member of a Regulatory Authority / National or European Institution, Agency or Body	2/ 91
Member of an Academic Institution	6/ 91
Other	13/ 91

3.2.2. Existing knowledge of CRA

While the distribution of CRA knowledge levels among respondents was presented in **Deliverable D2.1 - Section 7.3. – Figure 1**, this section provides a brief explanation of the weighted scoring methodology used to derive those results.

The assessment is based on seven structured questions covering core CRA concepts, including product classification, cybersecurity obligations, and conformity assessment procedures.

To derive the overall knowledge level of each respondent, a weighted scoring system was applied to their answers across seven key questions related to the CRA. Each response option was assigned a numerical value reflecting the depth of understanding, as follows:

- "I don't know anything about it" – **0 points**
- "I have heard of it, but would need effort or help to know its details" – **1 point**
- "I have read it and have understood the main concepts" – **2 points**
- "I have a deep understanding of the subject and, if needed, I can support/guide others" – **3 points**

For each respondent, the weighted scores from all seven questions were added together to calculate a **Sum of Weighted Score**. This score was then normalized to a percentage using the following formula:

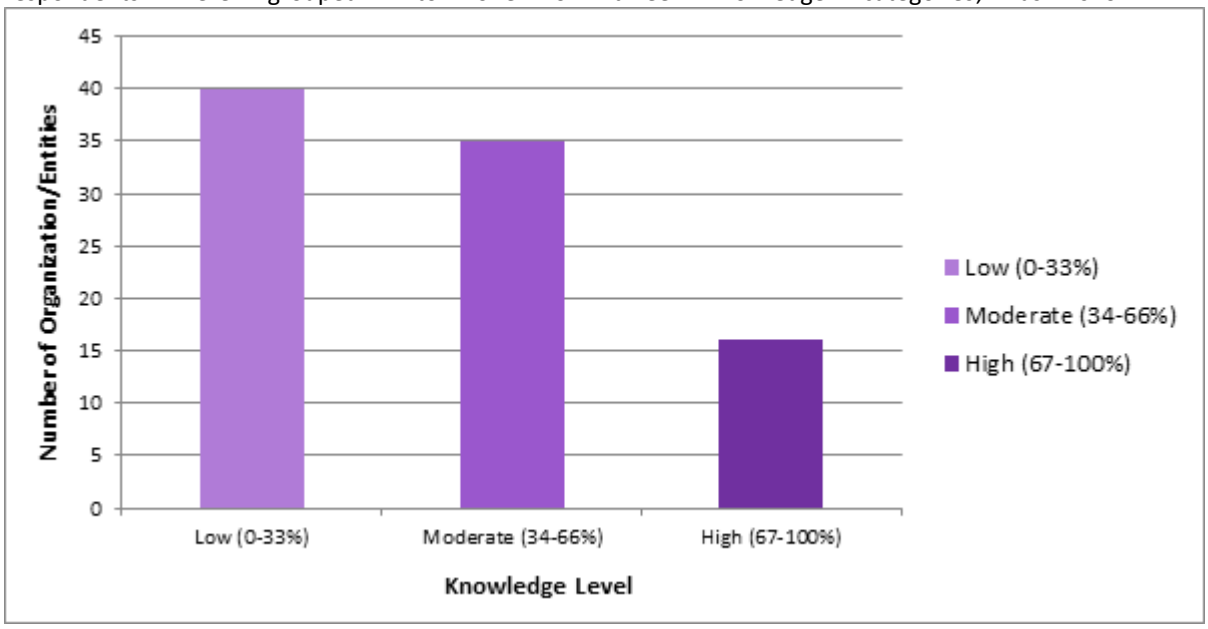
= (Sum of Weighted Score /Total Max Weighted Score) × 100%

where,

Sum of Weighted Score: This is the total number of points a respondent earned by summing the weight values of their selected answers across all questions.

Total Max Weighted Score: This is the maximum possible score a respondent could achieve if they selected the answer with the maximum weight (3 points) for every question. For all seven (7) questions, this total is 21 points.

This gave each respondent a CRA Knowledge Score expressed as a percentage. Based on this final score, respondents were grouped into one of three knowledge categories, as shown in **Figure** 1 below.



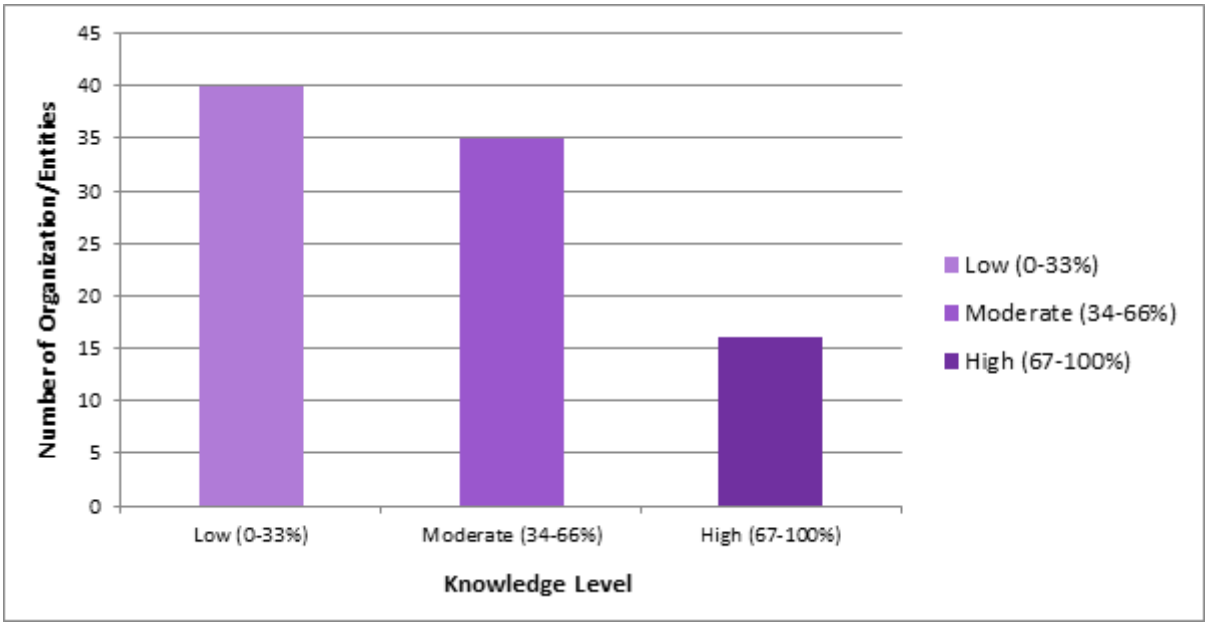


FIGURE 1: KNOWLEDGE LEVEL OF CRA

3.2.3. Existing knowledge and challenges for SMEs

From total 91 responses collected through the questionnaire, 46 belonged to SMEs, following the European Union definition[1]. Almost half of these responses belonged to SMEs identifying as Manufacturers / Developers of products with digital elements (22) and over 75% (36) belonged to the entities identified within the CRA as Economic Operators[2]. This section provides an overview of the responses and conclusions extracted from the questionnaire, for the SMEs and in comparison, to large organizations and public bodies.

Table 3 displays the average values for each question relating to knowledge:

TABLE 3: AVERAGE VALUES OF ALL QUESTIONS

Topic	Average value for SMEs – Economic Operators[3]		Average value for large enterprises
I know what is the **Scope and Requirements** of the Cyber Resilience Act (CRA)	5 – 0 14 – 1 16 – 2	1.31	1.56
I know the **definition** and can distinguish between products with **digital elements**	6 – 0 9 – 1 17 – 2 3 – 3	1.49	1.56

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

[2] Definition 12, Article 2, CRA: 'economic operator' means the manufacturer, the authorised representative, the importer, the distributor, or other natural or legal person who is subject to obligations in relation to the manufacture of products with digital elements or to the making available of products with digital elements on the market in accordance with this Regulation; More information on economic operators in D2.1.

[3] https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en

I know the **exceptions** to the application of the CRA	15 – 0 10 – 1 9 – 2 1 – 3	0.89	1.22
I know about the **classification** of products under the CRA and can assign products to the different classes	15 – 0 11 – 1 8 – 2 1 – 3	0.86	1.22
I understand the concept and details of the **essential cybersecurity requirements** mandated for products with digital elements	7 – 0 11 – 1 12 – 2 5 – 3	1.43	1.56
I understand the concept and details of **conformity assessment options** for a product with digital elements	8 – 0 13 – 1 13 – 2 1 – 3	1.20	1.28
I understand the concept and know of the contents of the **technical documentation** for a product with digital elements according to the CRA	12 – 0 14 – 1 9 – 2	0.91	1.28

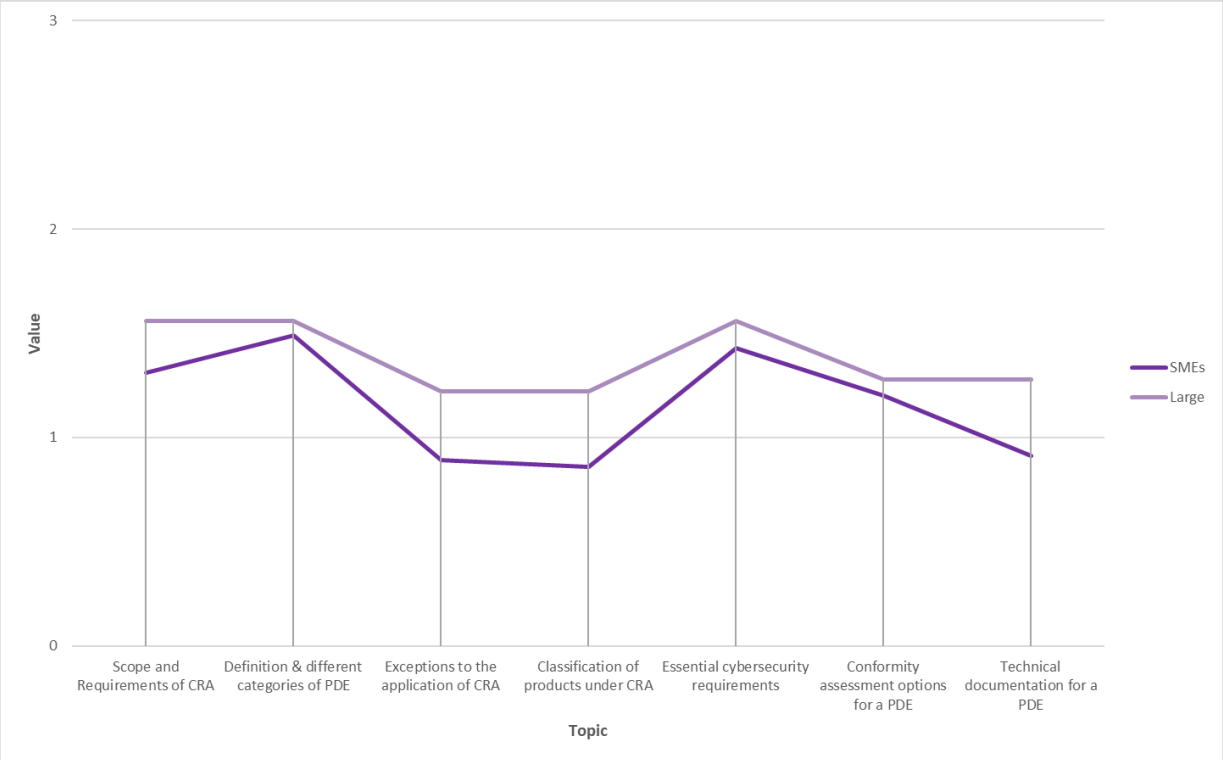


FIGURE 2: KNOWLEDGE OF CRA

Figure 2 above presents the extracted values (average values), indicating that:

- The professed knowledge on the topics presented within the questionnaire follow a similar trend between SMEs and Large enterprises.
- The knowledge of "**classification** of products under the CRA and can assign products to the different classes", "the **exceptions** to the application of the CRA" and "the concept and know of the contents of

the technical documentation for a product with digital elements according to the CRA" are the lowest ranking ones in all types of enterprises. The average value for SMEs on all questions is slightly less than 1.00, indicating that it is a bit less than "I have heard of it, but would need effort or help to know its details".

- For all types of enterprises, the maximum average value is 1.5, which is between "I have heard of it, but would need effort or help to know its details" and "I have read it and have understood the main concepts".

Table 4 displays the average values for each question relating to the challenges:

TABLE 4: AVERAGE VALUE IN CHALLENGES

Topic	Category	Average value for SMEs – Economic Operators[4]		Average value - large enterprises
We do not know whether our company **currently develops or sells "product(s) with digital elements"**	Organizational assessment / readiness	Strongly disagree – 21 Disagree – 6 Neither agree nor disagree – 3 Agree – 5 Strongly agree – 14	-0.69	-1.05
We do not **know if our organization is in scope of the CRA**	Organizational assessment / readiness	Strongly disagree – 9 Disagree – 6 Neither agree nor disagree – 11 Agree – 6 Strongly agree – 10	0.05	0.22
We do not know which are the **essential requirements** that the product with digital elements needs to comply with	Organizational assessment / readiness	Strongly disagree – 3 Disagree – 12 Neither agree nor disagree – 7 Agree – 11 Strongly agree – 9	0.26	0.28
We do not know how to construct the **technical documentation** of the product with digital elements	Organizational assessment / readiness	Strongly disagree – 3 Disagree – 11 Neither agree nor disagree – 7 Agree – 10 Strongly agree – 11	0.36	0.33
We have not **assessed** whether our "product with digital elements" complies **with CRA's security-by-design principles".**	Organizational assessment / readiness	Strongly disagree – 2 Disagree – 4 Neither agree nor disagree – 9 Agree – 16 Strongly agree – 11	0.71	0.94
We have **limited knowledge of the CRA scope and requirements**	Knowledge	Strongly disagree – 4 Disagree – 7 Neither agree nor disagree – 8 Agree – 12 Strongly agree – 22	0.45	0.06
We do not know which are the actual / **practical requirements of the CRA**	Knowledge	Strongly disagree – 3 Disagree – 8 Neither agree nor disagree – 9 Agree – 12 Strongly agree – 10	0.43	0.28

[4] The scoring system used here is the same as the one presented in the previous section.

We do not have an **understanding** what an EU declaration of conformity is and how this could be extracted	Knowledge	Strongly disagree – 3 Disagree – 9 Neither agree nor disagree – 12 Agree – 7 Strongly agree – 11	0.33	0.22
Topic	**Category**	**Average value for SMEs – Economic Operators**		**Average value - large enterprises**
We do not know which options exist in relation to the **conformity assessment** of products with digital elements	Knowledge	Strongly disagree – 3 Disagree – 8 Neither agree nor disagree – 10 Agree – 12 Strongly agree – 9	0.38	0.39
We do not have **access to tools** which would assist us in the **risk assessment process**	Access to tools	Strongly disagree – 6 Disagree – 6 Neither agree nor disagree – 11 Agree – 7 Strongly agree – 12	0.31	0.44
We do not have **access to tools** which would assist us in the **identification of our exposure to risk**	Access to tools	Strongly disagree – 6 Disagree – 8 Neither agree nor disagree – 9 Agree – 7 Strongly agree – 12	0.26	-0.61
We do not have **access to tools** to perform **vulnerability analysis**	Access to tools	Strongly disagree – 8 Disagree – 9 Neither agree nor disagree – 11 Agree – 7 Strongly agree – 7	-0.10	-0.83
We do not have **access to tools** to perform **penetration tests**	Access to tools	Strongly disagree – 7 Disagree – 9 Neither agree nor disagree – 11 Agree – 6 Strongly agree – 9	0.02	-0.89
We find it very difficult to **locate / get expert advice or direction on CRA compliance**	Expert advice / support	Strongly disagree – 5 Disagree – 6 Neither agree nor disagree – 11 Agree – 10 Strongly agree – 10	0.33	0.50
Preparing for CRA compliance requires **expert knowledge**	Expert advice / support	Strongly disagree – 1 Disagree – 2 Neither agree nor disagree – 7 Agree – 16 Strongly agree – 16	1.05	1.06

There is **limited or no funding available** to us, to prepare for CRA compliance	Funding / cost	Strongly disagree – 1 Disagree – 6 Neither agree nor disagree – 13 Agree – 8 Strongly agree – 14	0.67	0.44
The **tools** provided by different organizations, are **very costly**	Funding / cost	Strongly disagree – 1 Disagree – 1 Neither agree nor disagree – 24 Agree – 12 Strongly agree – 4	0.41	0.39
We do not know of any **training** / capacity building activity that **focuses on the CRA**	Training	Strongly disagree – 4 Disagree – 8 Neither agree nor disagree – 6 Agree – 15 Strongly agree – 9	0.41	0.56
I have **never participated in any training activities regarding the CRA**	Training	Strongly disagree – 1 Disagree – 6 Neither agree nor disagree – 2 Agree – 10 Strongly agree – 23	1.14	0.83

Figure 3 shows the average value of the responses of SMEs and large enterprises in challenges in the category: Organizational assessment / readiness

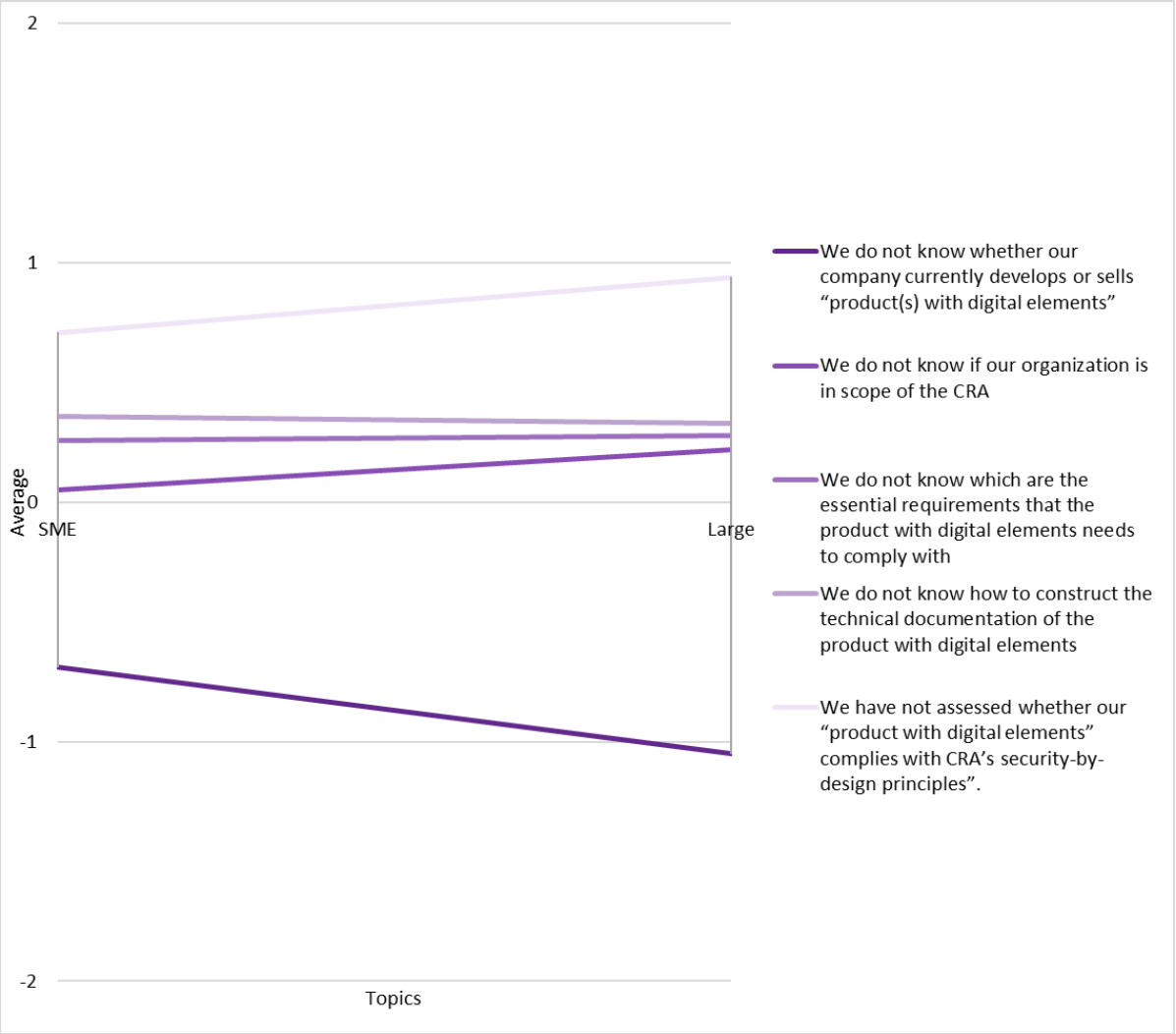


FIGURE 3: AVERAGE VALUE IN CHALLENGES IN ORGANIZATIONAL ASSESSMENT / READINESS

Figure 4 shows the average value of the responses of SMEs and large enterprises in challenges in the category: Knowledge.

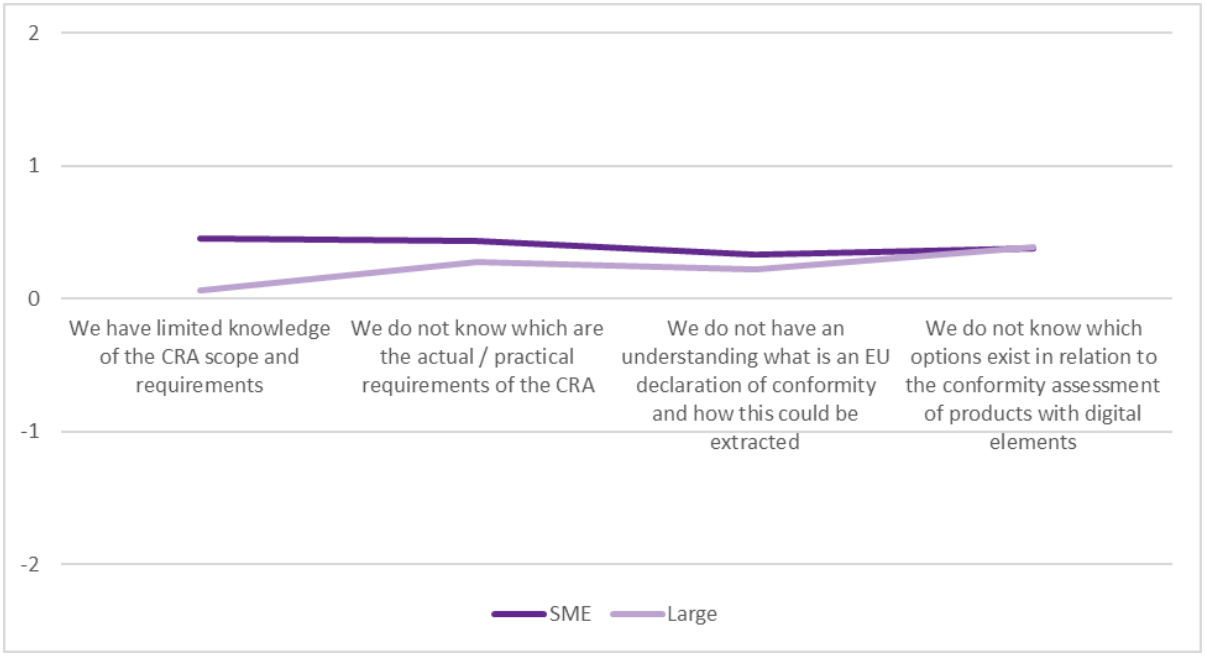


FIGURE 4: AVERAGE VALUE IN CHALLENGES IN KNOWLEDGE

Figure 5 shows the average value of the responses of SMEs and large enterprises in challenges in the category: Access to tools

.

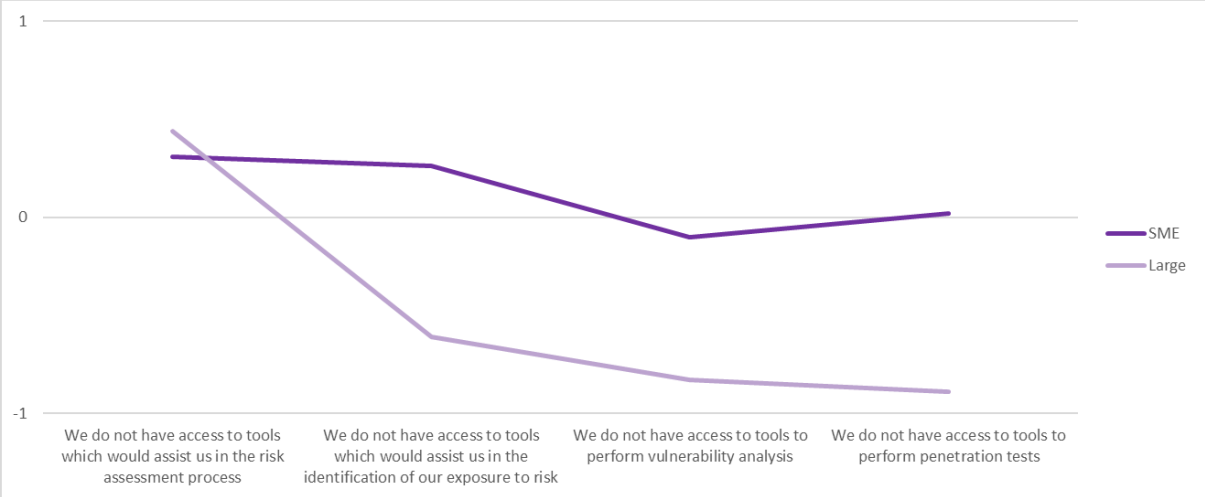


FIGURE 5: AVERAGE VALUE IN CHALLENGES IN ACCESS TO TOOLS

Figure 6 shows the average value of the responses of SMEs and large enterprises in challenges in the category: Expert advice / Support

FIGURE 6: AVERAGE VALUE IN CHALLENGES IN EXPERT ADVICE / SUPPORT

Figure 7 shows the average value of the responses of SMEs and large enterprises in challenges in the category: Funding / Cost.

FIGURE 7: AVERAGE VALUE IN CHALLENGES IN FUNDING / COST

Figure 8 shows the average value of the responses of SMEs and large enterprises in challenges in the category: Training.

FIGURE 8: AVERAGE VALUE IN CHALLENGES IN TRAINING

The extracted values (average values) indicate that:

- There are variations related to the challenges faced between SMEs and large enterprises.
- The greatest differences in opinion between SMEs and large enterprises (in absolute numbers) are presented in the question regarding access to tools. Specifically, SMEs neither agree not disagree (average value 0) with the statement "We do not have access to tools to perform penetration tests" whereas large enterprises disagree (average value -0.9).
- Both SMEs and large enterprises agree that they have never participated in any training activities regarding the CRA. The average value for SMEs is greater than that of large enterprises.
- Both SMEs and large enterprises agree that preparing for CRA compliance requires experts' knowledge.
- The only challenge that the SMEs are not in agreement (almost -0.7) is "We do not know whether our company currently develops or sells "product(s) with digital elements", indicating that they can identify that their organization currently develops or sells "product(s) with digital elements" or not.
- On the other hand, the large enterprises, disagree on the following: "We do not know whether our company currently develops or sells "product(s) with digital elements"", "We do not have access to tools to perform penetration tests", "We do not have access to tools to perform vulnerability analysis", "We do not have access to tools which would assist us in the identification of our exposure to risk". Indicating that some knowledge and access to tools regarding risk assessment, vulnerability assessments and penetration tests exists for large enterprises although, they have not "whether our "product with digital elements" complies with CRA's security-by-design principles" or know of the requirements regarding conformity assessment.
- Regarding cost and availability of funding, the responses do not provide a very clear picture. The trend is towards agreement (that there is a high cost to the tools and that funding is limited) but the average values are between 0.67 and 0.39.

3.2.4. Kind of support to understand and comply with CRA Requirements

Further analysis to Table 72 in **Deliverable D2.1 – CRA and EU Certification Analysis Towards a European Trustworthy Certified Digital Valley, Section 7.3,** was conducted, as shown in **Figure 9** below, to explore correlations between the types of organizations and their preferred forms of support. Manufacturers and developers consistently demonstrated the highest need across all categories, particularly for training, technical

assistance, tools, and consulting—reflecting their direct compliance responsibilities. Government and regulatory bodies prioritized training, policy guidance, and implementation tools, underlining their interpretive and supervisory role. The academic community showed a balanced demand across training, guidance, and tools, highlighting their dual focus on knowledge and capacity-building. End users leaned toward practical support such as technical assistance and consulting, while intermediaries (e.g. distributors, representatives) expressed lower but still diverse needs. These trends affirm the importance of delivering tailored support within the CURIUM Compliance Continuum, ensuring alignment with each stakeholder group's operational context and compliance challenges.

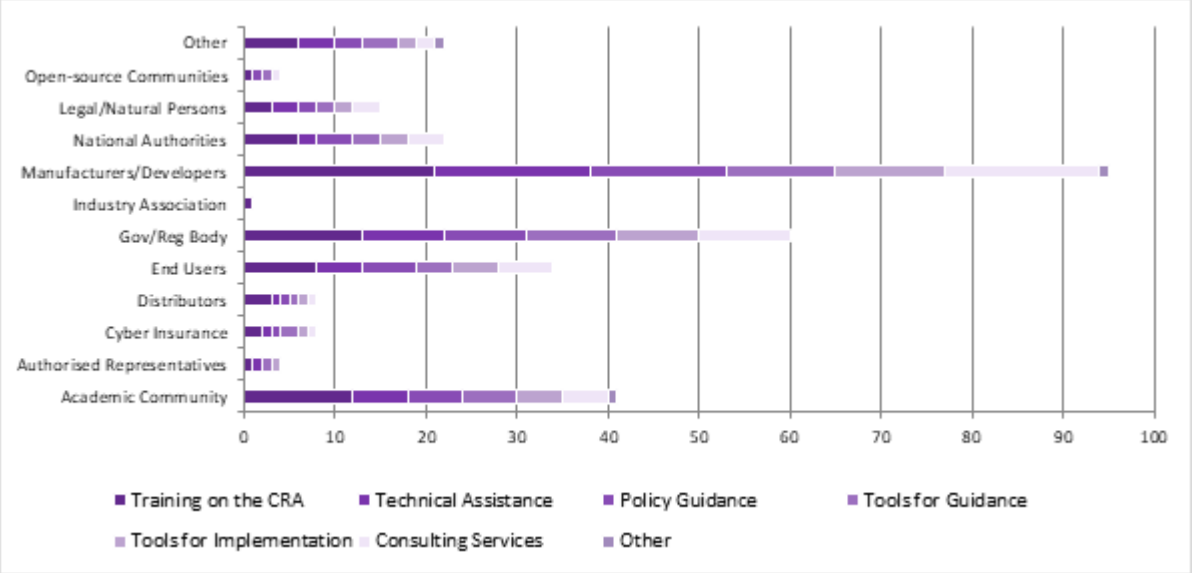


FIGURE 9: PREFERRED TYPES OF SUPPORT BY ORGANIZATION TYPE

3.2.5. Preference on type of training

Table 5 below summarizes the overall training preferences across all respondents and reveals clear trends in the types of learning formats considered most useful for supporting CRA compliance. Hands-on workshops using a testing environment received the highest level of interest, with 57 participants indicating this as a preferred option. This underscores a strong stakeholder demand for practical, experiential learning that allows direct engagement with real-world scenarios. Self-assessment guides and documentation (48 "Yes" responses) and live online courses (47) also emerged as widely favoured, reflecting a desire for both structured, instructor-led sessions and flexible reference materials that support self-directed learning. While self-paced online courses garnered moderate interest (43), they were slightly less popular, possibly due to the lack of real-time interaction. Notably, one-to-one advisory sessions received the lowest number of positive responses (29), suggesting that while tailored support has its place, most stakeholders prefer training formats that can be accessed more broadly or replicated at scale. Overall, the data highlights the importance of combining interactive, hands-on learning with flexible, accessible resources to effectively meet the diverse training needs of the CURIUM Compliance Continuum's target audience.

TABLE 5: TRAINING PREFERENCES

Training Preferences	Yes	No
Hands-on workshops using a testing environment	57	34
Live online courses	47	44
Self-paced online courses	43	48
One-to-one advisory sessions	29	62
Self-assessment guides and documentation	48	43

These training preferences were then analysed based on the type of organization / entity. As shown in **Figure 10** below, the results demonstrate that different organizational types favour distinct training approaches, reflecting their unique operational needs and levels of CRA familiarity.

Manufacturers and developers of products with digital elements represent the most active respondent group, with a strong preference for one-to-one advisory sessions and hands-on workshops using a testing environment, followed closely by live online courses. This indicates a pronounced need for personalized, practical guidance to support implementation efforts and navigate compliance complexities. The demand for direct support is consistent with the hands-on responsibilities these stakeholders hold in ensuring product conformity.

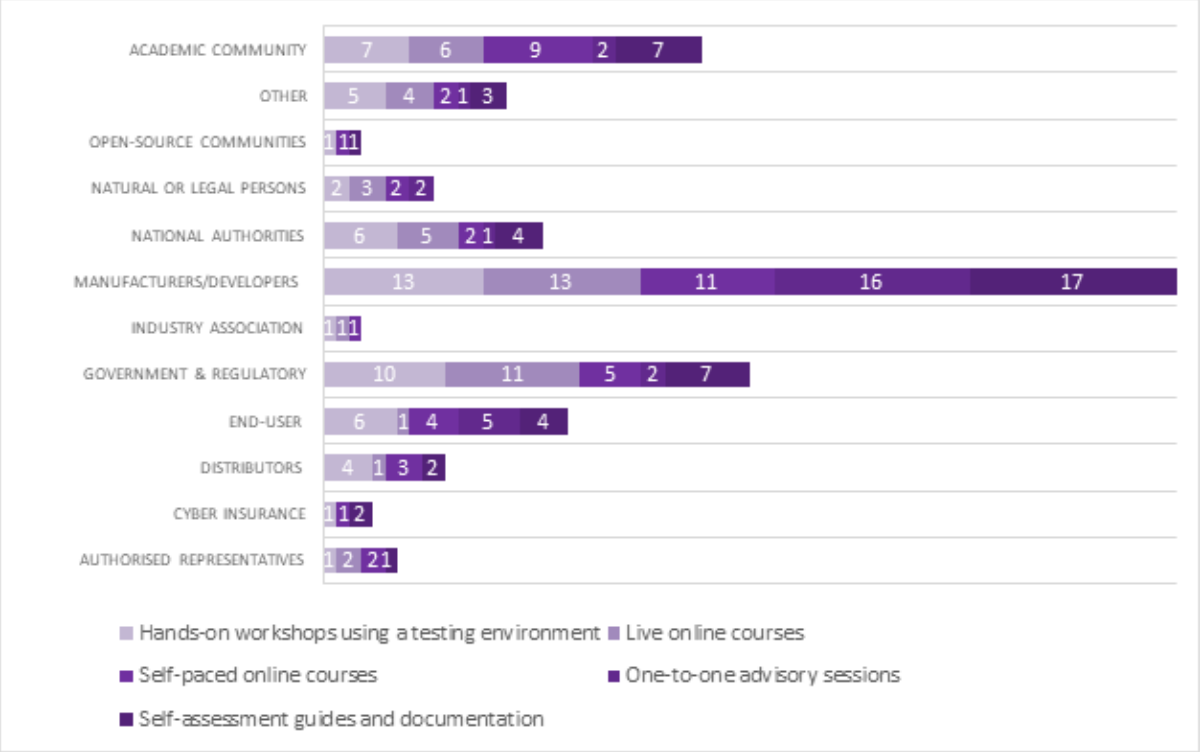


FIGURE 10: TRAINING PREFERENCES BY ORGANIZATION/ENTITY

National Authorities also display a wide engagement across all training types, with notable interest in self-assessment guides and documentation as well as hands-on workshops. This suggests that these entities value both structured self-learning materials and opportunities for interactive, scenario-based training, likely reflecting their dual role as regulatory enforcers and institutional leaders in CRA implementation.

The Academic Community prioritizes self-paced online courses and documentation, underscoring a preference for flexible, independent learning formats that align with academic schedules and the need for conceptual clarity. This pattern reinforces the importance of making high-quality, on-demand educational resources widely available.

Other stakeholder categories, such as distributors, government/regulatory bodies, open-source communities, and those identifying as "Other," exhibit more varied responses. However, the overall trend confirms a consistent appreciation for practical engagement formats, with recurring selections of workshops, advisory sessions, and live courses, suggesting a cross-sectoral need for hands-on exposure and contextualized instruction.

In summary, the findings underscore the necessity of offering a diversified training portfolio under the CURIUM Compliance Continuum. While interactive and customized formats appear especially critical for manufacturers, developers, and regulators, academic and institutional stakeholders equally require accessible, well-structured self-learning tools. These insights will directly inform the design and prioritization of training content, ensuring that the CURIUM project addresses the full spectrum of user expectations and operational realities.

3.2.6. Preferred host for training

Figure 11 below illustrates stakeholder preferences regarding the most suitable entities to deliver training related to the CRA. The majority of respondents selected National Cybersecurity Authorities (35%) as their preferred training providers, indicating a strong trust in nationally designated bodies to offer authoritative and context-specific guidance. This is closely followed by ENISA (29%), reflecting the agency's recognized role and credibility in shaping EU-wide cybersecurity practices. The European Commission (15%) also received considerable support, underscoring the importance stakeholders place on institutions directly involved in regulatory formulation. In contrast, only a small portion of respondents expressed preference for more general or decentralized options such as "Anyone" (12%), SME Associations (8%), and Other (1%), suggesting that stakeholders are less confident in informal or non-institutional providers. These findings highlight a clear expectation for CRA training to be led by established and authoritative actors, and strongly support the CURIUM project's intention to collaborate with national and European cybersecurity institutions in the design and delivery of its capacity-building activities.

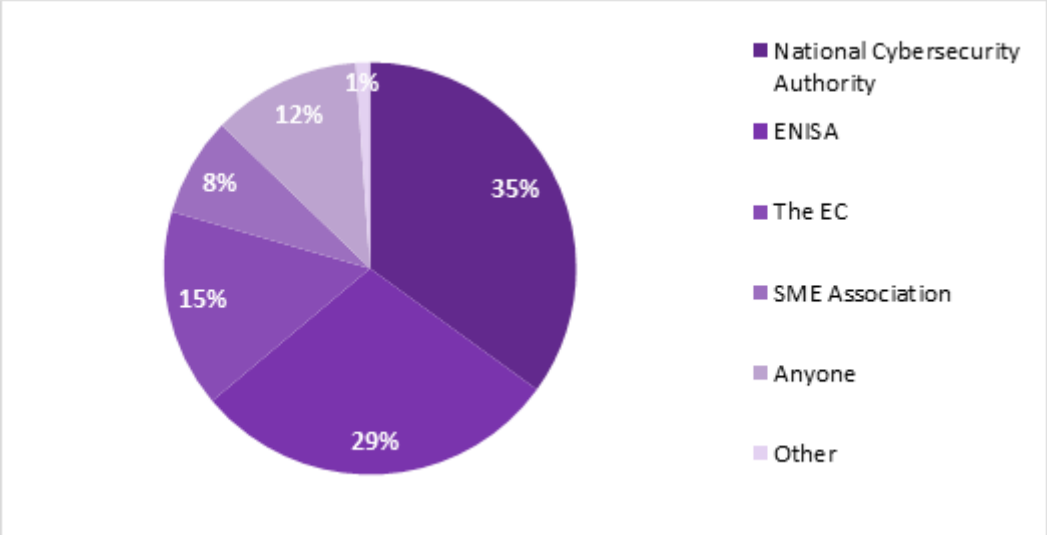


FIGURE 11: PREFERRED HOST FOR TRAINING

4. State of the Art

This section provides an overview of the state of the Art for each one of the technical components of the CURIUM Continuum.

4.1. Risk Assessment and Cyber Resilience

Cybersecurity risk management plays a critical role for assessment and management of risk for ensuring to overall system's resilience. It enables the identification of critical assets, vulnerabilities, and threats and the determination of suitable proactive control measures to tackle the related risks. According to the globally known and recognised information security standard of ISO/IEC 27000:2022 and its series, cyber risk can be defined as the effect of uncertainty on security objectives, specified for an ICT product/system/service[5]. In this regard, cybersecurity risk assessment provides the capability to investigate whether security requirements are met on ICT products / systems / services at the specified level of assurance, according to their criticality and intended use [6] . Moreover, cybersecurity risk assessment is the key-process to identify, assess and manage cyber risks on ICT products/systems/services and their accompanied vulnerabilities and threats. Risk assessment results can feed ICT stakeholders' decision making in adopting optimal mitigation strategies and countermeasures to meet the specified requirements and develop a Protection Profile that is subject to cybersecurity certification [7]. To this end, risk assessment process is a subset of an end-to-end cybersecurity certification evaluation process which can be utilized dually by:

- ICT stakeholders, as mentioned previously, scrutinize the risk posture of a Target of Evaluation[5] to undertake proper risk treatment that meets the security requirements at a specified level of assurance, according to the adopted certification scheme and prepare the Protection Profile with respective security claims,
- Assessors that conduct a conformity assessment as an assisting process to their security testing procedures by the respective authorized body (e.g. an ITSEF, security lab, etc.) to audit and evidence whether the security claims of a given Protection Profile are met.

Risk reflects three main concepts: i) event, ii) likelihood, and iii) severity. Nevertheless, the main focus is on undesirable events which pose a potential loss in a specific context (a set of negative circumstances). A risk event can be certain or uncertain and can be influenced by a single occurrence or a series of occurrences. Likelihoods indicate the frequency of an event and how probable it is to occur. NIST Cybersecurity Framework (CSF) 2.0 is a globally known risk-based taxonomy, designed for all audiences, industry sectors and organization types (from school and non-profit organizations to the largest agencies and corporations regardless of their degree of cybersecurity sophistication) providing them guidance to manage their cybersecurity risks [8]. It offers high-level cybersecurity outcomes that can be used by any organization of any size, sector, or maturity to better understand, assess, prioritize, and communicate its cybersecurity efforts. NIST SP 800-30 is a special publication

---

[5] SO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. [Online] Available: https://www.iso.org/standard/73906.html

[6] Regulation (EU) 2024/2847. Cyber Resilience Act (CRA). [Online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

[7] SO/IEC 15408: 2022. Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general mode [Online] Available: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:15408:-1:ed-4:v1:en

[8] NIST. Cybersecurity Framework (CSF) v2.0. [Online] Available: https://www.nist.gov/cyberframework

developed by NIST, which provides guidelines for securing IT infrastructure from a technical perspective[9]. The ETSI-TVRA methodology is an ETSI standard that orients security objectives, both to assets and their environments. It proposes a risk assessment methodology that implements ISO/IEC 15408 international standard for IT Evaluation, acknowledging inherent factors on which the attack potential is dependent [10].

4.1.1. Risk Management Methodologies and Tools

The resilience of ICT products to support the organization can be jeopardized by common threats (i.e., traditional cyberattack, cyber piracy, espionage, sabotage, etc.) and new rising threats (i.e., APTs, ransomware, botnet) capable of being supported by multiple sophisticated threat agents. In addition, the advent of emerging technologies (i.e., digital twins, IoT, Swarm Intelligence-based techniques, Big Data, adversarial learning techniques, etc.) has posed novel threats to the SC ecosystem[11]. Considering the analysis of the latest cyber threat landscape reports coming from dominant EU cybersecurity standardization bodies and prominent IT entities, it can be deduced that SC sophisticated cyberattacks have become a new emerging alarming scenario. Digital Supply Chains consist of interconnected dispersed nodes, changing dynamically and impeding the chance to adjust to the tremendously evolving threat landscape [12] . Therefore, a combination of both proactive/preventive approaches to size the robustness and reactive strategies to improve agility can be utilized to address this challenge. Additional guidelines have been provided by ENISA on IoT security to illustrate indications and good practices according to existing standards and research [13].

Considering the multi-level specificities of the modern ICTs, risk assessment approaches should be used to minimize the existence of vulnerabilities and the potential loss of the subject that is under risk evaluation promoting business continuity and security maintenance. Thus, for managing supply chain cybersecurity risks, ICT organizations need to understand their interactions with other entities, including multiple layers of sub-suppliers [14]. NIST SP 800-161 provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks introducing a multi-tiered, SCRM-specific approach [15].

The research work in analyses and quantifies cyber assets criticality participating in complex ICT services considering their interdependencies within the services together with ICT stakeholders' business value and

[9] NIST SP 800-30 Rev. 1 (2012). Guide for Conducting Risk Assessments [Online] Available: https://csrc.nist.gov/pubs/sp/800/30/r1/final

[10] ETSI. ETSI TS 102 165-1 V5.2.3 (2017-10) CYBER;Methods and protocols;Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA). Technical Specification (2017). [Online] Available: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

[11] Silvestri, S., Islam, S., Amelin, D. et al. Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. Int. J. Inf. Secur. 23, 31–50 (2024). https://doi.org/10.1007/s10207-023-00769-w

[12] Islam, S.; Papastergiou, S.; Kalogeraki, E.-M.; Kioskli, K. Cyberattack Path Generation and Prioritisation for Securing Healthcare Systems. *Appl. Sci.* **2022**, *12*, 4443. https://doi.org/10.3390/app12094443

[13] ENISA (2020). "Guidelines for Securing the Internet of Things". Online available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[14] Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2021). Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (No. NIST Internal or Interagency Report (NISTIR) 8276). National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8276

[15] NIST SP 800-161 (2022). "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations". [Online] available: https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

needs [16]. The estimation of the asset's criticality is considered for the calculation of cyber risks in a hybrid cybersecurity risk and conformity assessment approach. In Boiko et al. a qualitative research method is presented for analysing the Supply Chain process and identifying the most effective strategies for information support in Supply Chain environments to eliminate cyber risks [17]. Nevertheless, qualitative risk assessment does have the appeal of efficiency and is easy to communicate and explain to stakeholders; however, there are no commonly accepted ratings for safety and security that would apply as a standard. Additional complications arise from the need to map the existing infrastructure of an organization onto a fixed terminology with which the chosen risk assessment method works. CRAMM is a risk analysis method for all types of information systems and networks, identifying security requirements, detecting contingency requirements, and proposing possible solutions [18]. The STORM-RM is a collaborative and multi-criteria risk management ISO27001-based methodology promoting organization users to participate in the various risk assessment and treatment phases combining risk computation with the AHP algorithm [19] .

ISAMM is a risk management methodology, with supporting information security tools. It is a quantitative-mathematical approach in which risks are assessed and ranked by an Annual Loss Expectancy (ALE) [20]. ISAMM draws on a state-of-the-art knowledge base with contextual risk-reducing capabilities of security controls, which are established in the information security standard. The risk assessment can be done as a matrix that, for each control objective and threat, provides an estimate of the relative reduction in risk, if that control is implemented. Based on estimates of the current risks, implementation costs of missing security controls, as well as risk mitigation factors, and the economic benefit, the so-called Return on Security Investment (ROSI) is estimated and used to create a list of measures.

Several tools are now available for cybersecurity risk management. An integrated Government, Risk and Compliance (GRC) Scrut Platform aims to protect the cyber asset and at the same time achieve the relevant compliance [21]. The key feature of this platform is to provide the visibility of all organizational assets for risk assessment and management and focus both internal and external assets including third party application, code repositories, vendors, employees, and internal processes. Another comprehensive risk management solution is RiskWatch that provides organizations to assess, monitor, and mitigate various types of risks and designs to offer a user-friendly interface and customizable features to adapt to the unique needs of different industries [22]. Common functionalities of the tool include conducting comprehensive risk assessments, compliance management, security risk management, Business Continuity and Resilience and Vulnerability Management.

[16] Tešendić, D., Kalogeraki, E.M., Vivo, G., Polemi, N., Boberić K.D. (2023) "Quantifying asset criticality in supply chains" In Proceedings of the 9th International Conference on Engineering and Emerging Technologies (ICEET), 27-28 October

[17] Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. Procedia Computer Science, 149, pp. 65-70

[18] CRAMM, 2005) Insight Consulting, CRAMM User Guide, Issue 5.1, United Kingdom, 2005

[19] Ntouskas, T. and Polemi, N. (2012) "STORM-RM: a collaborative and multicriteria risk management methodology", International Journalof Multicriteria Decision Making, Vol. 2, No. 2, pp.159–177

[20] Harpes/Adelsbach/Zatti/Peccia: Quantitative Risk Assessment with ISAMM on ESA's Operations Data System. Telindus S.A., Security, Audit and Governance Services, Luxembourg. Filipe Neto Rodeia Macedo: Models for Assessing Information Security Risk. Instituto Superior Técnico, Lisbon 2009. International Journal of Computer Applications (0975 – 8887): A Comparative Analysis on Risk Assessment Information Security Models. November 2013

[21] https://www.scrut.io/

[22] https://www.riskwatch.com/cyberwatch/

Finally, the CRA Self-Assessment Tool (https://cyberstand.eu/cra-self-assessment-tool) has been developed to help SMEs evaluate their level of preparedness according to the Cyber Resilience Act (CRA). Well-structured questionnaires help the user to gain a better understanding of the key expectations outlined in the CRA and assess the alignment of the existing processes and security measures align with security requirements. The tool not only evaluates the overall preparedness of the organization but also identifies necessary improvements and enhancements. Also, it helps SMEs allocate their resources, both financial and human, effectively to ensure compliance and strengthen their overall cybersecurity resilience.

4.1.2. AI enabled Cybersecurity Risk Management

The adoption of AI for cybersecurity risk management is now widely considered due to the large volume of security data such as vulnerabilities associated with different ICT products and other infrastructure. AI models can support the prediction of various risk management components such as risk type, and vulnerability exploitability, which can be used to quantify the risk so that suitable mitigation actions can be taken into consideration for tackling the risk. An AI-driven, DLT (Distributed Ledger Technology)-based smart contract system is proposed for secure sharing of threat intelligence, risk modelling, and structuring of risk transfer instruments [23]. The approach provides the capabilities for risk mitigation decisions in an automatic manner and transfer of residual risks with AI-driven DLT-based smart contracts. The integration of AI and DLT technologies is planned to increase the security and efficiency of managing cyber risks. The ML and deep learning based secure data analytics architecture is utilized for attack identification and mitigation based on attack related data. The threat model addresses research challenges using different parameters such as reliability, accuracy, and latency. The NLP method based on Large Language Models and ML (XG-Boost) based model is proposed to obtain threat and vulnerability assessment for the healthcare ICT assets, exploiting constantly updated information crawled from the web and cybersecurity Knowledge Bases [24]. NLP based approach is further used to extract useful threat information specific to assets from text that contains security-related information to support cyber threat assessment and management is described in [25]. The approach allows to assess the threats related to several real-world scenarios by leveraging natural language documents crawled from cybersecurity news websites, demonstrating its effectiveness and usability. BERT based LLM model architecture with transparency obligation practices is proposed to detect the vulnerability from the source code data set [26]. The work tackles the black box nature of AI models using XAI practice with SHAP, LIME, and heat map. Architecture considers the entire life cycle of the model and experiment results shows an accuracy of 92.19 % with minimal primary training and validation loss.

4.2. Maturity Assessment for Controls

A maturity model provides the means of and scale for evaluating and assessing the current state of maturity. Such model also provides a means for developing a transformation roadmap to achieve a target state of maturity from a given current state of maturity. It quantifies the relative growth of certain salient aspects within various

[23] andey, P., Katsikas, S.: The future of cyber risk management: Ai and dlt for automated cyber risk modelling, decision making, and risk transfer. In: Handbook of Research on Artificial Intelligence, Innovation and Entrepreneurship, pp. 272– 290. Edward Elgar Publishing

[24] Gupta, R. et al. (2020) 'Machine learning models for secure data analytics: A taxonomy and threat model', Computer Communications, 153, pp. 406–440.

[25] Silvestri, S., Islam, S., Papastergiou, S., Tzagkarakis, C., Ciampi, M.: A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem. Sensors 23(2) (2023)

[26] Jean Haurogné, Nihala Basheer, Shareeful Islam, Vulnerability detection using BERT based LLM model with transparency obligation practice towards trustworthy AI, Machine Learning with Applications, Volume 18, 2024, 100598, ISSN 2666-8270

dimensions typically within, but not limited to, organizational boundaries. [27] Maturity models are widely used across various domains, including information security, software development, IT governance, and risk management. They enable organizations to evaluate their capabilities, benchmark against best practices, and identify areas for improvement.

Maturity models typically define a series of maturity levels, often ranging from "initial" or "ad hoc" (least mature) to "optimized" or "sustainable" (most mature). Each level describes progressively more advanced and reliable process characteristics.

ISO/IEC 27001 is a globally recognized standard for establishing an Information Security Management System (ISMS). It includes a set of controls outlined in Annex A to address various aspects of information security. A maturity assessment against ISO/IEC 27001 would involve evaluating the implementation, effectiveness, and integration of the controls. The objective is not only to ensure compliance but also to achieve higher levels of security assurance and operational efficiency.

Some of the maturity models that are related to information security are described below:

Capability Maturity Model Integration (CMMI): Is a globally recognized framework currently owned by ISACA for improving organizational performance. Originally created for the U.S. Department of Defence to assess software contractors, CMMI has evolved to address performance improvement across various industries and organizational sizes. It provides organizations with a structured approach to assess their current capabilities and implement strategies for continuous improvement.[28]

Maturity Levels:

- Initial (Level 1): Processes are unpredictable and reactive.
- Managed (Level 2): Processes are characterized by projects and are often reactive.
- Defined (Level 3): Processes are characterized for the organization and are proactive.
- Quantitatively Managed (Level 4): Processes are measured and
- Optimizing (Level 5): Focus on continuous process improvement.

CMMI's structured approach to process improvement complements ISO/IEC 27001 by providing a roadmap for enhancing information security processes and controls. Organizations can leverage CMMI to assess the maturity of their information security management systems (ISMS) and implement best practices that align with ISO/IEC 27001 requirements.

NIST Cybersecurity Framework (CSF)[29]: Developed by the U.S. National Institute of Standards and Technology, the NIST CSF provides guidelines for managing cybersecurity risks. It comprises:

- Core Functions: Identify, Protect, Detect, Respond, Recover.
- Implementation Tiers: Indicate the degree to which cybersecurity risk management practices exhibit the characteristics defined in the framework.

Implementation Tiers:

- Tier 1 – Partial: Risk management practices are not formalized.
- Tier 2 – Risk-Informed: Risk management practices are approved but not established organization-wide.
- Tier 3 – Repeatable: Risk management practices are formally approved and expressed as policy.
- Tier 4 – Adaptive: Risk management practices are adaptive and continuously improving.

The NIST CSF can be used alongside ISO/IEC 27001 to provide a comprehensive approach to managing cybersecurity risks.

[27] ISO/IEC 16680:2012(en). Information technology — The Open Group Service Integration Maturity Model (OSIMM). https://www.iso.org/standard/57404.html. 1.4. Terminology

[28] https://www.isaca.org/enterprise/cmmi-performance-solutions

[29] https://www.nist.gov/cyberframework

ENISA CSIRT Maturity Framework[30]: The European Union Agency for Cybersecurity (ENISA) developed the CSIRT Maturity Framework to assess and enhance the maturity of Computer Security Incident Response Teams (CSIRTs). It is based on the Security Incident Management Maturity Model (SIM3).

Maturity Levels:

- Basic: Foundational capabilities are established.
- Intermediate: Enhanced capabilities with some formalization.
- Advanced: Highly formalized and optimized capabilities.

This framework aids in assessing and improving incident response capabilities, aligning with ISO/IEC 27001 requirements for managing information security incidents.

ITIL Maturity Model[31]: The Information Technology Infrastructure Library (ITIL) Maturity Model assesses the service management capabilities of an organization and the maturity of its governance structure and management system.

Maturity Levels[32]:

- Level 1 The continual improvement practice is at level 1 or higher. Performance data is occasionally collected, some improvements are implemented.
- Level 2 The continual improvement practice is at level 2 or higher. Some areas of management are repeatedly evaluated and improved; these activities are reactive and largely undocumented
- Level 3 The continual improvement practice is at level 3 or higher. Performance objectives are documented and mapped to the business objectives. A common process for measurement and improvement is formally adopted.
- Level 4 The continual improvement practice is at level 4 or higher and applied to all or most aspects of the SVS. Organizational improvements are measured quantitatively, improvement dynamics are monitored and analysed, and improvements are implemented proactively.
- Level 5 The continual improvement practice is at level 5. Performance objectives are dynamically aligned with the business strategy. The continual improvement approach evolves to support the organization's vision and objectives.

ITIL's focus on service management complements ISO/IEC 27001 by ensuring that information security processes are integrated into overall IT service management.

COBIT Maturity Model[33]: Control Objectives for Information and Related Technologies (COBIT) is a framework for developing, implementing, monitoring, and improving IT governance and management practices.

Maturity Levels:

- Level 1 Initial – Work is completed, but the full goal and intent of the focus area are not yet achieved.
- Level 2 Managed – Planning and performance measurement take place, although not yet in a standardized way.
- Level 3 Defined – Enterprise-wide standards provide guidance across the enterprise.
- Level 4 Quantitative – The enterprise is data driven, with quantitative performance improvement.
- Level 5 Optimizing – The enterprise is focused on continuous improvement.

COBIT provides a governance framework that can be used to ensure that information security controls are aligned with business objectives, as required by ISO/IEC 27001.

---

[30] https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity

[31] https://www.axelos.com/for-organizations/itil-maturity-model

[32] https://eu-assets.contentstack.com/v3/assets/blt637b065823946b12/bltc4d875b75a1442ce/618029daa0038563ae7fdbd6/An_Overview_of_the_ITIL_Maturity_Model.pdf

[33] https://www.isaca.org/resources/news-and-trends/industry-news/2020/effective-capability-and-maturity-assessment-using-cobit-2019

Cybersecurity Capability Maturity Model (C2M2)[34]: Developed by the U.S. Department of Energy, C2M2 helps organizations evaluate and improve their cybersecurity capabilities, focusing on both information technology (IT) and operational technology (OT) assets and environments.

Maturity Indicator Levels (MILs):

- MIL1 – name: Initiated, description: Initial practices are performed, but may be ad hoc
- MIL2 – name: Performed, description: Practices are documented, Adequate resources are provided to support domain activities, Practices are more complete or advanced than at MIL1
- MIL3 – name: Managed, description: Activities are guided by policy (or other directives), Personnel have the skills and knowledge needed to perform their assigned responsibilities, Responsibility, accountability, and authority for practices are clearly assigned to personnel with adequate skills and knowledge, The effectiveness of activities in the domain is evaluated and tracked, Practices are more complete or advanced than at MIL2

C2M2 provides a detailed approach to assessing and improving cybersecurity capabilities, supporting the continuous improvement aspect of ISO/IEC 27001.

CIS Critical Security Controls®[35]: The CIS Controls® started as a simple grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and then share that information with a wider audience. The original goals were modest—to help people and enterprises focus their attention and get started on the most important steps to defend themselves from the attacks that really mattered.

The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls.

Implementation Groups:

- IG1: An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off the-shelf (COTS) hardware and software.
- IG2 (Includes IG1): An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.
- IG3 (Includes IG1 and IG2): An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

[34] https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[35] https://www.cisecurity.org/controls

NIS Directive compliant Cybersecurity Maturity Assessment Framework[36]: Cybersecurity Maturity Assessment Framework (CMAF) is tailored to the NIS Directive requirements. CMAF can be used either as a self-assessment tool from Operators of Essential Services and Digital Service Providers or as an audit tool from the National Competent Authorities for cybersecurity.

Maturity Levels:

- Maturity Level 1: Initial – Reactive: The organization has started implementing the requirement, but the extent of the implementation is partial or reactive.
- Maturity Level 2: Basic – Managed: There is a concrete plan regarding the fulfillment of the requirement. The necessary controls are implemented but are partially measured and partially controlled.
- Maturity Level 3: Advanced – Defined: There is a standardized method regarding the fulfilment of the requirement. The necessary controls are implemented, measured, and controlled at the described level.
- Maturity Level 4: Effective – Quantitatively: Managed The organization has set specific objectives. The objectives (were possible S.M.A.R.T. compliant) are being monitored, measured, analyzed, and evaluated. The necessary controls are implemented, measured and controlled at the described level.
- Maturity Level 5: Efficient – Optimized: The organization has implemented methods for the continuous improvement of the implemented controls and the security posture of the organization. A full risk-based approach is followed and a cost benefit balance is applied. The necessary controls are implemented, measured, and controlled at the described level.

4.3. Maturity Assessment of Digital Products

The "Maturity Assessment of Digital Products" plays a critical role in supporting manufacturers, developers, importers, and conformity assessment bodies in evaluating how well digital products comply with CRA requirements. The main objective of maturity assessment of digital products is to identify the strengths and the gaps meeting CRA obligation, provide structural guidance for improvement and risk mitigation and support conformity assessment procedures and post-market mitigation.

Each digital product is assessed across the following CRA-relevant dimensions:

- Security by design: threat modeling, security architecture, code audit, etc.
- SBOM Management: existence and maintenance of Software Bill of Materials.
- Vulnerability Management (+Handling): process for detection, disclosure, reporting any known vulnerabilities.
- Technical Documentation: availability, compliance, structure, up-to-date status of the technical and user documentation.
- Post-Market Monitoring/Analysis: continuous threat and legal intelligence.
- Compliance with Standards: alignment with relevant standards (vertical, horizontal).

The maturity assessment framework proposed in CURIUM is a vital instrument for aligning digital product development and maintenance with CRA obligations. The implementation within the CURIUM ensures that manufacturers and developers can continuously evaluate and enhance their products' cybersecurity posture in a structured, repeatable, and auditable manner.

4.4. Vulnerability Assessment and Penetration Testing

In the modern cybersecurity landscape, Vulnerability Assessment and Penetration Testing remain foundational pillars in securing network and web services and have become critical components of an organisation's security

[36] https://ieeexplore.ieee.org/document/9202470

posture[37]. As cyber threats continue to evolve in complexity, so too must the defence framework. The tools, methods, and techniques employed to detect, assess, and mitigate vulnerabilities must align with current best practices in order to ensure that the systems can remain resilient against the increasingly sophisticated attacks.

Traditional approaches rely heavily on periodic and manual testing. Nowadays, organisations emphasise ongoing vulnerability scanning and penetration testing integrated into their development and operational workflows rather than sporadic audits[38] [39]. This change is necessary due to the dynamic nature of cyber threats and the extreme frequent deployment cycles which characterize the modern IT environments. Automation is a major pillar driving this transformation. AI-powered tools are introduced to vulnerability scanning and penetration testing, enabling faster and more accurate identification of security weaknesses[40]. Machine Learning models analyse attack patterns to predict potential exploits. This automation reduces manual effort while enhancing coverage and precision.

Despite the aforementioned advances in automation, the role of a human, with security expertise, in the procedure remains indispensable. Human-augmented penetration testing is focusing on enhancing security overall by providing creative exploitation techniques and complex attack simulations that the automated tools may miss. Exercises including offensive (Red) and defensive (Blue) teams' collaborations foster an enhanced security posture by addressing the security aspects holistically, taking into consideration both the attacker's and defender's insights. This hybrid approach ensures that both broad vulnerability detection and deep, context-aware analysis are achieved[41].

Regarding network and web service vulnerabilities, current best practices reflect the criticality of these domains. Network vulnerability assessments use advanced scanning tools to identify potential misconfigurations, open ports, outdated services, and protocol weaknesses. Penetration testing complements the assessment by attempting to exploit the discovered vulnerabilities, in a controlled environment, in order to validate their feasibility and by extend their impact to the system.

Web services tend to be exposed through APIs and cloud-hosted applications and for that reason they require specialised testing. Automated scanners focus on identifying common web server misconfigurations, outdated software components, and known vulnerabilities such as cross-site scripting (XSS), SQL injection, directory traversal, etc. Penetration testing extends this by simulating real-world attack vectors to uncover potential business logic flaws and chained exploits that automated tools might overlook.

A trend that rises in web service security is the integration of vulnerability assessment and penetration testing into Continuous Integration/Continuous Deployment (CI/CD) pipelines. This specific approach, the moving of testing and security activities to the earliest stages of Software Development Lifecycle (SDLC), is called "shift-left" and allows for the identification and remediation of vulnerabilities before deployment[42].

Despite the significant advancements in vulnerability assessment and penetration testing, there are still several challenges. One major issue is the increasing number of known vulnerabilities that organisations must deal with. New vulnerabilities are being discovered regularly, and security teams need to put a lot of effort to keep up with

[37] https://cyberpanel.net/blog/vulnerability-assessment-vs-penetration-testing

[38] https://fort1.com.au/2025-trends-the-role-of-managed-vulnerability-assessments-and-penetration-testing-in-compliance/

[39] https://ntgit.com/why-your-business-needs-penetration-testing-and-vulnerability-assessments-in-2025/

[40] Komaragiri, Venkata & Edward, Andrew. (2022). AI-Driven Vulnerability Management and Automated Threat Mitigation. International Journal of Scientific Research and Management (IJSRM). 10. 980-998. 10.18535/ijsrm/v10i10.ec05

[41] https://www.yeahhub.com/emerging-trends-in-vulnerability-assessment-and-penetration-testing-vapt-for-2025/

[42] https://faulted.io/blog/top-5-penetration-testing-trends-in-2025

patching and remediation efforts. The sheer variety of available tools regarding vulnerability scanning leads to an overwhelming feeling, with organisations often to be unsure of which solution would be best or even sufficient for their specific needs.

Moreover, zero-day vulnerabilities -unknown vulnerabilities for which no patch exists- will always going to pose a significant threat. While penetration testing tools can identify a vast number of known vulnerabilities, they can't discover zero-day exploits. This stresses out the need for continuous research in the field[43].

4.5. Relevant Research Projects

CYRENE[44] focuses on enhancing security, privacy, resilience for the services within the Supply Chain based sectors using a novel and dynamic Conformity Assessment Process (CAP). CAP supports the supply chain context to recognize, identify, model, and dynamically analyse cyber risks. The CAP also supports forecasting, treatment and response to advanced persistent threats and handle daily cyber-security and privacy risks, incidents and data breaches. In this context, the project provides the capabilities for both self-assessments, where organisations self-assess the security, resiliency and privacy of their supply chain and Third-party assessment, where an independent party performs the assessment, and self-attestation of the manufacturer or service provider makes a public statement. Therefore, the certification schemes offered by CYRENE include Supply Chain, ICT-based or ICT-interconnected Supply Chain, and SCs' (e.g. Maritime, Transport or Manufacturing) IoT devices and ICT systems.

CYRENE follows four circles of consideration that holistically covers CT-based SCs starting from ICT systems, equipment and devices such as SCADA systems, IoT, Communication network assets, local hubs, switches, and servers to individual and Interdependent Critical Information Infrastructures (CIIs) . The key outcomes of the project are CYRENE's conformity assessment process with multi-level evidence-driven Supply Chain risk assessment and dynamic vulnerability assessment with data protection and security declaration. These outcomes and tools are integrated into a prototype to implement conformity assessment process which evaluated through pilots for carrying the conformity assessment and best practice guidelines are provided upon completion of the pilot cases.

CUSTODES[45] focuses to enhance trust in ICT through versatile cybersecurity certification by creating a dynamic and collaborative Composite Inspection and Certification (CIC) System. CIC system of the project implements a Composite Certification process that delivers certification as a service, enabling the continuous monitoring, effective assessment of the controls and the validation of the cyber-security posture of the ICT products, services, and processes under security audit and evaluation. The project targets different stakeholders including Self-Assessors (e.g. providers or end-users of the systems), Conformity Assessment Bodies (CABs) or any National Cybersecurity Certification Authorities (NCCA) to establish a Europe-wide ecosystem for conducting audits, inspections and certifications. CUSTODES aims to achieve not only interoperability and stakeholder alignment on security practices but also enhance control and trust of the Composite Products and resilience of the composite Target of Evaluation.

The outcome of the project includes key distinct components to support cyber security certification initiated with Dynamic Risk Assessment aims at providing a harmonized risk-based approach for identifying the security objectives and requirements and at building the Security Profiles (SPs) of Composite TOE. The next component is the Composite Conformity Assessment Process aims to evaluate the Composite TOE against a set of Security Requirements defined in the relevant SPs. The outcome also includes Certificate Discovery component which facilitates the reuse of certification evidence, to further open-up the certification-related data and to increase transparency and consistency of the certification process. Finally, Certification Sharing component offers threat

[43] https://deepstrike.io/blog/penetration-testing-statistics-2025

[44] homepage - cyrene

[45] Custodes

intelligence and certification sharing capabilities, enabling collaboration, secure and privacy-aware exchange of information among different stakeholder including assessors, TOE providers and other relevant third parties.

OSCRAT[46] - The aim of the project is to enhance cybersecurity resilience among European SMEs through the development of an open-source, completely free, tool dedicated to supporting compliance with the CRA. The project goal is to equip small and medium-sized European enterprises, policy & decision makers, Digital Innovation Hubs and industrial associations with all the necessary resources to enhance cybersecurity practices in the modern digital landscape. The project will deliver few tools as a SBOM generator, IR tool, Vulnerability assessment tool, Centralized documentation and Audits capabilities.

CRYCY[47] is an initiative of collaboration of 11 top European Cybersecurity technology providers supporting the deployment of the CRA. The aim of this initiative to lower the barriers for small and medium European (SME) engineering companies to be able to facilitate the necessary security requirements for their products with digital element and support SME – also software developers, to understand and be compliant with the CRA requirements.

CYBERSTAND[48] aims to empower European stakeholders to engage in the development of standards and conformity in relation to the Cyber Resilience Act (CRA). To reach this goal, the work of CYBERSTAND will be based on the following activities:

- Support EU experts in the contribution to standardization efforts: CYBERSTAND.eu will select and onboard more than 200 experts through 6 cycles of Specific Service Procedures (SSPs), assigning a total of 1.500.000 € for developing and working on harmonized standards
- Contribute and reinforce European values, ethics and policy in cybersecurity: CYBERSTAND.eu will influence the future cybersecurity ecosystem through promotional and educational materials and tools, with +100 European experts trained in cybersecurity standardization
- Foster the development on harmonized standards in conformity with the CRA: CYBERSTAND.eu will contribute to +10 standardization of work items, showcasing +30 use cases and supporting the contents of cybersecurity chapter in the Rolling Plan for ICT standardization
- Deliver a series of events and publications: CYBERSTAND.eu will increase the European influence and leadership in international cybersecurity standardization through stakeholder consultations, policy briefs and events, aiming at improving the general awareness of cybersecurity standards in Europe.

[46] www.oscrat.eu

[47] www.cra-cy.eu

[48] Cyberstand

5. CURIUM Technical Tools and Services

5.1. Objectives of the Tools and Services

The objective of the CURIUM Tools and Services are aligned with the goals of supporting CRA compliance, SME cyber-security resilience and EU certification preparedness. The primary objective of the tools developed and deployed under the CURIUM project is to empower European SME with practical, scalable and accessible means to achieve compliance with the CRA and related EU cyber-security regulation. Recognizing that SMEs often lack the internal capacity, technical expertise, or financial resources to fully implement complex cybersecurity compliance frameworks, CURIUM aims to close this gap through a suite of integrated tools and support services.

These tools and services are designed to:

- Facilitate Conformity Assessment and Compliance (CAC) processes for “product with digital elements”, especially IoT, by offering interactive support for meeting CRA requirements such as technical documentation, vulnerability management, and post-market monitoring.
- Support the generation and management of technical documentation aligned with CRA Annex V and VII, through intuitive interfaces, versioning systems, and DEMF-compliant secure storage.
- Bridge regulatory gaps by providing audit-ready reporting, ensuring SMEs are better prepared for third-party assessments or future certification schemes.
- Foster innovation and reusability by building upon open standards, open-source components, and API-ready modules that can be adopted, integrated, or extended by stakeholders beyond the project lifecycle.
- Offer a user-friendly interface, ensuring that even non-expert users can efficiently perform vulnerability scans, interpret results, and prioritise security efforts based on the severity of identified risks.
- Provide customisable scans addressing different SME environments, ensuring flexibility and adaptability for diverse compliance needs and regulatory requirements.

Overall, the tools developed in CURIUM are not stand-alone utilities, but modular building blocks designed to integrate into an ecosystem of European trust-enabling technologies, with a focus on practicality, modularity, and regulatory alignment. These tools will play a key role in establishing a European Trustworthy Certified Digital Valley, supporting cyber-secure innovation while maintaining regulatory compliance across digital product lifecycles.

5.2. Tools-Specific Description

5.2.1. DPRA, Digital Product Risk Management / Risk Management Suite

This suite for the DPRA is an evidence-driven, step-wised dynamic approach which aims to consider threats, vulnerabilities and risks arising from interdependent assets of ICT product and entire infrastructures of the organization. The tool provides capabilities to the organisations for managing their security risks in a holistic and cost-effective manner by assessing both individual and cascading risk.

In the context of the CURIUM project, this DPRA will support 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 is on the adopted assurance level and assurance evaluation criteria pre-defined by the interested party, will take advantage of multi-order risk assessment and impact assessment capabilities to

identify/assess vulnerabilities, threats, risks on the assets of a given ICT product and its digital element. This tool provides the capability to decompose the products to identify the individual digital elements comprising them. This analysis will not solely focus on the individual parts of a product but will also consider the technical interdependencies between them, which may raise significant security issues. Modelling the digital elements of the product will offer a visual representation of all cyber aspects and information, enhancing understanding of potential problems, threats, failures, and dysfunctions. Additionally, adapting and applying this digital elements-based approach to decomposing a product facilitates and guides the specification of all relevant cybersecurity requirements. Based on this analysis and modelling of digital elements, a requirement specification stage becomes necessary to identify all relevant cybersecurity requirements associated with both the digital products as a whole and with the individual cyber components.

The tool exhibits following key features:

- Open intelligence facilitates the DPRA to adopt and incorporate a variety of taxonomies, catalogues, and models developed and maintained by organizations such as NIST, MITRE, and FIRST, as well as standards and specifications like NIST 800-53 and ISO/IEC 15408. This allows to automate the population of the adopted asset-threat-vulnerability model with data from reputable sources such as CPE, CAPEC, CWE, and CVE. All these taxonomies and methodologies have been designed to complement each other and work in concert as interconnected aspects of a common framework. For instance, various techniques outlined in ATT&CK are associated with specific CAPEC identifiers. Moreover, CAPEC enumerated attack patterns are documented alongside their corresponding weaknesses, establishing a direct link and robust relationship with the CWE catalogue. Additionally, the CWE catalogue provides observed examples for each weakness, represented in the form of a CVE identifier, which may be associated with a series of known CPEs. Lastly, a mapping has been established between the functional and assurance requirements defined in ISO/IEC 15408 (Common Criteria) and the security controls outlined in Special Publication 800-53.
- The ICT product declaration feature allows to declare the asset related to the ICT products and defined the cyber dependencies among the assets. This future allows the creation of an IT product-based asset inventory include digital element such as computing and networking related devices owned, managed, or otherwise used by the organisations.
- The Vulnerabilities Management feature identifies the possible vulnerabilities from the CVEDetails portal that are relevant with the identified asset in real time. All the vulnerability information is based on the CVE naming standard and are organized according to severity determined by the Common Vulnerability Scoring System Version 3 (CVSSv3) standard. Therefore, according to the CVE metamodel, a unique ID is declared, the value of the CVSS Score (ranging from 1 to 10) is determined and the access complexity, authentication, exploitability and the various impacts (in confidentiality, integrity and availability) are estimated.
- The asset dependency modelling allows to visualize the dependencies among the assets for the discovery of attack paths given a specific set of assets. This provides capabilities to visualize of the entire infrastructure along with the linked security and risk related information such as threats, vulnerabilities and attack-types that are relevant to the individual assets that have been declared
- The Threats and Controls declaration feature acts as a comprehensive dictionary of known threats as well as the corresponding mitigation controls that can be used to advance organizations understanding and enhance their defences. This allows to synchronize the MITRE attack identifiers and associates the identified vulnerabilities with one or more weakness identifiers.
- The Risk Assessment is responsible to provide guidance for the conduction of a risk assessment based on the identified asset, vulnerabilities, threats and impact. The tool considers both individual and cascading risk assessment where individual risk refers to the impact of potential exploitation of vulnerabilities for a specific asset and cascading risk estimation quantifies the risk based on assets and their vulnerability chain.
- Risk Reporting provides the outcome of risk assessment including asset, vulnerability, threat and risk level so that organizations can undertake suitable control to mitigate the risks.

The Risk Management suite high level architecture is presented the below **Figure 12**.

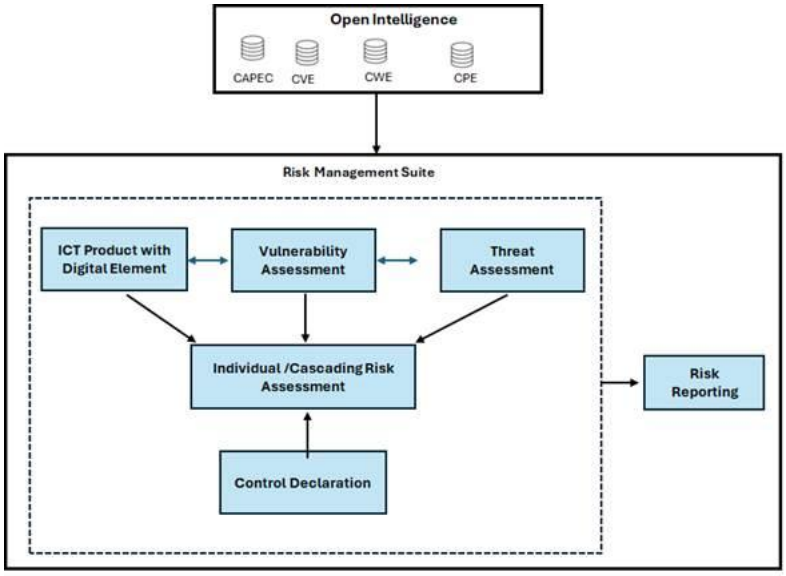


FIGURE 12: RISK MANAGEMENT SUITE, HIGH LEVEL ARCHITECTURE.

5.2.2. CyReA, Cyber Resilience Assessment / Governance, Risk and Compliance tool

This interactive user tool provides capacities related to the cyber resilience assessment of ICT products. 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 CRA of the incorporated digital elements. 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 CRA. Following the guidelines of the CRA, the CyReA service categorizes digital products into two main groups based on their risk level.

- The first group includes non-critical digital products that do not exhibit any significant security flaws and have not disclosed vulnerabilities with high severity levels. SMEs with such products are required to conduct a self-assessment to identify potential weaknesses that necessitate immediate mitigation actions and improvements.
- The second group further classifies products into two classes (I and II) based on their criticality and intended use. "Class I" includes digital products such as Identity and Access Management software, browsers, password managers, and malicious software detection tools, which have a lower cybersecurity risk level compared to those in Class II. Class II encompasses higher-risk products with critical cybersecurity vulnerabilities such as Hypervisors and container runtime systems supporting virtualized execution of operating systems, Firewalls, intrusion detection & prevention systems, and microprocessors & microcontrollers. There are also critical classes of products that fall under class II including Hardware devices with security boxes, smart meter gateways, smart card, etc.

This tool incorporates a wizard to fulfil the needs of the cybersecurity implementers. The wizard contains systematic manner guidelines and support to understand the specific SME current context and category based on the possible satisfaction of the mandatory requirements. The overall high-level architecture of the tool consists of an end-user interface and a series of questions formulated to capture the user response. Users need to interact with the interface provided by the tool and provides answers to the questions. The application provides responsive web interfaces for easier questionnaire filling and developed as script-based application. These applications utilize the REST API provided at backend which consists of three modules, i.e., REST services implementation, user management service and document processor. REST services implementation is the mediator between the external applications and the underlying database. The user management service supports all the common user management operations, like user creation and password change, hiding the

underlying identity and authentication logic. The document processor is used for parsing Microsoft Word documents (in .docx format) by replacing variable values and conditionally rendering text. **Figure 13** below presents the high-level architecture of the Governance, Risk and Compliance tool.

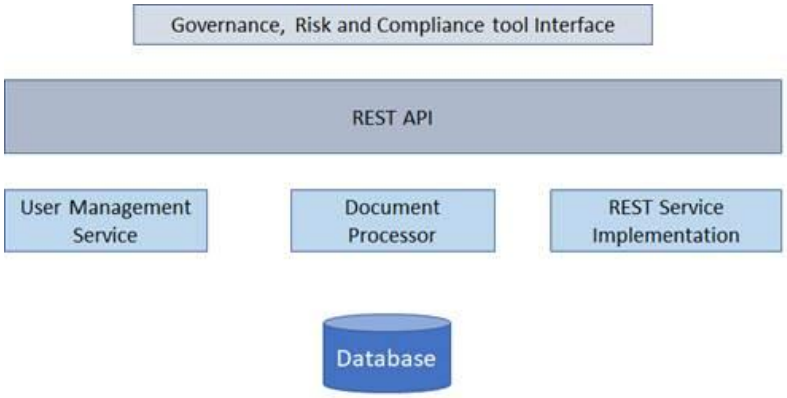


FIGURE 13: HIGH LEVEL ARCHITECTURE OF THE GOVERNANCE, RISK AND COMPLIANCE TOOL

5.2.3. PSTVA, Penetration Self-Testing and Vulnerability Assessment Services and Tools

The Penetration Self-Testing and Vulnerability Assessment (PSTVA) Services and tools will provide an evaluation of the infrastructure, identifying vulnerabilities and misconfigurations that could pose security risks. It constitutes an integrated suite designed to support micro, small, and medium enterprises in evaluating the security level and cyber resilience of their digital products. PSTVA facilitates the understanding of security weaknesses and risks associated with the digital products, analyses the result after performing the tests with suitable scenarios and test cases, and provide recommendations for overall assurance of security and resilience. In this context, it provides a practical way to validate the effectiveness of the capability to detect and prevent potential vulnerabilities in digital products, not only by examining malware tests that can affect digital products, but by also taking into consideration adversarial behaviour and tactics to exploit vulnerabilities for attack.

PSTVA service leverages a combination of automated and semi-automated tools which can be orchestrated through a central dashboard, allowing users to define their own test cases. It can conduct thorough scans to detect weaknesses across the network, applications, and systems. In this context, the PSTVA service will accumulate and consolidate the produced results, including findings, threat and vulnerability metrics, and prioritisation of countermeasures, in a unified format based on widely used standards for enumerating, describing, measuring, and encapsulating data about security weaknesses, vulnerabilities, configurations, and threats.

The PSTVA service identifies and prioritises vulnerabilities in digital products by following a structured, multi-step process that combines automated and semi-automated techniques with manual analysis and contextual security assessment:

Asset Discovery and Inventory
PSTVA begins by cataloging all relevant digital assets—such as servers, applications, and cloud resources—to ensure comprehensive coverage of the environment. This step provides visibility into what needs to be protected and assessed.

Vulnerability Identification
Using a combination of automated scanning tools and, where necessary, manual techniques, PSTVA systematically scans these assets to detect known vulnerabilities, misconfigurations, and potential security weaknesses. These tools reference extensive databases of known vulnerabilities and attack vectors, and users can define custom test cases to fit their specific needs.

Documentation and Analysis
All identified vulnerabilities are documented with details about their location, severity, and potential impact. This documentation is essential for understanding the context and scope of each issue.

Vulnerability Prioritisation
PSTVA prioritizes vulnerabilities based on several factors:

- **Severity:** Using standardised scoring systems like Common Vulnerability Scoring System (CVSS) to rate the technical severity of each vulnerability.
- **Exploitability:** Assessing whether the vulnerability can be exploited in the current environment and the likelihood of exploitation.
- **Business Impact:** Considering the criticality of the affected asset and the potential damage if the vulnerability is exploited.

Remediation Guidance
For each prioritised vulnerability, PSTVA provides actionable recommendations for remediation, including patching, configuration changes, or additional security controls if they are available.

Reporting and Monitoring
PSTVA consolidates findings into a unified report, highlighting the most critical vulnerabilities and their remediation steps. The service also supports monitoring to detect new vulnerabilities and track remediation progress, ensuring ongoing security and resilience.

Table 6 shows the PSTVA Vulnerability Identification and Prioritisation.

TABLE 6: PSTVA VULNERABILITY IDENTIFICATION AND PRIORITISATION

Step	Description
Asset Discovery	Catalog all digital assets to be assessed
Vulnerability Identification	Use automated and manual tools to detect vulnerabilities and misconfigurations
Documentation & Analysis	Record details of each vulnerability (location, severity, impact)
Prioritisation	Rank vulnerabilities by severity, exploitability, business impact, and threat intelligence
Remediation Guidance	Provide actionable steps to address each vulnerability
Reporting & Monitoring	Generate unified reports and enable monitoring for new risks

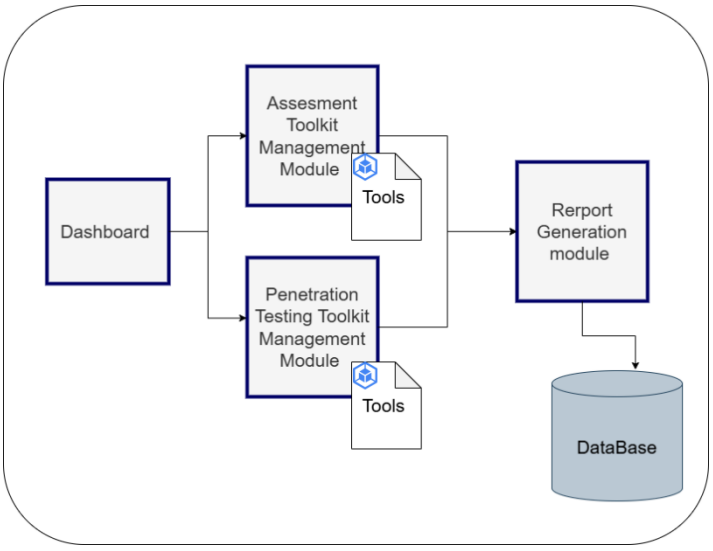


FIGURE 14: HIGH LEVEL ARCHITECTURE OF THE PENETRATION SELF-TESTING AND VULNERABILITY ASSESSMENT MODULE.

5.2.4. CAC, Conformity Assessment and Compliance Tool

The Conformity Assessment and Compliance (CAC) Tool, which is currently under development, will support users (SME) in both of (ex-ante and post-market monitoring) activities and support them to meet

the rigorous expectation from the market. The first tool capability will be automated self-assessment process with the full visualisation of the whole process which will help SME to understand the requirements and identify possible gaps. Second functionality will be technical documentation management, where the tool will asset and assist the users in the process of creation of technical documentation considering requirements coming from CRA. The tool will also have functionality to import the SBOM, in order to define what are the main components of the product (software). Post market analysis will support SME to see the status of the product, after position on the market. CAC tool will have possibilities to generate few important reports, i.e. Declaration of Conformity, Maturity Status, report about SBOM, technical documentation, etc. Tools functionality will be adapted according to users (SME) needs and feedback from the community.

This tool provides the following key features:

- Explain to the users that only basic tests should be performed to validate the cyber resilience of products with digital elements, for which a 'basic' assurance level has been considered. Products with a 'substantial' assurance level should be well-protected, covering at least vulnerabilities and weaknesses that have been disclosed and can be exploited by attackers with a certain level of expertise and skills. Thus, for the 'substantial' assurance, the testing assessment activities should ensure an adequate level of security. The user will be notified about the need for third party assessment.
- Guide the SME through the process of checking compliance with the CRA and visualize the whole process.
- Guide the SME through the process of uploading technical documentation, as well as “evidence” to justify which security requirements are fulfilled.
- Evaluate digital products based on the uploaded evidence (documentation) with assurance level.
- Generate a Statement of Conformity (DoC) as a certificate attesting to the completion of the evaluation process.
- Generate an enriched report based on the uploaded and required technical documentation, in accordance with the CRA.
- Implement Post-market Analysis/Monitoring capability with notification to the SME about new vulnerabilities or new regulatory/legal changes in CRA.

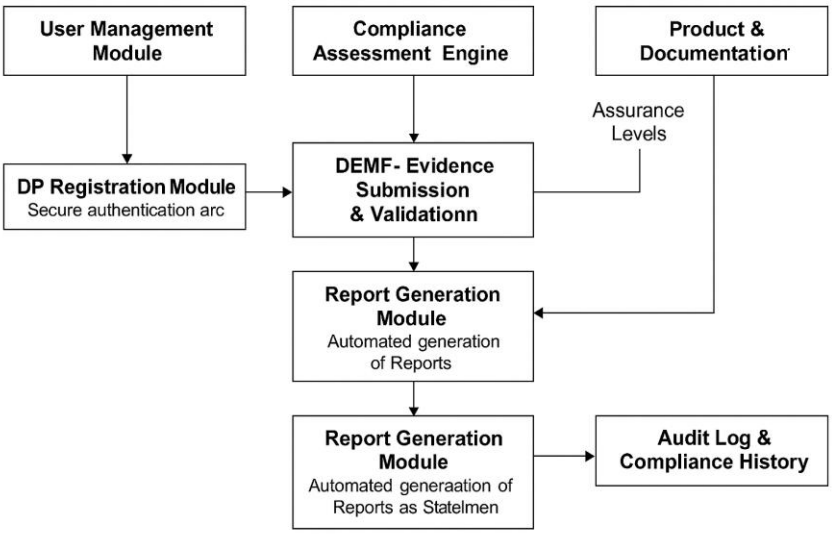


FIGURE 15: HIGH LEVEL ARCHITECTURE OF THE CAC - CONFORMITY ASSESSMENT AND COMPLIANCE MODULE

In **Figure 15** we can see high-level proposed architecture with defined modules functionality.

5.2.5. DPMA, Digital Product Maturity Assessment service

The Digital Product Maturity Assessment (DPMA) Tool is a structured and modular cybersecurity assessment instrument designed to help organizations—particularly SMEs, micro-enterprises, and start-ups—evaluate the cybersecurity maturity of their digital products. Developed in alignment with the CRA and grounded in widely accepted frameworks like ISO/IEC 27001 and ISO/IEC 27003, the DPMA Tool provides a practical, systematic, and scalable approach to identifying cybersecurity gaps and compliance readiness across product life cycles.

The tool addresses a critical market need: while regulatory and standards-based cybersecurity requirements are becoming more comprehensive, many organizations lack the time, resources, or technical capabilities to interpret and implement these requirements effectively. The DPMA Tool bridges this gap by translating high-level, vendor- and technology-neutral cybersecurity principles into actionable assessment tasks, using a threat-centric lens that reflects the evolving cyber risk landscape.

Currently implemented in Microsoft Excel. It enables users to evaluate their compliance posture against a set of cybersecurity requirements, assess threat coverage, and calculate a maturity score based on customized grading schemes. Users are guided to input detailed information on their digital product architecture, applied controls, and internal governance. Each entry is linked to source clauses (e.g., from ISO 27003), includes grading fields, and is scored using multipliers and maturity levels to reflect the importance and completeness of each item.

Beyond simple compliance checking, the DPMA Tool facilitates strategic cybersecurity planning by helping organizations understand the specific threats their products may face, the adequacy of their current protections, and the roadmap toward their target maturity level. The tool's outputs include an overall maturity score (expressed as a percentage), requirement-level performance, and customizable commentary that supports traceability.

To enhance its practical utility, the DPMA Tool includes built-in filtering, sorting, and data validation mechanisms, enabling users to focus on specific security domains, functional areas, or threat scenarios. The structure is modular, allowing for future expansion—such as integration with external threat databases, automation through VBA, or eventual migration to a cloud-based platform.

In essence, the DPMA Tool supports organizations in transforming compliance efforts into proactive cybersecurity governance, making cybersecurity maturity assessment both accessible and strategic.

5.3. Requirements

This section provides an enumeration of the technical, functional and operational requirements of the tools comprising the CURIUM Continuum. These requirements have been defined following the methodology presented in Deliverable D.2.1. The project partners have analyzed the requirements and have performed a state-of-the-art analysis on the tools needed (covering the areas of risk assessment, risk mitigation controls, identification of scope and applicability, penetration testing and vulnerability analysis and maturity assessment of products in relation to the CRA). Followingly, a mapping was performed between the tools and the requirements to be fulfilled. To facilitate the readability and the understanding of the requirements, they have been split into three different categories: technical, functional and operational requirements.

Based on available standards, the definitions for each category of these requirements are:

- Technical Requirements: Based on ISO/IEC/IEEE 24765:2017[49], a technical requirement is a requirement relating to the technology and environment, for the development, maintenance, support and execution of the software.

[49] ISO/IEC/IEEE 24765:2017 Definition 3.4187. https://www.iso.org/obp/ui/en/#iso:std:iso-iec-ieee:24765:ed-2:v1:en

- Functional Requirements: Based on ISO/IEC/IEEE 41062:2024 [50], a functional requirement is a requirement that specifies a function that a system or system component performs.
- Operational or Non-functional Requirements: Based on ISO 22163:2023 [51], an operational or non-functional requirement is a technical requirement that defines attributes serving as constraints or restrictions and ensuring the usability and effectiveness but not affecting the functionality of products and services.

The result of the mapping of tools of the CURIUM Continuum against the different requirements, as well as their connection to the preliminary results identified within the D2.1. are presented in Table 7. Within this table, the category of the requirement is indicated by its initial letter: F for Functional requirements, O for operational or non-functional requirements and T for technical requirements.

In this table, we initially present the Functional Requirements. Especially for these requirements we have included the following columns: Functional Requirement Group as depicted in D2.1., SWOT analysis including the parts of the SWOT analysis covered / treated through the incorporation of each requirement as depicted in D2.1. and the column Survey showing the result of the survey as presented in Section 3.2 of this document. With these columns we explain how our Survey and SWOT analysis drive (and lead to) the definition of our Functional Requirements.

Next, we describe the Technical Requirements. These are the requirements that are identified from a technical perspective and are linked with the setup and deployment of the various tools and services inside CURIUM. Due to the nature of these requirements, none of the analysis or mapping presented in the rest of the columns (SWOT, Survey) is applicable.

Finally, we conclude the table with the Non-Functional requirements. Likewise, for this type of requirements we only present a mapping with the SWOT analysis (in the respective column) since the rest are again not applicable.

[50] ISO/IEC/IEEE 41062:2024, Term 3.1.8. https://www.iso.org/obp/ui/en/#iso:std:81503:en

[51] on ISO 22163:2023. Definition 3.1.3.5. https://www.iso.org/obp/ui/en/#iso:std:iso:22163:ed-1:v1:en

TABLE 7: CURIUM REQUIREMENTS

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
F	FR-001	Provide step-by-step **guidance** for creating **Technical Documentation** (CRA Annex V)	CAC	**FRG4.** A stakeholder, needs to be supported in the creation of some of the technical documentation imposed by the CRA. (Question: Which are the contents of the technical documentation that need to be drafted?)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Knowledge Question 7**: I understand the concept and know of the contents of the technical documentation for a product with digital elements according to the CRA → Average answer: I have heard of it, but would need effort or help to know its details. **Challenge Question 12**: We do not know how to construct the technical documentation of the product with digital elements → Average answer: Neither agree nor disagree.
F	FR-002	**Upload** and **validate** cybersecurity **evidence** (documents, test results)	CAC	**FRG4.** A stakeholder, needs to be supported in the creation of some of the technical documentation imposed by the CRA. (Question: How the documentation already produced by the stakeholder, maps to the requirements of the CRA (Annex VIII)?)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **O1.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. So, there is a lot that could be provided to stakeholders through the capacity building activities. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Knowledge Question 7**: I understand the concept and know of the contents of the technical documentation for a product with digital elements according to the CRA → I have heard of it, but would need effort or help to know its details. **Challenge Question 12**: We do not know how to construct the technical documentation of the product with digital elements → Average answer: Neither agree nor disagree.
F	FR-003	Generate automated Technical Documentation and manage	CAC	**FRG4.** A stakeholder, needs to be supported in the creation	Taking advantage of:	**Knowledge Question 7**: I understand the concept and know of the contents

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
		Digital Product (DP) metadata (type, version, context, lifecycle)		of some of the technical documentation imposed by the CRA. (Question: Which are the contents of the technical documentation that need to be drafted?)	**S3.** Highly knowledgeable partners that support the provision of the tools. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	of the technical documentation for a product with digital elements according to the CRA → Average answer: I have heard of it, but would need effort or help to know its details. **Challenge Question 12**: We do not know how to construct the technical documentation of the product with digital elements → Average answer: Neither agree nor disagree.
F	FR-004	Generate automated EU Declaration of Conformity	CAC	**FRG4.** A stakeholder, needs to be supported in the creation of some of the technical documentation imposed by the CRA. (Question: How to draft a EU Declaration of Conformity?)	Taking advantage of: **S1.** Two cybersecurity authorities strongly related to the implementation of the EUCC and the supervision of the market related to the implementation of the CRA are involved in the project. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondents need access to technical and organizational tools to guide you through the requirements.
F	FR-005	Scan execution	PSTVA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Identifying and documenting vulnerabilities and components contained in products with digital elements)	Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Challenge Question 7**: We do not have access to tools to perform vulnerability analysis → Neither agree nor disagree. **Challenge Question 8**: We do not have access to tools to perform penetration tests → Neither agree nor disagree. **Challenge Question 16**: The tools provided by different organizations, are very costly→ Agree. **Offering Question 1**: What kind of support would help you understand

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
						and comply with CRA requirements → 50% of the respondents need access to technical and organizational tools to guide you through the requirements.
F	FR-006	Report generation	PSTVA	**FRG4.** A stakeholder, needs to be supported in the creation of some of the technical documentation imposed by the CRA. (Question: How to draft a EU Declaration of Conformity?)	Taking advantage of: **S1.** Two cybersecurity authorities strongly related to the implementation of the EUCC and the supervision of the market related to the implementation of the CRA are involved in the project. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondents need access to technical and organizational tools to guide you through the requirements.
F	FR-007	Report access and management	PSTVA	**FRG4.** A stakeholder, needs to be supported in the creation of some of the technical documentation imposed by the CRA. (Question: How to draft a EU Declaration of Conformity?)	Taking advantage of: **S1.** Two cybersecurity authorities strongly related to the implementation of the EUCC and the supervision of the market related to the implementation of the CRA are involved in the project. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondents need access to technical and organizational tools to guide you through the requirements.
F	FR-8	Provide the ability for the user to assess their performance on specific cybersecurity controls and identify the level of these	DPMA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential**	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. Responding to:	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
		controls against a structured scale.		**requirements** imposed by the CRA. (Question: Identifying controls (measures) for treating cybersecurity risks based on their desired level of residual risk)	**W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-9	Provide the ability to identify possible mitigating measures to threats.	DPMA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Identifying controls (measures) for treating cybersecurity risks based on their desired level of residual risk)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-10	Facilitate the decision-making activities of the users, related to risk mitigation actions.	DPMA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Identifying controls (measures) for treating cybersecurity risks based on their desired level of residual risk)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements →

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
						50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-011	Support in the establishment of a roadmap towards achieving the desired maturity level of specific controls.	DPMA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Identifying controls (measures) for treating cybersecurity risks based on their desired level of residual risk)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-012	Allow tracking of achieved vs. targeted states.	DPMA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Identifying controls (measures) for treating cybersecurity risks based on their desired level of residual risk)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. Responding to: **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-013	Extract the information of possible controls to be implemented.	DPMA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA.	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. Responding to:	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Challenge Question 5:** We do not have access to tools which would assist us in

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
				(Question: Identifying controls (measures) for treating cybersecurity risks based on their desired level of residual risk)	**W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. As such, they may be unable to fully articulate their needs at this stage.	the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-014	The Risk Management (RM) suite shall allow users to decompose ICT product and its corresponding individual assets	DPRA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Assessing the cybersecurity risks associated with a product with digital elements)	Taking advantage of: **S5.** The tools comprising the CURIUM Continuum are based on standards. **O4.** A great portion of the products with digital elements are composite systems. The manufacturers should be able to decompose their systems and populate an SMOB to support further conformity assessment processes.	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-015	The specification of security objectives and corresponding security requirements for ICT product shall be specified by RM suite	DPRA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Assessing the cybersecurity risks associated with a product with digital elements)	Taking advantage of: **S5.** The tools comprising the CURIUM Continuum are based on standards. **O4.** A great portion of the products with digital elements are composite systems. The manufacturers should be able to decompose their systems and populate an SMOB to support further conformity assessment processes.	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements →

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
						50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-016	The identified ICT products shall be decomposed to formulate an ICT product-based asset inventory	DPRA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Assessing the cybersecurity risks associated with a product with digital elements)	Taking advantage of: **S5.** The tools comprising the CURIUM Continuum are based on standards. **O4.** A great portion of the products with digital elements are composite systems. The manufacturers should be able to decompose their systems and populate an SMOB to support further conformity assessment processes.	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-017	The RM suite shall rely on open intelligence based on wide-known security taxonomies and open repositories (e.g. NIST NVD, CAPEC MITRE) to identify threats, vulnerability and risks for each ICT product.	DPRA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Question: Assessing the cybersecurity risks associated with a product with digital elements)	Taking advantage of: **S5.** The tools comprising the CURIUM Continuum are based on standards. **O4.** A great portion of the products with digital elements are composite systems. The manufacturers should be able to decompose their systems and populate an SMOB to support further conformity assessment processes.	**Challenge Question 14:** We find it very difficult to locate / get expert advice or direction on CRA compliance → Agree **Offering Question 1**: What kind of support would help you understand and comply with CRA requirements → 50% of the respondent's technical assistance (for the implementation of relevant security controls)
F	FR-018	The vulnerabilities related to specific ICT products shall identify and prioritized for the risk level calculation.	DPRA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Identifying and documenting vulnerabilities and	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **S5.** The tools comprising the CURIUM Continuum are based on standards.	**Challenge Question 7**: We do not have access to tools to perform vulnerability analysis → Neither agree nor disagree. **Challenge Question 8**: We do not have access to tools to perform penetration tests → Neither agree nor disagree.

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
				components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products)		**Challenge Question 16**: The tools provided by different organizations, are very costly→ Agree.
F	FR-019	The RM suite shall illustrate interdependence among ICT products with threat and vulnerabilities for visualization of the product cyber dependencies and calculate both individual and cascading risk	DPRA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Identifying and documenting vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **S5.** The tools comprising the CURIUM Continuum are based on standards.	**Knowledge Question 5**: I understand the concept and details of the essential cybersecurity requirements mandated for products with digital elements → I have heard of it, but would need effort or help to know its details **Challenge Question 16**: The tools provided by different organizations, are very costly→ Agree.
F	FR-020	The RM suite shall publish the outcome of risk assessment through a comprehensive risk and control list	DPRA	**FRG3.** A stakeholder, needs to be **guided** in the **performance** of some of the **essential requirements** imposed by the CRA. (Extracting an outcome (documented) on cybersecurity risks associated	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **S5.** The tools comprising the CURIUM Continuum are based on standards.	**Challenge Question 5:** We do not have access to tools which would assist us in the risk assessment process → Neither agree nor disagree. **Challenge Question 16**: The tools provided by different organizations, are very costly→ Agree.

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
				with a product with digital elements)		
F	FR-021	The questionnaire shall include several sections which is associated with key CRA areas related requirements including cybersecurity requirements for products with digital elements, Vulnerability handling requirements, and Class I, Class II and Critical Class	CyReA	**FRG2.** A stakeholder, needs to be **informed** on the **requirements** for products with digital elements (Questions: Which are the essential cybersecurity requirements set out in Part I of Annex I of the CRA that their products with digital elements need to meet. Which are the processes the need to put in place to comply with the essential cybersecurity requirements set out in Part II of Annex I of the CRA. Which are their obligations (based on their type) regarding conformity assessment.)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. Responding to: **T4.** The requirements of the CRA and the activities related to conformity assessment are not straight forward and, in some cases, difficult to understand.	**Knowledge Question 5**: I understand the concept and details of the essential cybersecurity requirements mandated for products with digital elements → I have heard of it, but would need effort or help to know its details **Knowledge Question 6**: I understand the concept and details of conformity assessment options for a product with digital elements → I have heard of it, but would need effort or help to know its details **Challenge Question 10:** We do not know which are the essential requirements that the product with digital elements needs to comply with → Neither agree or disagree **Challenge Question 11:** We do not know which options exist in relation to the conformity assessment of products with digital elements→ Neither agree or disagree
F	FR-022	The response of each question shall be characterized by the order of their appearance in the context of a question	CyReA	**FRG1.** A stakeholder, needs to be able to **identify** if they, for one or more products, are within the **scope of the CRA**. (Questions: Which type of economic operator they are. If they have a product with digital elements, following the	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **O2.** Some of the partners of the project are already involved in the ongoing standards developing activities related to the CRA and possible feedback of the	**Knowledge Question 1:** I know what is the Scope and Requirements of the Cyber Resilience Act (CRA). Answer: I have heard of it, but would need effort or help to know its details **Knowledge Question 2:** I know the definition and can distinguish between products with digital elements.

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
				existing definition. What is the classification category of their product with digital elements. If they belong in an exception of the CRA.)	project could be provided to that community also. Responding to: **T4.** The requirements of the CRA and the activities related to conformity assessment are not straight forward and, in some cases, difficult to understand.	Answer: I have heard of it, but would need effort or help to know its details **Knowledge Question 3:** I know the exceptions to the application of the CRA. Answer: I have heard of it, but would need effort or help to know its details. **Challenge Question 2:** We have limited knowledge of the CRA scope and requirements → Neither Agree or Disagree **Challenge Question 3:** We do not know if our organization is in scope of the CRA → Neither Agree or Disagree
F	FR-023	Based on the answers to the questions, the user should be able to understand if they fall within the scope of the CRA at least one of their products with digital elements.	CyReA	**FRG1.** A stakeholder, needs to be able to **identify** if they, for one or more products, are within the **scope of the CRA**. (Questions: Which type of economic operator they are. If they have a product with digital elements, following the existing definition. What is the classification category of their product with digital elements. If they belong in an exception of the CRA.)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **O2.** Some of the partners of the project are already involved in the ongoing standards developing activities related to the CRA and possible feedback of the project could be provided to that community also. Responding to: **T4.** The requirements of the CRA and the activities related to conformity assessment are not straight forward and, in some cases, difficult to understand.	**Knowledge Question 1:** I know what is the Scope and Requirements of the Cyber Resilience Act (CRA). Answer: I have heard of it, but would need effort or help to know its details **Knowledge Question 2:** I know the definition and can distinguish between products with digital elements. Answer: I have heard of it, but would need effort or help to know its details **Knowledge Question 3:** I know the exceptions to the application of the CRA. Answer: I have heard of it, but would need effort or help to know its details. **Challenge Question 2:** We have limited knowledge of the CRA scope and requirements → Neither Agree or Disagree

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
						Challenge Question 3: We do not know if our organization is in scope of the CRA → Neither Agree or Disagree
O	FR-024	ICT product shall be clearly categorized into four distinct classes including Default, Important Class I, Important Class II and Critical Class	CyReA	**FRG1.** A stakeholder, needs to be able to **identify** if they, for one or more products, are within the **scope of the CRA**. (Questions: Which type of economic operator they are. If they have a product with digital elements, following the existing definition. What is the classification category of their product with digital elements. If they belong in an exception of the CRA.)	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **O2.** Some of the partners of the project are already involved in the ongoing standards developing activities related to the CRA and possible feedback of the project could be provided to that community also. Responding to: **T4.** The requirements of the CRA and the activities related to conformity assessment are not straight forward and, in some cases, difficult to understand.	**Knowledge Question 1:** I know what is the Scope and Requirements of the Cyber Resilience Act (CRA). Answer: I have heard of it, but would need effort or help to know its details **Knowledge Question 2:** I know the definition and can distinguish between products with digital elements. Answer: I have heard of it, but would need effort or help to know its details **Knowledge Question 3:** I know the exceptions to the application of the CRA. Answer: I have heard of it, but would need effort or help to know its details. **Challenge Question 2:** We have limited knowledge of the CRA scope and requirements → Neither Agree or Disagree **Challenge Question 3:** We do not know if our organization is in scope of the CRA → Neither Agree or Disagree
O	FR-025	The questionnaire response shall be correctly documented as a supporting document for the compliance achievement.	CyReA	**FRG1.** A stakeholder, needs to be able to **identify** if they, for one or more products, are within the **scope of the CRA**. (Questions: Which type of economic operator they are. If they have a product with digital elements, following the existing definition. What is the	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **O2.** Some of the partners of the project are already involved in the ongoing standards developing activities related to the CRA and possible feedback of the project could be provided to that community also.	**Knowledge Question 1:** I know what is the Scope and Requirements of the Cyber Resilience Act (CRA). Answer: I have heard of it, but would need effort or help to know its details **Knowledge Question 2:** I know the definition and can distinguish between products with digital elements.

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
				classification category of their product with digital elements. If they belong in an exception of the CRA.)	Responding to: **T4.** The requirements of the CRA and the activities related to conformity assessment are not straight forward and, in some cases, difficult to understand.	Answer: I have heard of it, but would need effort or help to know its details **Knowledge Question 3:** I know the exceptions to the application of the CRA. Answer: I have heard of it, but would need effort or help to know its details. **Challenge Question 2:** We have limited knowledge of the CRA scope and requirements → Neither Agree or Disagree **Challenge Question 3:** We do not know if our organization is in scope of the CRA → Neither Agree or Disagree
T	TR-001	HTTPS/TLS 1.3 must be used in order to access the tools	All	N/A	N/A	N/A
T	TR-002	SSO will be used for seamless access across the tools	All	N/A	N/A	N/A
T	TR-003	Containerization and independent deployment of the tool(s)	All	N/A	N/A	N/A
T	TR-004	Data Storage for evidence will be encrypted and immutable	CAC	N/A	N/A	N/A
T	TR-005	All user actions with timestamps, geo-location will be stored	CAC	N/A	N/A	N/A
T	TR-006	Import & parse CycloneDX, SPDX, and JSON SBOM formats	CAC	N/A	N/A	N/A
T	TR-007	API integration with NVD, OSV.dev, and/or OpenCVE, MISP	CAC	N/A	N/A	N/A
T	TR-008	All formats will be in PDF, Word, XML for technical documentation and reports	CAC	N/A	N/A	N/A

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
T	TR-009	Secure document storage with version control and encryption (DEMF)	CAC	N/A	N/A	N/A
T	TR-010	Local Execution	PSTVA	N/A	N/A	N/A
T	TR-011	Browser-based UI	PSTVA	N/A	N/A	N/A
T	TR-012	Container Caching	PSTVA	N/A	N/A	N/A
T	TR-013	Support hybrid scan targets: local filesystem, Docker images, cloud registries, and web URLs with secure credential handling.	PSTVA	N/A	N/A	N/A
T	TR-014	Able to view through Microsoft Excel 2016 or later. Operable on Windows and macOS.	DPMA	N/A	N/A	N/A
T	TR-016	Ability to use (Excel) functions: SUM, IF, COUNTIF, XLOOKUP, INDEX/MATCH, and more in order to filter through and select needed results. Conditional formatting dynamically updates cell visuals based on rule conditions (e.g., scores of "0" appear red).	DPMA	N/A	N/A	N/A
T	TR-017	Integrity. Sheet-level protection and locked formula cells to maintain integrity. Data validation rules to restrict incorrect entry (e.g., dropdowns for grading).	DPMA	N/A	N/A	N/A
O	NFR-001	The system should be accessible via any browser	All	N/A		N/A
O	NFR-002	The tools must be usable by non-cybersecurity experts/non-technical people (SMEs)	All	N/A	Taking advantage of / responding to **O1. / W3** Limited information about the CRA and its requirements is	N/A

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
					known by the affected economic operators, especially the ones that fall within the SME definition. So, there is a lot that could be provided to stakeholders through the capacity building activities.	
O	NFR-003	Each tool must provide error handling and guided help messages	All	N/A	Taking advantage of / responding to **O1. / W3** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. So, there is a lot that could be provided to stakeholders through the capacity building activities.	N/A
O	NFR-004	The system must be GDPR compliant (data processing, retention, consent)	All	N/A	Responding to **T5.** Information of the CURIUM Continuum user (and their interaction with the system) could be accessed by unauthorized parties, making the user more reluctant to use the tools.	N/A
O	NFR-005	The dashboard will have clean, simple UI	All	N/A	Taking advantage of / responding to **O1. / W3** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition. So, there is a lot that could be provided to stakeholders through the capacity building activities.	N/A
O	NFR-006	The system should allow easy updates and patches	DPRA CAC PSTVA	N/A	Responding to **T1.** Key issues related to the implementation of the CRA are still currently being defined by the European Policy makers.	N/A

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
O	NFR-007	The system should be resource efficient	PSTVA	N/A	Responding to **T2.** Implementing a resource efficient system will offer an advantage over alternative solutions.	N/A
O	NFR-008	Enforce Least privilege execution to avoid privileged containers unless necessary.	PSTVA	N/A	Responding to **T5.** Implementing least privilege execution reduces the attack surface of the system. Avoiding privileged containers ensures better isolation and limits the impact of any potential breach, reassuring users about the security of their data.	N/A
O	NFR-009	Provide user manuals for CLI and Web UI explaining installation, configuration, and usage.	PSTVA	N/A	Taking advantage of / responding to **O1/ W3** comprehensive manuals will lower the knowledge barrier for SMEs and other stakeholders.	N/A
O	NFR-010	Maintain detailed technical documentation including architecture.	PSTVA	N/A	Responding to **T1** Key issues related to the implementation of the CRA are still currently being defined by the European Policy makers.	N/A
O	NFR-011	RM suite shall be flexible enough to allow the legitimate users to use the DPR service with strong authentication and authorization practice.	DPRA	N/A	Responding to **T5.** Information of the CURIUM Continuum user (and their interaction with the system) could be accessed by unauthorized parties, making the user more reluctant to use the tools.	N/A
O	NFR-012	The Dashboard of RM suite shall be a clean, intuitive interface that makes it easy for users to find information and perform tasks without extensive training.	DPRA	N/A	Taking advantage of / responding to **O1. / W3** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the SME definition.	N/A
O	NFR-013	The RM suite shall allow the user to connect through	DPRA	N/A	Responding to **T5.** Information of the CURIUM Continuum user (and their interaction	N/A

Cat.	ID	Requirements Description	CURIUM Technical Tool	Functional Requirement Group	SWOT	Survey
		standard browser and securely store risk assessment outcome.			with the system) could be accessed by unauthorized parties, making the user more reluctant to use the tools.	
O	NFR-014	The RM suite shall provide a high degree of interoperability to integrate the data from the open intelligence in real time.	DPRA	N/A	Responding to: **W5.** The CURIUM Continuum is not a fully integrated platform of tools. It is a compilation of 5 components not interlinked.	N/A
O	NFR-015	The tool shall allow access to legitimate users to provide response to the questionnaire	CyReA	N/A	Responding to **T5.** Information of the CURIUM Continuum user (and their interaction with the system) could be accessed by unauthorized parties, making the user more reluctant to use the tools.	N/A
O	NFR-016	The tool shall provide a systematic list of questions related to the cyber resilience assessment of the products with digital elements through an on-line wizard based interactive capability to allow the user to respond to the relevant questions	CyReA	N/A	Taking advantage of: **S3.** Highly knowledgeable partners that support the provision of the tools. **O2.** Some of the partners of the project are already involved in the ongoing standards developing activities related to the CRA and possible feedback of the project could be provided to that community also. Responding to: **T4.** The requirements of the CRA and the activities related to conformity assessment are not straight forward and, in some cases, difficult to understand.	N/A

6. Knowledge and Capacity Services

The CURIUM project is committed to enhancing the resilience, security, privacy, and accountability of hardware and software products with digital elements. By developing a Compliance Continuum (a set of cybersecurity-oriented tools and services for information, guidance, security testing, and compliance facilitation), CURIUM simplifies and automates the regulatory alignment process, particularly with the CRA. This approach is essential for addressing the cybersecurity challenges of highly interconnected digital products while reducing the cost and time required for certification.

A key dimension of CURIUM's mission is to empower European SMEs, particularly micro and small enterprises, in their regulatory alignment journeys by strengthening their cybersecurity competencies. Through training, security testing, consulting, and awareness-raising activities, the project will equip SMEs with the necessary knowledge and tools to conduct effective self-assessments and prepare their products for third-party certification. 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.

6.1. Key pillars of the Capacity Building strategy

CURIUM's Capacity Building strategy is based on five pillars:

Pillar 1: Training and Education

CURIUM will deliver training material in the form of documentation for the services of the CURIUM Compliance continuum and tools, as well as material and guidelines for relevant EU policies and regulations. The material will combine existing material, platforms and activities offered by the consortium partners as well as external sources. It is not only about compiling and designing training material but also actual delivery of the education programs.

As part of the planning activity, a Training Activity Catalogue (TAC) is established and maintained to collect and summarize the project's multifaceted training efforts. The Training Activity Catalogue is structured as follows:

TABLE 8: TRAINING ACTIVITY CATALOGUE TEMPLATE

COURSE TITLE	RESPONSIBLE	DELIVERY MONTH	DESCRIPTION	DELIVERY MODE

Where Delivery mode could be an on-site / on-line / hybrid course with lectures, coursework & assessment, a webinar with presentations and panel discussions, a workshop etc. The initial version of the TAC includes training activities related to a./ EU Policies and Regulations and b./ CURIUM Tools and Services. Continuous engagement with targeted stakeholders and analysis of the results of the performed survey which aimed to elicit the stakeholders' needs and requirements, in combination with the skills and knowledge brought forward by the project partners, will enable us to expand and update our catalogue and make it relevant and valuable. In the scope of the project's networking and clustering activity, It is planned that part of the training activities will be organised in collaboration with other running cybersecurity projects, as well as organisations and initiatives which offer trainings in the area.

Pillar 2: Experimentation and Testing

CURIUM will provide SMEs access to testing infrastructures for compliance validation and technical experimentation. CURIUM partner p-NET has developed and operates an end-to-end experimentation platform of smart 5G and beyond networks and services, from the on-boarding of applications to orchestration and provisioning of experiment resources including control and monitoring capabilities during the experiment. Operating under the Network Slice as a Service (NSaaS) model, the facility offers customized network slices

tailored to the needs of different verticals. Each vertical utilizes these slices to conduct trials for a range of use cases, assessing and documenting KPIs under diverse network conditions. p-NET's Testing and Experimentation Facility (TEF) is based on a private 5G stand-alone core network with the robustness, reliability, and standards' conformance level of a commercial public network and the capability to support a range of activities such as: hosting equipment vendors for conformance testing; developing and testing new 5G/6G functionality; performing KPI Measurements and cybersecurity assessments; carrying out end-to-end trials; supporting hands-on training.

Indicative Testing Scope includes:

- Full End-to-End Service Functionality
    - Verify that the service flow—from device to application to backend—operates as intended
- QoS and SLA Enforcement
    - Confirm the network enforces quality of service rules under varying conditions e.g. video call quality during network congestion
- Security & Access Control
    - Test user/device authentication, encryption, and data protection
- Failure and Recovery
    - Verify service resilience in case of node or link failure
- Regulatory Compliance
    - Ensure 5G SA applications comply with industry regulations, including data privacy, security standards, and national telecom guidelines
- Security
    - Perform vulnerability assessments and penetration testing on 5G infrastructure, focusing on high-risk scenarios that cannot be tested in a commercial network.

Pillar 3: Consulting and Support Services

The project will design and develop a Consulting and Support Framework, which will

- Define the purpose and scope of advisory services
- Identify key experts and advisors within the consortium
- Identify targeted stakeholders
- Develop guidelines for offering advisory services
- Define how to promote the services and engage stakeholders
- Define how they will be delivered.

The scope of the services includes tailored advisory and technical assistance to SMEs for CRA implementation.

Pillar 4: Awareness and Knowledge Transfer

The activity relates to dissemination of cybersecurity best practices and regulatory guidance, engaging stakeholders and contributing to knowledge exchange between actors from different sectors (government, policy makers, academia, industry, etc.) and will be implemented in close collaboration T5.1., which is devoted to the project's dissemination and communication activity.

Pillar 5: Collaboration and Sustainability

The activity focuses on strengthening engagement with European cybersecurity institutions and initiatives (such as ENISA, ECCC, NCCs, etc.) to ensure long-term impact. To streamline it, a list of such institutions and initiatives together with the person responsible for establishing the relation and maintaining the collaboration is created.

TABLE 9: COLLABORATION TABLE TEMPLATE

#	Institution / Initiative	Description of Scope	Link	Forms of collaboration	Partner Responsible	Progress Made

6.2. Capacity Building implementation plan

For the strategy implementation, the Capacity Building plan is structured in two main phases:

Phase 1 - Definition of the plan. Runs from M1 to M6 and its outcome are documented in the present deliverable, and

Phase 2 - Implementation & Monitoring of the Capacity Building activity and will run from M7 to M18

In the following, the Objectives and Key Actions of the two phases are presented.

Phase 1: Definition (M1-M6, January - June 2025)

Objectives:

- Establish the detailed Capacity Building plan.
- Identify key stakeholders and their training needs.
- Start developing partnerships with relevant EU bodies (ENISA, ECCC, NCCs, etc.) and initiatives (EDIHs, related projects, networks of SMEs, etc).
- Define the scope and structure of training programs – events and supporting materials.

Key Actions:

1. Needs assessment & Stakeholder mapping

- Survey SMEs and industry stakeholders on cybersecurity gaps: using the input from the CURIUM survey (detailed in section 3.2 of the present document), engaging with stakeholders at different events, and industry research, we identified key user groups, their training needs, and the type of support they require, ensuring the plan reflects end-user perspectives.
- Define Personas and user requirements for training and support services.

2. Training Program Design

- Review existing training resources from consortium partners and external sources.
- Define structured training courses, content formats and delivery methods: different Personas will have different learning preferences. Informed by the CURIUM survey findings, which highlighted a demand for practical and interactive formats, the training will prioritize hands-on workshops, live online courses, and self-assessment guides. We will also collaborate with authoritative providers like National Cybersecurity Authorities and ENISA, as preferred by stakeholders, to enhance credibility and trust. A combination of content formats will ensure accessibility and engagement.
- Issue certificate of attendance.

3. Testing and Experimentation Framework

- Promote the Testing and Experimentation Facility and Services provided by p-NET and encourage SMEs to provide their testing requirements and use it.
- Define compliance verification testing scenarios.

4. Consulting and Support Framework

- Identify key experts and advisors within the consortium.
- Develop guidelines for providing advisory services. The survey results identified a need for technical assistance and consulting, particularly among manufacturers. Relevant identified needs analysis will guide the organization and scope of these services.

5. Awareness and Knowledge Transfer Plan

- Develop a dissemination and communication strategy to engage SMEs and other stakeholders, in collaboration with WP5, plan and implement numerous outreach events (information days, webinars, workshops etc.).

6. Collaboration and Sustainability Roadmap

- Identify synergies with ongoing EU initiatives (Cybersecurity Skills Academy).
- Explore partnerships with EDIHs and National Authorities for long-term impact.

Phase 2: Implementation & Monitoring (M7-M18, July 2025 - June 2026)

Objectives:

- Deliver and evaluate training programs.
- Facilitate access to testing and experimentation.
- Provide ongoing consulting and support services.
- Organize awareness-raising events and workshops.
- Networking and establishment of strategic collaborations.
- Monitor KPIs and adjust strategy for impact maximization.

Key Actions:

1. Training Delivery

- Provide at least 10 training sessions (external, from consortium members or developed inside the project)
- Engage SMEs through interactive workshops and e-learning modules.
- Integrate real-world case studies and practical compliance exercises (KPI>5).

2. Testing and Experimentation Rollout

- Open p-NET's infrastructure for SME testing. The CURIUM survey highlighted SMEs' need for practical testing support, which will inform the design of testing scenarios to ensure they address real-world compliance challenges.

3. Consulting and Support Services

- Launch advisory sessions for SMEs on CRA compliance.
- Provide hands-on support.

4. Awareness and Knowledge Dissemination

- Organize 1 scientific workshop and 2 information days.
- Develop and distribute best practice guides (KPI>5).

5.Networking and Strategic Collaborations

- Engage with EU and international security and networking bodies, agencies and organizations (KPI>10)

- Collaborate with similarly themed projects and initiatives identified (KPI>5), and perform joint activities such as co-organized workshops (>2).

6. Monitoring & Evaluation

- Track KPIs
- After each training, conduct feedback surveys and refine training content/format (aim to achieve 90% positive evaluation of the training material by trainees).

6.3. Expected Outcomes

The expected outcomes from the implementation of the Capacity Building Plan and the provision of relevant Services are summarized in the following list:

- Enhanced cybersecurity knowledge among SMEs.
- Increased adoption of CRA compliance measures.
- Stronger collaboration between SMEs, regulators, and research institutions.
- Sustainable capacity-building framework for continued impact beyond the project timeline.
- Integration with EIT Digital's ecosystem: Leverage existing networks to continue training and support activities.
- Engagement with EU Cybersecurity Skills Academy: Explore long-term partnerships for skill-building initiatives.
- Collaboration with National Authorities: Strengthen regulatory knowledge-sharing mechanisms.
- Open-source contributions: Encourage the use and expansion of project-developed cybersecurity resources.

7. CURIUM Compliance Continuum Blueprint Design

Following the detailed technical specifications of the five CURIUM tools and services outlined in Section 5, this section presents the architecture of the modular interplay of these components within the comprehensive CURIUM compliance ecosystem. The design of this interplay establishes a seamless compliance continuum that addresses the full spectrum of CRA regulatory requirements.

7.1. Systematic Guidance for CE Marking Compliance

The ongoing digital transformation has resulted in an increasingly complex cybersecurity threat landscape, concurrent with evolving business requirements and market dynamics. This environment necessitates the establishment of comprehensive security governance frameworks that encompass digital products throughout their complete development lifecycle, spanning from initial conceptual design through implementation phases to final production deployment. Such frameworks must ensure adherence to all essential security requirements at each developmental stage while facilitating transparent communication of security attributes, thereby guaranteeing both product integrity and secure end-user implementation.

The main goal of the CURIUM compliance ecosystem is to function as a centralized environment specifically designed to serve SMEs operating as manufacturers and owners of ICT products. The primary objective is to provide systematic guidance throughout the CE marking compliance process, ensuring that manufacturers and product owners can demonstrate that their products have undergone appropriate assessment procedures and comply with essential cybersecurity requirements applicable to incorporated digital components.

The CE marking serves as a formal declaration indicating that the requisite evaluation processes have been completed and represents the manufacturer's attestation of product compliance with applicable regulatory standards, while recognizing that such marking constitutes a declaration rather than definitive proof of compliance.

The implementation of the CRA significantly expands the existing cybersecurity legislative framework, thereby enhancing the CE marking process through the establishment of specific regulatory obligations. These regulations apply to all economic operators throughout the supply chain, including EU-based manufacturers as well as importers and distributors of goods within the European Union, thereby facilitating the free movement of compliant products across the European internal market.

7.2. The Blueprint Design

Within this regulatory and technological context, the CURIUM project establishes a foundational framework for achieving compliance of digital products with cybersecurity essential requirements as mandated by current and emerging European legislation. The project's systematic approach addresses the comprehensive needs of economic operators seeking to navigate the complex compliance landscape effectively.

Figure 16 illustrates the preliminary architectural schematic of the Compliance Continuum, demonstrating the CURIUM technical tools as components that constitute the modular ecosystem.

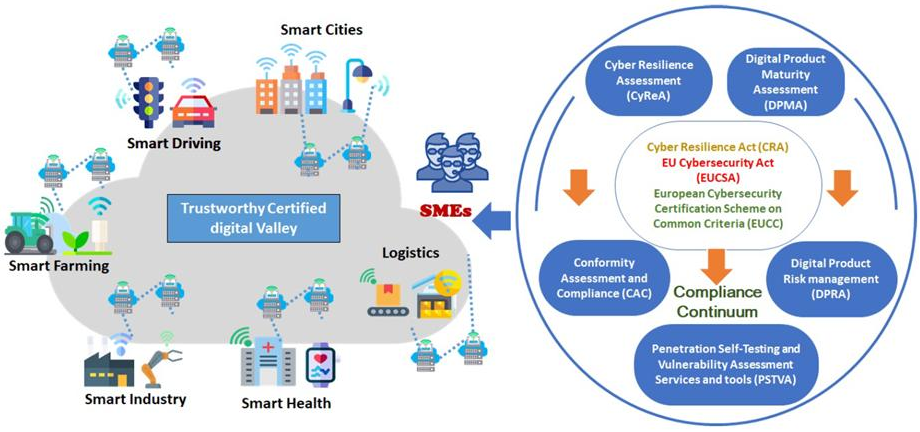


FIGURE 16: CURIUM CONTINUUM SUPPORTING THE EUROPEAN SMES AND INDUSTRY: PRELIMINARY SCHEMATIC

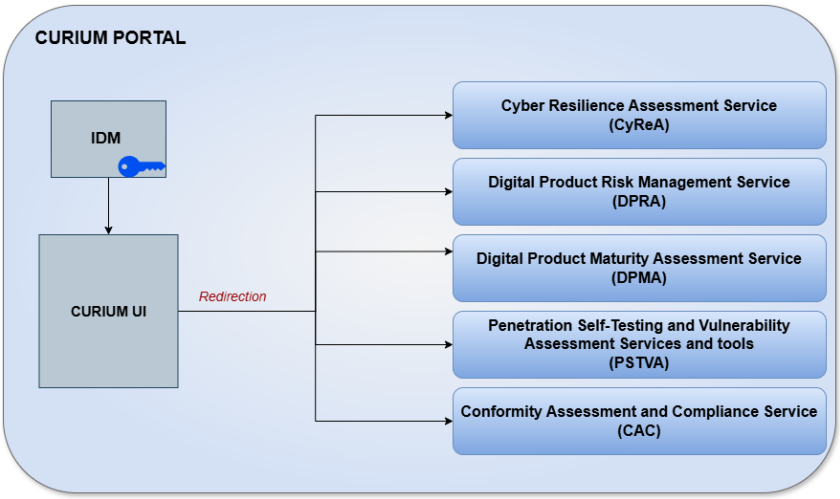


FIGURE 17: CURIUM COMPLIANCE CONTINUUM BLUEPRINT DESIGN

As illustrated in **Figure 17**, the CURIUM Compliance Continuum provides authorized stakeholder organizations, including SMEs, with comprehensive access to the CURIUM User Interface (CURIUM UI). The CURIUM UI functions as the central access portal that seamlessly connects the framework's five core technical assessment tools: CyReA, DPRA, DPMA, PSTVA, and CAC (ref. To Section 5 for the detailed description of these tools). These technical tools are architected as modular components within the CURIUM ecosystem, designed without mandatory interdependencies to ensure maximum flexibility and adaptability to diverse organizational contexts. The toolkit specifically addresses cyber-resilience conformity assessment requirements as stipulated under the CRA regulatory framework. Specifically, the CURIUM Compliance Continuum primarily targets the systematic verification and assessment of non-critical digital products, as depicted **Figure 18**, thereby supporting European SMEs in achieving regulatory compliance while maintaining operational efficiency and resource optimization.

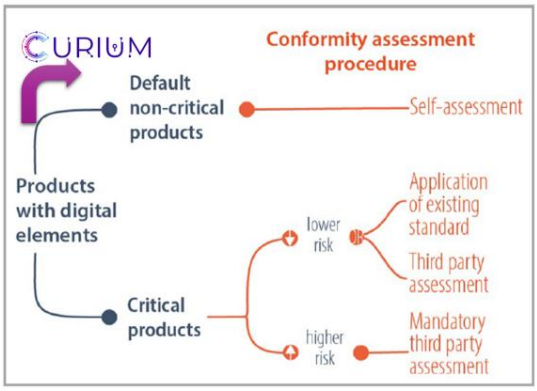


FIGURE 18: CYBER-RESILIENCE CONFORMITY ASSESSMENT BORROWED FROM THE EU-CRA

Particularly, the framework provides flexible implementation pathways for its five technical tools, allowing stakeholders to adapt their approach based on specific organizational needs and regulatory contexts. While the framework does not mandate a rigid sequential application of all tools, it aligns with EC recommendations regarding systematic risk-based approaches to digital product compliance.

In accordance with EC guidance, the CURIUM Compliance Continuum framework prioritizes initial risk categorization of digital products as a foundational step. CyReA tool has been specifically developed to address this requirement (Section 5.2.2), though its application remains voluntary for participating SMEs to ensure maximum accessibility and adoption flexibility.

Building upon the initial categorization phase, the CURIUM Compliance Continuum offers comprehensive self-assessment capabilities through its modular technical toolkit. Following EC recommended practices, organizations are advised to proceed systematically through complementary assessment phases: risk evaluation via the DPRA tool (Section 5.2.1), verification of product-specific essential requirements through the DPMA (Section 5.2.5), validation of vulnerability handling protocols using the PSTVA tool (Section 5.2.3), and completion of conformity assessment procedures through the CAC tool (Section 5.2.4).

This structured yet adaptable approach ensures alignment with European regulatory frameworks while maintaining the flexibility essential for diverse SME operational contexts and resource constraints.

The comprehensive assessment methodology generates detailed reporting outputs through each of the five technical tools, providing organizations with systematic documentation of identified vulnerabilities and compliance gaps. To elaborate on one, the DPRA delivers capabilities by quantifying threat levels and risk assessments, enabling organizations to implement proportionate and targeted mitigation strategies aligned with their specific risk profiles.

The CURIUM Compliance Continuum framework is further strengthened by its foundational Knowledge and Capacity Services component, which provides essential support for effective tool deployment and regulatory compliance. Supplemented by the Training Activity Catalogue (TAC), this critical pillar of the ecosystem is comprehensively detailed in Section 6, encompassing training resources, technical guidance, and capacity-building initiatives designed to maximize the framework's accessibility and effectiveness for European SMEs navigating the evolving cybersecurity regulatory landscape.

7.3. Open-Source Indicative Tools

While the CURIUM Compliance Continuum leverages open-source software components within each of its five technical tools, its primary advantage lies in the systematic integration and contextual adaptation of these resources for European regulatory compliance requirements. Unlike disparate open-source solutions that require extensive configuration and regulatory interpretation, the CURIUM framework provides a cohesive ecosystem specifically designed to address the CRA and CE marking obligations for SMEs.

This integrated approach directly addresses documented market needs. According to Table 83 of D2.1 CRA and EU certification analysis towards a European Trustworthy Certified Digital Valley, survey findings reveal substantial demand for comprehensive compliance support: 49 of 91 respondents require technical assistance for implementing relevant security controls, 46 seek access to technical and organizational tools for navigating CRA requirements, and 41 need tools specifically designed to facilitate CRA implementation. These results demonstrate significant market interest in solutions that can effectively interpret and implement CRA requirements.

To contextualize the CURIUM framework's positioning within the existing tool landscape, **Table 10** lists indicative open-source tools and their capabilities. This list illustrates the gap between available standalone solutions and the integrated compliance support that SMEs require for effective CRA adherence.

TABLE 10: INDICATIVE OPEN-SOURCE TOOLS WITH CAPABILITY DESCRIPTIONS.

#	Tool		
1	**Nmap**	Description	Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.
		Dependencies	Npcap for Windows (included in Nmap OEM)
		Integration	XML output parsing.
		Owner	Insecure.org (Nmap Project)
		Licence	Nmap Public Source License (based on GNU GPLv2)
		Other notes	Supports Windows, Linux, and Mac OS.
2	**Netdiscover**	Description	Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks. It can also be used to inspect your network ARP traffic, or find network addresses using auto scan mode, which will scan for common local networks.
		Licence	GPL-3.0
		Other notes	
3	**Nikto**	Description	Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files or CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.
		Licence	GNU GPL v2
		Other notes	

4	**OpenVAS Scanner**	Description	A vulnerability scanner that identifies vulnerabilities in systems and networks.
		Dependencies	Various Python packages for ospd-openvas.
		Integration	OSP (Open Scanner Protocol).
		Owner	Greenbone Networks GmbH
		Licence	GPL
		Other notes	Requires openvas-smb for Windows support; part of the Greenbone Vulnerability Management solution.
5	**Secret Scanner (GitHub)**	Description	Scans repositories for accidentally committed secrets like credentials.
		Dependencies	Nonspecific; relies on GitHub's infrastructure.
		Integration	Integrated with GitHub repositories; can be extended via the Secret Scanning Partner Program.
		Owner	GitHub
		Licence	Part of GitHub's services; no specific license for end-users.
		Other notes	Available for public repositories and can be enabled for private ones.
6	**Bandit**	Description	A tool designed specifically for finding common security issues in Python code.
		Dependencies	Python and various Python packages.
		Integration	Nonspecific.
		Owner	Open-source community (originally developed by OpenStack)
		Licence	Apache License 2.0
		Other notes	Supports profiles for specific vulnerability checks.
7	**Grype**	Description	A vulnerability scanner for container images and file systems.
		Dependencies	Various Go packages.
		Integration	Can be integrated into CI/CD pipelines or used standalone.
		Owner	Anchore, Inc.
		Licence	Apache License 2.0
		Other notes	Supports scanning of container images and file systems for vulnerabilities.

8	**Vault**	Description	Vault provides organizations with identity-based security to automatically authenticate and authorize access to secrets and other sensitive data.
		Dependencies	Installation (binary) package available
		Integration	Integrations | Vault | HashiCorp Developer
		Owner	HashiCorp
		Licence	Mozilla Public License 2.0 (MPL 2.0)
		Other notes	While the core Vault product is open source, HashiCorp also offers an enterprise version called "Vault Enterprise" that includes additional features like disaster recovery, automated backups, and enhanced access control capabilities, which requires a paid license.
9	**CycloneDX**	Description	An open-source tool supporting building of Software Bills of Materials (SBOMs): Both a specification for SBOMs and a suite of tools that can generate them for various ecosystems
		Dependencies	CycloneDX Core Libraries (JDK, .NET, Node.js), Command-line Tools (pip, npm, Maven), Build System Plugins (Maven, Grandle, npm)
		Integration	Maven projects, Grandle projects, npm/Node.js, Python, CI/CD pipelines, REST API
		Owner	managed by the OWASP Foundation (Open Web Application Security Project)
		Licence	Apache License 2.0.
10	**Metasploit Framework**	Description	Metasploit Framework is one of the most widely used penetration testing frameworks in cybersecurity. It's an open-source tool that helps security professionals test network and system vulnerabilities by providing a platform to develop, test, and execute exploits.
		Dependencies	Git, Ruby, PostgreSQL, Nmap
		Integration	CI/CD pipelines, API integration, Security Tool Integration
		Owner	Rapid7 and available in both free Community and commercial Pro editions
		License	BSD-style license
		Other notes	While it's a powerful legitimate security tool, its capabilities also make it a favourite among malicious actors, highlighting the dual-use nature of many cybersecurity tools.
11	**TheHive**	Description	TheHive is an open-source, scalable security incident response platform designed for security operations

			centres (SOCs), computer security incident response teams (CSIRTs), and information security teams.
		Dependencies	Cortex, MISP
		Integration	JAVA, ElasticSearch, Node.js/npm
		Owner	TheHive Project
		Licence	AGPL-3.0 license (GNU Affero General Public License version 3.0)

8. CURIUM validation plan

The CURIUM validation plan aligns with the project's objectives, leverages p-NET and EIT Digital's extensive network of companies and SMEs, and aims to ensure that CURIUM's tools and services meet their cybersecurity needs while aligning with the CRA and other relevant EU policies.

The plan is founded on the following key points:

- Stakeholder identification and engagement: in collaboration with T5.3, the project will leverage partners' networks and EIT Digital's pan-European ecosystem, including startups, SMEs, universities, and industry partners, to identify and involve key stakeholders (SMEs, national authorities, and cybersecurity experts).
- Agile validation cycles: it will conduct at least two major release rounds with smaller interim releases to allow continuous feedback. Each cycle will include solution deployment, stakeholder testing, and feedback collection through workshops, hands-on sessions, and online surveys. The validation process will evaluate various aspects of the proposed solution like functionality, usability, ease of access, knowledge capacity, financial factors, etc.
- Co-creation and feedback loops: it will involve end-users in requirements elicitation, solution testing, and refinement phases to ensure the solution addresses real-world needs. Feedback will be used to iteratively improve functionality, usability, and CRA compliance.
- Validation tools and channels: it will use p-NET's infrastructure to deploy solutions on secure cloud-based testing environments for stakeholders to evaluate. The plan fully relies on the project's communication and dissemination strategy (Task 5.1), utilizing channels such as the project's website, social media, and partners' own networks to ensure effective awareness and stakeholder engagement.

8.1. Validation methodology

The methodology that the project will follow details the systematic processes to execute the validation plan, following an agile, iterative process with multiple rounds of solution releases, feedback collection, and refinement, fostering co-creation with stakeholders. This methodology aims to ensure that CURIUM's solutions are practical, accessible, and aligned with the CRA, facilitating adoption by SMEs and micro-enterprises across the EU. For this, the validation plan will evaluate two distinct aspects:

- **System validation**: confirms that the CURIUM tools and services meet their defined technical, functional, and non-functional requirements (sourced from T2.1, T2.2 and T2.3 and presented in section 5.3 of this deliverable), with a focus on the mandatory ones
- **Performance monitoring**: tracks the project's progress and impact through Key Performance Indicators (KPIs) outlined in the Grant Agreement

8.2. System validation

The methodology validates that the CURIUM system meets its most relevant requirements by classifying them, mapping them to evaluation aspects, and defining evaluation methods to support the assessment of the system's performance and impact. Requirements are sourced from Task T2.1 (functional and non-functional requirements, including SRs and VRs, derived from the EU digital market analysis and CRA/regulatory landscape), Task T2.2 (end-user requirements for SMEs, covering technical, operational, regulatory, and legal aspects) and T2.3 (technical specifications of the Compliance Continuum). The steps defined are:

1 - Identify evaluation aspects: define the criteria for assessing the system's success:

- Functionality: assess whether the tools and services effectively support CRA compliance, such as secure product development and vulnerability management. Validation would consider security aspects like confidentiality, integrity, authentication, accountability, non-repudiation etc.
- Reliability and Functional Stability: these include aspects like availability, fault tolerance and recovery and verification that functionalities operate correctly across different scenarios.

- Usability and ease of access: evaluate how intuitive and accessible the solutions are for SMEs with limited resources, ensuring they can adopt them without significant barriers.
- Knowledge capacity: measure the increase in SMEs' awareness on the scope and CRA requirements, focusing on training materials, workshops, and best practices.
- Financial factors: analyse the cost-effectiveness of the solutions for SMEs, ensuring that financial constraints do not hinder adoption.

2 - Requirement classification and prioritization: technical, functional, and non-functional requirements are prioritized using the MoSCoW methodology. "Must have" requirements, critical for CRA compliance and core functionality, are the primary focus of validation.

3 - Validation approach: For each "Must have" requirement, the plan defines evaluation aspects (functionality, usability, knowledge capacity, financial factors) and methods (testing, user feedback, etc.) to confirm compliance.

4 - Documentation: validation results will be documented in reports, using tables to list requirements, evaluation methods, and verification means, ensuring transparency and traceability.

Table 11 will be used to present the system relevant requirements, mapping them to evaluation aspects, and evaluation methods, with the following format:

TABLE 11: SYSTEM REQUIREMENTS TEMPLATE

ID	Requirement description	Evaluation aspect	Evaluation method	Means to verify	Monitored by
		Functionality, Usability and ease of access, Knowledge capacity, Financial factors			

8.3. Performance monitoring

Performance monitoring tracks the project's success through KPIs from the Grant Agreement, focusing on process effectiveness and outcomes. This includes:

- Engagement metrics: measures stakeholder participation (workshops, feedback collection, etc.) and awareness (for example, CRA knowledge increase) using defined methods (attendance logs, surveys, etc.), which is critical for robust system validation and alignment with project goals.
- Operational metrics: monitors milestones like release rounds, tool deployment, and documentation accuracy through reports and logs, ensuring that the evaluation process is systematic and transparent.
- Outcome metrics: assesses broader impacts, such as cost reduction or tool adoption, via end-user reports and consortium data.

Performance monitoring involves working closely with T5.3 to schedule engagement activities (workshops, events, trainings), collecting feedback and participation data, measuring system compliance using the evaluation methods defined, and refining the system iteratively based on results, documenting outcomes in validation reports. Engagement activities will be communicated via Task 5.1 channels (project website, social media) to maintain transparency and attract further engagement.

Table 12 will be used to collect the project's KPIs and the way they will be monitored.

TABLE 12: PERFORMANCE MONITORING TEMPLATE

#	KPI Name	Target	Objective	Means to verify	Monitored by

8.4. Time plan

The validation plan will be executed over the project duration (18 months), with key activities scheduled to align with release rounds, engagement events, and documentation milestones. The timeline below outlines the major activities of the validation plan, referencing the methodologies described in the previous section.

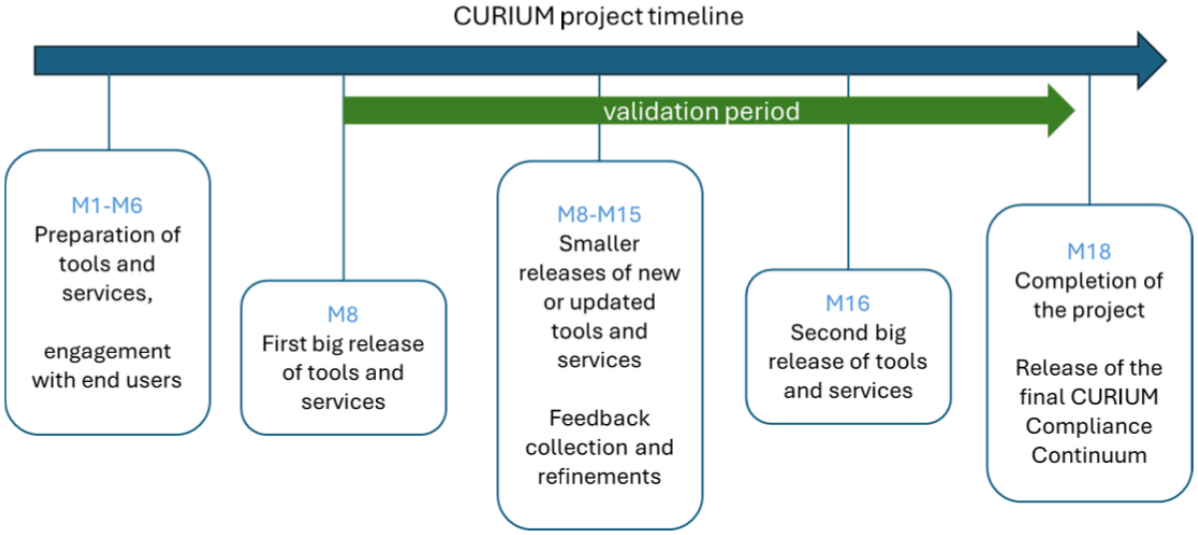


FIGURE 19: VALIDATION PLAN TIME LINE

- **M1-M6 (Preparation Phase):**
  Finalize the detailed validation plan (Task 2.4), identify stakeholders, and raise awareness through project presentations, the website, and social media. Engage with relevant communities such as European Digital Innovation Hubs (EDIHs), ENISA, and the European Cybersecurity Competence Centre (ECCC), to ensure diverse input for validation. Begin analysing the KPIs from the Grant Agreement, exploring initial methods for their monitoring, with a focus on identifying cases where external input is needed to assess compliance. For these KPIs, this analysis serves as a preliminary step to inform the design of surveys to gather external input for validating associated metrics.
- **M8 (First Release Round):**
  Release the first round of tools and services and initiate the co-creation phase.
- **M8-M15 (Iterative Validation):**
  Deploy smaller releases and gather continuous feedback through online surveys and workshops. Conduct a first workshop with hands-on sessions to collect feedback from SMEs and micro-enterprises and then organize a second one to evaluate improvements. Refine the solution based on input, focusing on the evaluation aspects and CRA compliance.
- **M16 (Second Major Release Round):**
  Release the second major round of tools and services.
- **M18 (Final Validation and Adoption):**
  Conduct a final workshop, focusing on early adopters. Develop IPR agreements, demos, and training materials to facilitate adoption. Highlight success stories from engaged stakeholders to attract potential adopters.

8.5. Assessment methodologies for KPIs

This section outlines the assessment methodology for the KPIs defined in the Grant Agreement, initiating their analysis and planning during the M1-M6 preparation phase. The project team is actively reviewing all KPIs to assess their scope and implications, developing an Excel (xls) document to track and manage the full list of KPIs, where a responsible partner is being assigned for monitoring each to ensure accountability and effective tracking throughout the project lifecycle.

For some KPIs, particularly those related to process aspects (stakeholder engagement, release rounds, etc.), initial evaluation methods have been defined to guide measurement. The table below presents an example of the work in progress, showcasing some entries that have been completed as part of this ongoing effort, with further refinement planned as validation activities advance.

TABLE 13: PERFORMANCE MONITORING OF PROCESS KPIS

#	KPI Name	Target	Objective	Means to verify	Monitored by
19	Number of release rounds	at least 2	Operational	Document the deployment in project reports to confirm the target is met	AEGIS
20	Number of Alliances/Communities engaged for validation	>5	Engagement	Maintain a stakeholder engagement log to record interactions and contributions	DSA
21	Percentage of end-users providing feedback	>90%	Engagement	Identify the total number of end-users invited to participate in validation activities. Maintain a log of all end-users invited to provide feedback, recording who responds. Collect their feedback through workshops, online surveys, and testing sessions, using multilingual feedback forms and accessible channels (project website, email) to maximize participation, focusing on how well system requirements meet their needs. Establish a reasonable timeframe for feedback submission (7-14 days with reminders). Calculate the percentage of end-users providing feedback for each validation activity and then determine an overall project average to assess the KPI	DSA
22	Increase in SMEs' awareness of CRA requirements	>80%	Engagement	Conduct pre- and post-training surveys during workshops to measure awareness of CRA requirements. Include specific questions on CRA obligations (incident reporting, security updates, etc.) to quantify knowledge gains	DSA
12	Number of workshops/training sessions	at least 3	Engagement	Report attendance, feedback, and outcomes to confirm the target	SPH

13	Number of tools/services evaluated	>10	Operational	Catalogue the tools and services tested during each release round	AEGIS
14	Number of CRA compliance use cases/best practices	>5	Engagement	Develop and document use cases during validation workshops, focusing on practical applications of requirements for SMEs	SPH
29	Maintain compliance documentation accuracy	>=98%	Operational	Feedback and metrics will be documented in a requirements traceability matrix to ensure transparency	CYS

9. Conclusions

Deliverable D2.2 "CURIUM Compliance Continuum blueprint, knowledge capacity and validation plan" showcases the technical foundation and approach of the CURIUM project by outlining the Compliance Continuum's modular architecture, its toolset and their requirements, the supporting capacity-building strategy and validation plan. By integrating stakeholder-driven end-user requirements, EU regulatory alignment, and iterative, agile validation processes, the deliverable ensures that CURIUM addresses the real-world cybersecurity challenges faced by SMEs and micro-enterprises.

The document builds on the work initiated in D2.1, complementing initial findings with expanded user research, risk assessment methodologies, and a clearly defined technical blueprint that integrates five tools and services within an accessible interface. Moreover, the knowledge and capacity-building strategy emphasizes accessibility, inclusiveness, and hands-on training to increase SME readiness for CRA compliance.

The outlined validation plan, aligned with milestones MS4 and MS5, introduces a structured evaluation methodology, engagement processes, and an initial assessment of KPIs. It ensures that CURIUM remains agile and responsive, with iterative feedback loops to improve its effectiveness and usability. Overall, D2.2 forms a reference for guiding the development, deployment, and continuous improvement of CURIUM throughout the project lifecycle.