Ref. Ares(2025)5155757 - 27/06/2025

Cra sUppoRt contInuUM

D2.1 CRA and EU certification analysis towards a European Trustworthy Certified Digital Valley

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	D2.1 CRA and EU certification analysis towards a European Trustworthy Certified Digital Valley		
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**	27.06.2025.
Type	R (Report)	**Dissemination Level**	PU - Public
Lead Beneficiary	APIRO		
Responsible Author	APIRO		
Contributions from	All partners		

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
0.1	07.03.2025	5	Initial Table of Contents and assignment of activities and sections to partners	APIRO
0.2	04.04.2025	45	Contribution from partners (1st part)	APIRO, CYS, NCSA, P-NET, NLG, EIT, AEGIS, SPHYNX, DSA
0.3	09.05.2025	90	Contribution from partners (2nd part)	APIRO, CYS, NCSA, P-NET, NLG, EIT, AEGIS, SPHYNX, DSA
0.4	30.05.2025	100	Deliverable final updates before internal review	APIRO
0.5	04.06.2025	100	Deliverable available for internal review	APIRO
0.6	10.06.2025	100	Internal review	CYS, EIT
1.0	13.06.2025	100	Update the deliverable according to the reviewers' comments	APIRO
1.1	24.06.2025	100	Final, QC-approved version	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 6
2. Glossary of terms and abbreviations 7
3. Introduction 12
3.1. Mapping Deliverable Contents to Related CURIUM GA outputs 12
2.2. Deliverable Overview and Report Structure 12
4. High level methodology for the elicitation of the CURIUM Continuum requirements 13
4.1. Step 1. Identification of current legal, regulatory and standardization requirements. 13
4.2. Step 2. SWOT analysis. 14
4.3. Step 3. Stakeholder questionnaire. 14
5. Overview of the EU digital market, the CRA and relevant policies and regulations. 16
5.1. Europe's Digital Decade 16
5.2. The EU Cybersecurity Strategy 18
5.3. Preventive policy instruments 19
5.3.1. The "NIS Directive" 20
5.3.2. The "NIS 2 Directive" 21
5.3.3. Cybersecurity Act 21
5.3.4. The (EU) Cybersecurity Certification Framework 22
5.3.5. The EUCC scheme 22
5.3.6. Cyber Resilience Act 23
5.3.7. The Union Rolling Work Programme for European cybersecurity certification (URWP) 24
5.3.8. EU toolbox for 5G security 25
5.3.9. Cyber Solidarity Act 26
5.3.10. DORA 27
5.3.11. Network Electricity Code 27
5.3.12. Directive 2014/53/EU 28
5.3.13. Regulation for EUIBAs 29
5.3.14. Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 30
5.3.15. Regulation (EU) 2019/2144 30
6. Breakdown of the requirements of the CRA regarding products with digital elements. 32
6.1. Structure of the CRA 32
6.2. Scope of the CRA 34
6.2.1. Important products with digital elements 35
6.2.2. Critical products with digital elements 37
6.2.3. Products with digital elements belonging to the "Default" category 38
6.2.4. High-risk AI systems 38
6.3. CRA scope exclusions 38
6.4. CRA interested parties (including Economic Operators) 40

© CURIUM, 2025

6.5. Obligations of Economic operators 40
6.5.1. Manufacturers (Articles 13, 14, 15) 40
6.5.2. Authorized Representatives (Articles 18, 15) 41
6.5.3. Importers (Articles 19, 15) 42
6.5.4. Distributors (Articles 20, 15) 42
6.5.5. Open-Source Software Stewards (Articles 24,15) 43
6.6. Essential Cybersecurity Requirements 43
6.7. Technical Documentation 44
6.8. Proof of conformity 46
6.9. EU Declaration of Conformity 48
7. Analysis of related certification policies, standards and developments on standardization. 49
7.1. Standardization and the CRA 49
7.2. Support to standardization 54
7.2.1. Cyberstand.eu 54
7.2.2. STAN4CR2 54
7.3. Certification aspects of the CRA 55
7.4. EUCC and CRA interplay 56
8. Results 58
8.1. Analysis of legal, regulatory and standards requirements 58
8.2. SWOT analysis 59
8.3. The Stakeholder questionnaire results 60
9. Conclusions 65
10. Annex I 66
Demographics (Profile of the respondent) 67
Existing knowledge of the CRA 69
Challenges 70
Offerings 72
11. Annex II 74

Table of Figures

Figure 1. The 2030 Digital Decade principles – Digital Compass 17
Figure 2. A map to the instruments to support the EU policy for Cyber Defence 19
Figure 3. The EU legislative landscape - 2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION 20
Figure 4. Relationship between risks, mitigating measures and supporting actions for 5G network security 25
Figure 5. Conclusions on key measures – EU toolbox 26
Figure 6. Relationship between conformity assessment options and different categories of products with digital elements 56
Figure 7. Number of respondents per country 62
Figure 8. Number of responses by Organization/Entity Type 63
Figure 9. Knowledge level of CRA 63

List of Tables

Table 2-1 Abbreviations 7
Table 2-2 Glossary of important terms 9
Table 3-1 Adherence to CURIUM GA Deliverable & Tasks Descriptions 12
Table 6-1 Example of proposed Annex I for the technical descriptions of important products with digital elements 37
Table 6-2 Example of proposed Annex I for the technical descriptions of critical products with digital elements 38
Table 7-1 Overall list of the identified standards with their respective mapping towards the security requirements 50
Table 7-2 Overall list of the identified standards with their respective mapping towards the vulnerability handling requirements 52
Table 7-3 Projects, their description and status being developed by CEN/CLC/JTC 13/WG 9 53
Table 7-4 Summary of conclusions on the EUCC | CRA interplay for critical products 56
Table 8-1 Identification of Functional Requirements (FRs) 58
Table 8-2 Results of the SWOT analysis 59
Table 8-3 Kind of support for CRA requirements 64

1. Executive Summary

This deliverable aims to provide the methodology and the results of the analysis performed by the CURIUM project for the elicitation of the requirements for the tools and activities of the CURIUM project. Specifically, this deliverable (the first technical one of the project), describes the methodology adopted by the CURIUM project in order to determine the requirements of the CURIUM Continuum.

The CURIUM Compliance Continuum serves as a framework for organizations to assess their current level of compliance, identify areas for improvement, and develop strategies to enhance their overall compliance posture. For this Continuum, requirements have to be identified in order to fit the needs and expectations of the interested parties, to avoid possible risks and take advantage of possible opportunities in order to effectively fulfil the project's objectives.

The methodology for the elicitation of the requirements mentioned above is split into three distinct steps. Below, each step is very briefly presented along with its main outcomes:

1. State of the Art Analysis regarding current legal, regulatory, standardization and certification policies. This analysis provides the requirements of the different regulatory documents as they relate to the scope of the CURIUM project. These requirements are extensive and are presented in a grouped manned within Section 8.1.

2. SWOT analysis. This analysis provides an overview of the strengths, weaknesses, opportunities and threats to the project. Through this analysis a number of circumstances that could be exploited and avoided by the project have been identified.

3. Stakeholder questionnaire. The stakeholder questionnaire provides the needs of the various categories of stakeholders, in relation to the scope of the project. The results in this deliverable are provided at a high level, since the detailed results are documented in D2.2. Deliverable D2.2. 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 is directly linked to tasks 2.1 and 2.2.

2. Glossary of terms and abbreviations

This section of the document provides a Glossary of terms and abbreviations utilized within this document.

Table 2-1 Abbreviations

Abbreviation / Term	Description
AVA_VAN	Certification bodies issue EUCC certificates at two assurance levels: 'substantial' (AVA_VAN levels* 1 or 2) and 'high' (AVA_VAN levels 3, 4 or 5). The assurance level determines the depth and rigour of the evaluation.
CSIRT	A computer security incident response team is a group of IT professionals that provides an organization with services and support surrounding the assessment, management and prevention of cybersecurity-related emergencies, as well as coordination of incident response efforts.
DSPs	Digital service providers are companies that provide online services to their clients such as cloud services, hosting, software development and more.
ECCF	The EU's Cybersecurity Certification Framework for Information and Communication Technology (ICT) products enables tailored and risk-based EU certification schemes.
EUCC	The EUCC arose from the EU Cybersecurity Act, which called for ENISA to develop an EU-wide cybersecurity certification scheme to regulate ICT products, ultimately for adoption by the EC.
EU-CyCLONe	The EU-CyCLONe - European cyber crisis liaison organisation network, is a cooperation network for the national authorities of Member States in charge of cyber crisis management. The network was launched in 2020 and formalized on 16th of January 2023 when NIS 2 art 16 entered into force.
EU CSA	The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
FRG	Group of functional requirements elicited by the state of the art analysis.
MSS	Managed security services are services carrying out or providing assistance for activities relating to customers' cybersecurity risk management.
NIS 2 Directive	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
OES	Operators of Essential Services are public or private entities providing services essential to the maintenance of critical societal and/or economic activities.
ENISA	The European Union Agency for Cybersecurity, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. It contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.

© CURIUM, 2025

URWP	The Union Rolling Work Programme for European cybersecurity certification identifies strategic priorities for future European cybersecurity certification schemes.
DORA	The Digital Operational Resilience Act (DORA) is a regulation introduced by the European Union to strengthen the digital resilience of financial entities. It ensures that banks, insurance companies, investment firms and other financial entities can withstand, respond to, and recover from ICT disruptions, such as cyberattacks or system failures.
RED (Radio Equipment Directive 2014/53/EU)	Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.
LVD (Low Voltage Directive 2014/35/EU)	Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits
EMC Directive	Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility.
EUIBAs	EUIBAs are EU Institutions, Bodies, and Agencies responsible for implementing EU policies and operations.
ISMS	Information Security Management System is a suite of activities concerning the management of information risks. The ISMS is an overarching management framework through which the organization identifies, analyses and addresses its information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts.
CRA	Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). The Cyber Resilience Act enhances cybersecurity standards of products that contain a digital component, requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products.
NCCAs	National Cybersecurity Certification Authorities (NCCAs) are designated by each EU Member State under the EU Cybersecurity Act to supervise and enforce cybersecurity certification schemes, oversee national compliance, authorize assessment bodies, and coordinate with ENISA and the European Cybersecurity Certification Group.
CERT-EU	CERT-EU is an inter-institutional service provider administratively hosted in the European Commission. As the Cybersecurity Service for the Union institutions, bodies, offices and agencies, its mission is to contribute to the security of their ICT infrastructure by helping them to prevent, detect, mitigate and respond to cyber attacks
HS	A Harmonised European Standard is a European standard developed at the request of the Commission by one of the European standardisation organisations (ESOs), in view of applying Union harmonisation legislation.
CS	Common Specifications are detailed practical rules setting out how particular types of devices should comply with certain requirements of Regulation (EU) 2017/746.
SDOs	Standards Development Organizations
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology

CyReA	Cyber Resilience Assessment (CyReA) service (one of the parts comprising the CURIUM Compliance Continuum)
DPMA	Digital Product Maturity Assessment (DPMA) service
DPRA	Digital Product Risk management (DPRA) service
CAC	Conformity Assessment and Compliance (CAC) service
PSTVA	Penetration Self-Testing and Vulnerability Assessment (PSTVA) Services and tools

Table 2-2 Glossary of important terms

Term	Description
ADCO (Administrative Cooperation group)	European cooperation on market surveillance takes place through informal groups of market surveillance authorities, called Administrative Cooperation Groups.
Common Criteria (ISO/IEC 15408)	Common Criteria, formally known as ISO/IEC 15408, is an international standard for evaluating and certifying the security of IT products and systems.
CURIUM Compliance Continuum	The Compliance Continuum serves as a framework for organizations to assess their current level of compliance, identify areas for improvement, and develop strategies to enhance their overall compliance posture. The CURIUM project aims to enhance the resilience, security, privacy, and accountability of all hardware and software products with digital elements, through the design and development of a novel Compliance Continuum provided via a set of cybersecurity-oriented tools and services information, guidance, trustworthy Security Testing and essential requirements fulfilment facilitation.
Cybersecurity Act	The Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.
Cybersecurity Emergency Mechanism	Cybersecurity Emergency Mechanism should be established to support Member States upon their request in preparing for, responding to, mitigating the impact of and initiating recovery from significant cybersecurity incidents and large-scale cybersecurity incidents and to support other users in responding to significant cybersecurity incidents and large-scale-equivalent cybersecurity incidents
Cybersecurity Incident Review Mechanism	Cybersecurity Incident Review Mechanism aims to review and assess significant or large-scale incidents.
Declaration of conformity	An EU declaration of conformity (DoC) is a mandatory document that you as a manufacturer or your authorised representative need to sign to declare that your products comply with the EU requirements.
Declaration on Digital Rights and Principles	The Declaration on Digital Rights and Principles presents the EU's vision for digital transformation. This vision puts people at the centre, in line with EU values and fundamental rights. It provides a reference framework for citizens and guides the EU and Member States on our journey to digital transformation.
Digital Decade	The Digital Decade policy programme 2030 sets up an annual cooperation cycle to achieve the common objectives and targets. This governance framework is based on an annual cooperation mechanism involving the Commission and Member States.
Directive (EU) No 2019/944	Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU.

© CURIUM, 2025

Electricity Regulation (EC) No 2019/943	Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity.
Essential Cybersecurity Requirements	The Essential Cybersecurity Requirements mandate that digital products be designed, developed, and maintained to ensure protection against cyber threats, secure data integrity and confidentiality, and include processes for vulnerability handling throughout their lifecycle.
EU Cyber Solidarity Act	The EU Cyber Solidarity Act will improve the preparedness, detection and response to cybersecurity incidents across the EU.
EU Cybersecurity Reserve	The EU Cybersecurity Reserve will consist of incident response services from private service providers ('trusted providers'), that can be deployed at the request of Member States or Union Institutions, bodies and agencies to help them address significant or large-scale cybersecurity incidents.
EU Cybersecurity Strategy	The EU Cybersecurity Strategy aims to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies.
EU toolbox for 5G security	The EU toolbox for 5G security is a set of robust and comprehensive measures for an EU coordinated approach to secure 5G networks.
European Digital Identity Regulation	The European Digital Identity (EUDI) Regulation will revolutionise digital identity in the EU by enabling the creation of a universal, trustworthy, and secure European digital identity wallet
GSR EU regulation - 2019/2144	Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166.
ICT products, ICT services and ICT processes	ICT products, services, and processes refer to the hardware, software, and systems (products), the delivery and support of digital functions (services), and the structured activities involved in managing and operating these technologies (processes).
Joint Cyber Unit	The Commission proposed to build a new Joint Cyber Unit to tackle the rising number of major malicious cyber incidents impacting the life of businesses and citizens across the European Union. The Joint Cyber Unit aims to bring cybersecurity communities together in a platform to foster cooperation and to enable the existing networks to realise their full potential.
NIS Cooperation Group	The Network and Information Systems Cooperation Group was established by the NIS Directive to ensure cooperation and information exchange among Member States.
Regulation (EU) 2019/881	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
Regulation (EU) 2023/203	Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by

	Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664
Regulation (EU) 2024/482	Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).
Regulation 2023/2841	Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.
UNECE R155	UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system [2025/5].
Ex-post and ex-ante	Based on NIS 2 essential entities should be subject to a comprehensive *ex ante* and *ex post* supervisory regime, while important entities should be subject to a light, *ex post* only, supervisory regime. Important entities should therefore not be required to systematically document compliance with cybersecurity risk-management measures, while the competent authorities should implement a reactive ex post approach to supervision and, hence, not have a general obligation to supervise those entities. The *ex post* supervision of important entities may be triggered by evidence, indication or information brought to the attention of the competent authorities considered by those authorities to suggest potential infringements of the Directive.

3. Introduction

3.1. 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 3-1 Adherence to CURIUM GA Deliverable & Tasks Descriptions

CURIUM GA Component Title	CURIUM GA Component Outline	Related Objectives
TASKS		
Task 2.1	*Analysis of EU digital market, CRA and relevant policies and regulations.* *This task will initially conduct a complete overview of the EU digital market, the CRA and relevant policies and regulations. It will classify, associate and construct the list of requirements for the design and development of the CURIUM Continuum, involved tools and services. The task will end up defining the functional and non-functional requirements from security, usability, (technical) perspectives, for the delivery and validation activities in WP3 and WP4.*	*O2.1. Detailed analysis of the security of the EU digital market, the CRA as well as relevant policies and regulations.*
Task 2.2	*End users' requirements including regulatory aspects* *This task focuses on collecting 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.*
DELIVERABLE		
D2.1. CRA and EU certification analysis towards a European Trustworthy Certified digital Valley. *This deliverable will analyze the security requirements imposed by the CRA and relevant certification and standardization policies including legal and regulatory aspects. It will reflect the outcomes of T2.1 and T2.2.*		

2.2. Deliverable Overview and Report Structure

This deliverable aims to provide the results of the analysis performed by the CURIUM project for the elicitation of the requirements for the tools and activities of the CURIUM project.

This deliverable is structured as follows:

Section 1: presents an Executive Summary of this document.

Section 2: creates a connection between the requirements of the GA and this document. The introduction also presents the structure of the document and the glossary of Terms to support the understanding of the document.

Section 4:	presents an overview of the methodology employed by the CURIUM project in order to extract 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.
Section 6:	provides an overview of the EU digital market, the CRA and relevant policies and regulations. This section presents the connection between the EU Cybersecurity strategy and the various preventive policy instruments. The latter are briefly described.
Section 7:	contains a detailed breakdown of the requirements of the CRA.
Section 0:	contains the identification and analysis of related certification and standardization policies.
Section 8:	provides a high-level overview of the results of the methodology introduced in this document.
Section 8:	concludes the document and provides a link to deliverable D2.2.

4. High level methodology for the elicitation of the CURIUM Continuum requirements

This section presents the methodology constructed by the project to define the functional and non-functional requirements from security, usability and (technical) perspectives. These requirements will be used to design the CURIUM Continuum (Tasks 2.2. and 2.3.) and will facilitate the delivery and validation activities in WP3 and WP4.

As presented also in the project proposal, the overall project CURIUM will follow 4 clear phases of development: Definition, Design, Implementation, Validation. These phases are interlinked with the project's objectives and are organized into five (5), work packages (WPs) to successfully deliver the desired results.

The first phase defines the current state of play and identifies and prioritizes the critical problems that must be addressed. Task 2.1 and this deliverable, support this first phase of the project development: Definition.

This first phase, and through the methodology utilized by the project and described followingly, shall identify the current state of play and identify and prioritize the critical problems that must be addressed.

The methodology of the project, consists of the following steps:

- Step 1. Identification of current **legal, regulatory, standardization and certification** requirements. Information from the work performed within this step of the methodology is provided in Sections 5, 6 and 7, where as a summary of the results is provided in Section 8.1.
- Step 2. **SWOT analysis**. A summary of the results of this step is provided in Section 8.2.
- Step 3. **Stakeholder questionnaire**. A summary of the results of this step is provided in Section 8.3.

Within sections 4.1 – 4.3, each step of the methodology is further described, and the expected outcomes are defined.

4.1. Step 1. Identification of current legal, regulatory and standardization requirements.

Starting from the European Cybersecurity Strategy and the European Digital Decade framework, the project shall identify requirements related to cybersecurity that could be considered within the scope of the project and should be taken into consideration.

Since the project is focused on the creation of tools to support implementation of the EU Cyber resilience Act (CRA), the focus shall be on the CRA, but also other legislation should also be reviewed to identify any related requirements.

The analysis would include existing preventive policy instruments on cybersecurity, cybersecurity evaluation and certification. The analysis shall also include the analysis of the current standardization landscape to support the CRA.

The expected outcome of this process is:

- Legal, regulatory, standard and certification related requirements for the CURIUM Continuum.

4.2. Step 2. SWOT analysis.

SWOT analysis is a strategic analysis tool for use in context analysis. The acronym refers to the domains it considers: Strengths, Weaknesses, Opportunities and Threats. It combines an assessment of the strengths and weaknesses of an organisation, geographical area or sector with assessment of the opportunities and threats posed by the environment.[1]

SWOT analysis considers internal and external factors to maximise the potential of strengths and opportunities, while minimising the impact of weaknesses and threats. When used as a tool for context analysis, SWOT complements PESTEL by identifying possible strategic approaches. It is also closely linked in the design phase to public policy analysis and stakeholder analysis; these in turn are often integrated in PESTEL in the preliminary identification phase.

Through this process the following shall be identified as they relate to the CURIUM Continuum:

- Opportunities: Positive externalities which can provide an advantage for the effective application of the CRA through the novel Compliance Continuum but remain beyond the project's control.
- Threats: Negative externalities which can put the effective application of the CRA through the novel Compliance Continuum at risk but remain beyond the project's control.
- Strengths: Positive internal factors controlled by the project, and which provide foundations for the future.
- Weaknesses: Negative internal elements which are controlled by the project and to which key improvements can be made.

The expected outcomes of this process are:

- Additional expectations that could be fulfilled by the project and non-functional requirements designed to remedy weaknesses and avoid threats.
- Critical problems which need to be addressed.

4.3. Step 3. Stakeholder questionnaire.

The objective of the questionnaire is the collection of needs and requirements of the end users of the CURIUM Compliance Continuum. The Compliance Continuum shall serve as a framework for organizations to assess their current level of compliance, identify areas for improvement, and develop strategies to enhance their overall compliance posture. Furthermore, the project aims to provide capacity building abilities, to support other stakeholders also (e.g. users of products with digital elements).

To achieve these objectives, the Compliance Continuum will provide two groups of services:

Group 1: Tools and services that automate the process of compliance and alignment with the CRA. Through these services and tools, end users will be able to evaluate various cybersecurity aspects of their digital products, perform automated assessments to identify levels of maturity and compliance requirements, test their products for security issues and vulnerabilities, produce technical documentations and recommendations for further actions that need to be taken, etc.

Group 2: knowledge and capacity building. Utilizing the already established services of P-NET (competence centre), EIT (Europe's largest digital innovation ecosystem and partner of 8 EDIHs) and the involvement of partners, the project will offer support for experimentation and testing for conformance, training, consulting,

[1] https://wikis.ec.europa.eu/display/ExactExternalWiki/SWOT+analysis+-+strengths%2C+weaknesses%2C+opportunities+and+threats

supporting, awareness raising and knowledge transferring and linking and collaboration (also with EU policymakers, and National Authorities).

The CURIUM Continuum aims to provide tools and knowledge to a variety of stakeholders, which and based on the terminology employed by the CRA, are the following:

Economic Operators of products with digital elements

- Manufacturers / Developers of products with digital elements
- Authorized representatives of manufacturers of products with digital elements
- Importers of products with digital elements
- Distributors of products with digital elements
- Natural or legal persons who are 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 the CRA

Users of products with digital elements

- End user of products with digital elements
- Consumer Associations
- Industry Associations

National and European policy makers

- National authorities
- European Bodies, Institutions or Agencies (e.g. ENISA, EC, etc.)
- Government and/or Regulatory body

Other entities affecting, being affected or perceive themselves affected[2]

- Academic Community
- Open-source communities
- Cyber Insurance

The main objectives of the questionnaire were to collect the following information:

- the extent that different types of stakeholders possess knowledge of the various parts and requirements of the CRA;
- the challenges faced by different stakeholders, in relation to their compliance with the CRA and
- the type and method of support they would like to receive in relation to the CRA and the tasks that need to be performed.

The structure and content of the questionnaire is presented in Annex I, whereas the results from the implementation of the questionnaire for the period of March – early May 2025 are presented in D2.2.

The expected outcome of this process is:

- Requirements of the different categories of stakeholders in relation to the CRA (in terms of services, tools and capacity building)

[2] The title used in this case is derived from the definition of the term stakeholder based on ISO/IEC 27000:2018. This group is meant to encompass stakeholders that do not belong to other explicit groups.

5. Overview of the EU digital market, the CRA and relevant policies and regulations.

5.1. Europe's Digital Decade

Digital technologies are changing peoples' lives[3] - from the way we communicate to how we live and work. Digitalisation has the potential to provide solutions for many of the challenges Europe and Europeans are facing and offers opportunities such as:

- creating jobs
- advancing education
- boosting competitiveness and innovation
- fighting climate change and enabling a green transition

Following the COVID-19 pandemic, digitalisation is a key component for both economic recovery and the resilience of Europe's health and care sectors. Digitalisation has given the EU further impetus to accelerate technological transition, by boosting eHealth and promoting enabling technologies like cloud computing, quantum technologies and high-performance computing.

To make our societies and economies fit for the digital age, the EU is committed to creating a **safe digital space for citizens and businesses** in a manner that is inclusive and accessible for all. This means enabling a digital transformation that safeguards EU values and protects citizens' fundamental rights and security, while also enhancing Europe's digital sovereignty.

Digital society and digital technologies bring with them new ways to learn, entertain, work, explore, and fulfil ambitions. They also bring new freedoms and rights and give EU citizens the opportunity to reach out beyond physical communities, geographical locations, and social positions.[4]

However, there are still many challenges associated with the digital transformation. The digital world should be based on European values – where no one is left behind, everyone enjoys freedom, protection and fairness. Europe's Digital Decade is where everyone has the skills to use everyday technology. Even small businesses use technology to make better business decisions, interact with their customers or improve parts of their business operations. Connectivity reaches people living in villages, mountains and remote areas, so everyone can reach online opportunities and participate in the benefits of the digital society. Key public services and administrative procedures are online for the convenience of citizens and businesses.

The Digital Decade is a comprehensive framework that guides all actions related to digital. The aim of the Digital Decade is to ensure all aspects of technology and innovation work for people.

The framework for the Digital Decade includes the Digital Decade policy programme, the Digital Decade targets, the objectives, the multi-country projects and the Digital Decade rights & principles:

- The Digital Decade targets are measurable goals for each of the four areas: connectivity, digital skills, digital business, and digital public services.
- The Digital Decade objectives guide Member State actions. The Commission informs about the Member States' actions in the annual report.
- The Digital Decade policy program allows the EU and the Member States to work together to reach the Digital Decade targets and its objectives. It lays down a mechanism to monitor progress towards 2030. Every year, the Commission publishes a report to take stock of the progress made.
- The multi-country projects allow Member States to pool investments and launch large-scale, cross-border projects.

[3] https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/

[4] https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

- The Digital Decade rights and principles reflect EU values, which have to be respected in the digital world, as signed in the Declaration on Digital Rights and Principles.

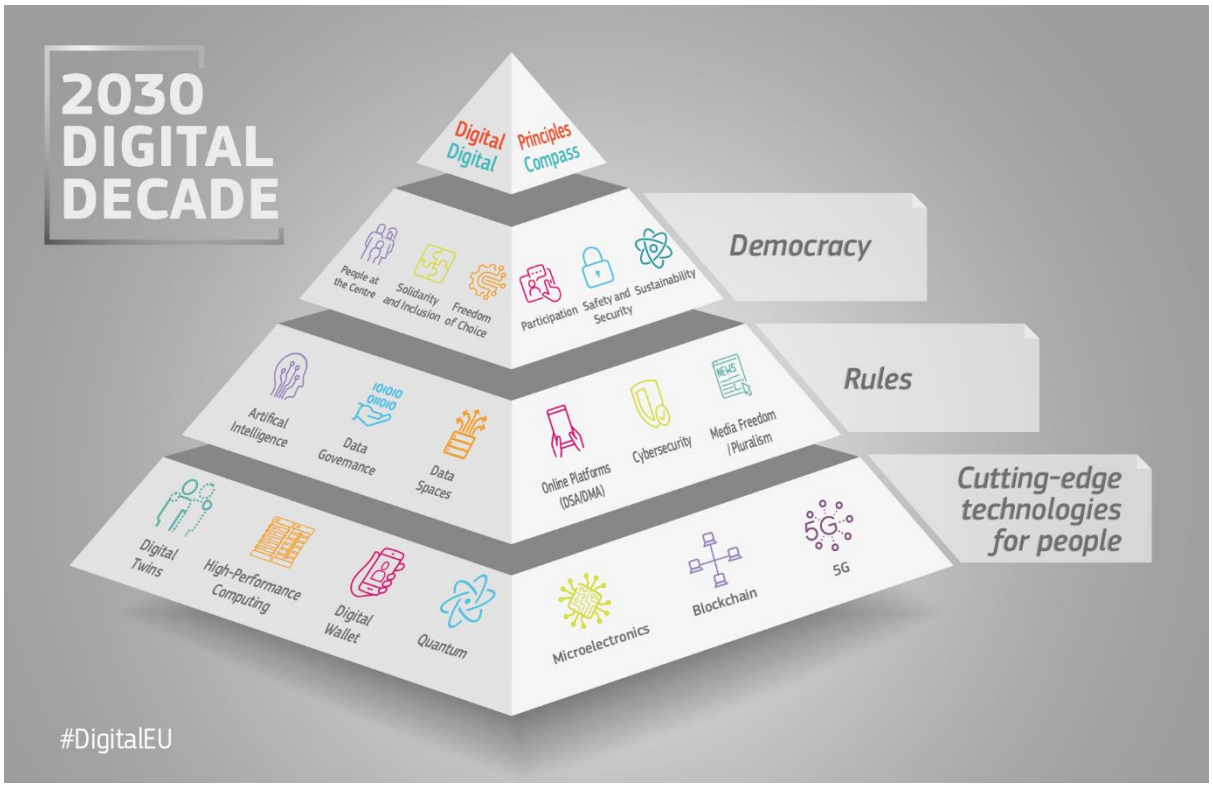

Figure 1. The 2030 Digital Decade principles – Digital Compass[5]

The Digital Decade policy programme sets out digital ambitions for the next decade in the form of clear, concrete targets. The main goals can be summarised in 4 points:

1. a digitally skilled population and highly skilled digital professionals
2. secure and sustainable digital infrastructures
3. digital transformation of businesses
4. digitalisation of public services

Alongside the targets, the Digital Decade objectives ensure that the digital transformation in Europe benefits all people, by:

- Building a safe & secure digital world
- Ensuring everyone can participate in digital opportunities, and no one is left behind
- Making sure small businesses and industry can access to data
- Enabling start-ups & SMEs to adopt digital technologies, including cloud, data analytics, and Artificial Intelligence (AI)
- Promoting the deployment of innovative infrastructures
- Ensuring SMEs can compete in the digital world on fair terms
- Providing public services online
- Promoting research focussed on measuring the impact of digital technologies, and developing sustainable, energy and resource efficient innovations

[5] https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

- Ensuring all organisations adopt cybersecurity measures

On the path towards the Digital decade, the Member States report to the Commission about the planned actions that support the defined objectives.

Commission actions and policies in digital are already guided by these objectives and principles. As we will have more and more innovations, the Digital Decade framework ensures that the European vision for the digital transformation is clear and widely supported by all future actions across Europe.

5.2. The EU Cybersecurity Strategy[6]

If the move to digital is to be successful, European citizens and businesses must be able to benefit from new technologies without compromising their cybersecurity. The EU's Cybersecurity Strategy aims to strengthen our collective cybersecurity and our response to cyberattacks. It will build a stable and secure global Internet where the rule of law, human rights and democratic values are protected.

The strategy has three areas of action:

1. resilience, technical sovereignty and leadership.
2. operational capacity to prevent, deter and respond.
3. cooperation to advance global and open cyberspace.

The strategy describes how the EU can harness and strengthen all its tools and resources to be technologically sovereign. It also lays out how the EU can step up its cooperation with partners around the world who share our values of democracy, rule of law and human rights.

The EU's technological sovereignty needs to be founded on the resilience of all connected services and products. All the four cybercommunities – those concerned with the internal market, with law enforcement, diplomacy and defence – need to work more closely towards a shared awareness of threats. They should be ready to respond collectively when an attack materialises, so that the EU can be greater than the sum of its parts.

The strategy covers the security of essential services such as hospitals, energy grids, railways and the ever-increasing number of connected objects in our homes, offices and factories. The strategy aims to build collective capabilities to respond to major cyberattacks. It also outlines plans to work with partners around the world to ensure international security and stability in cyberspace. Moreover, it outlines how a Joint Cyber Unit can ensure the most effective response to cyber threats using the collective resources and expertise available to Member States and the EU.

On 10 November 2022, the Commission and the High Representative presented a Joint Communication on the new EU Policy for Cyber Defence[7]. The main aim of the policy is to enhance cooperation and investments in cyber defence and provide better protection against an increase in cyberattacks. For now, both parties will keep track on the progress of the policy through an annual report, with Member States encouraged to contribute. An implementation plan could be set up in cooperation with Member States.

[6] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022JC0049

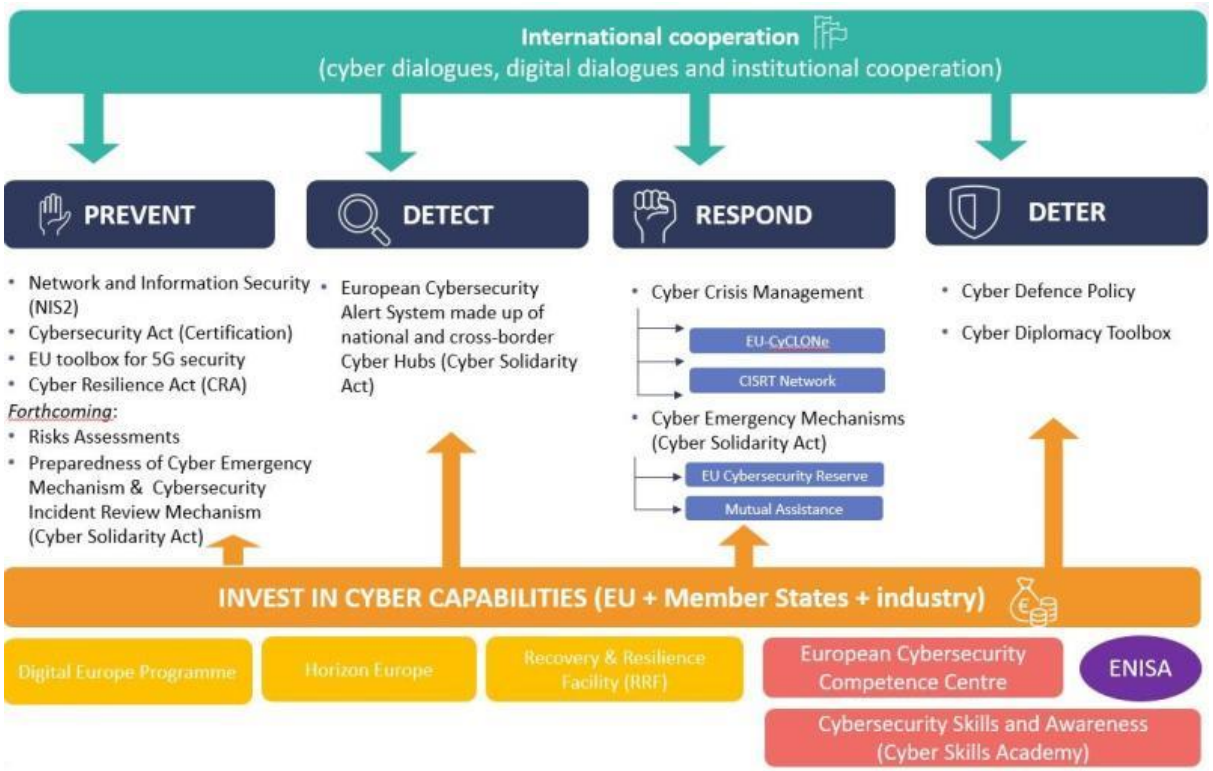

Figure 2. A map to the instruments to support the EU policy for Cyber Defence[8]

As part of these activities, on 15 January 2024, the Commission launched a European action plan to strengthen the cybersecurity of hospitals and healthcare providers. Part of the Political Guidelines of the 2024-2029 Commission mandate, the action plan focuses on improving threat detection, preparedness, and crisis response in the healthcare sector. It aims to provide tailored guidance, tools, services, and training to hospitals and healthcare providers. Several specific actions will be rolled out progressively in 2025 and 2026, in collaboration with health providers, Member States, and the cybersecurity community. This initiative marks the first sector-specific initiative to deploy the full range of EU cybersecurity measures.

5.3. Preventive policy instruments

The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy at the end of 2020.[9]

The Strategy covers the security of essential services such as hospitals, energy grids and railways. It also covers the security of the ever-increasing number of connected objects in our homes, offices and factories.

The Strategy focuses on building collective capabilities to respond to major cyberattacks and working with partners around the world to ensure international security and stability in cyberspace.

This section provides an overview of key cybersecurity related policy instruments.

[8] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[9] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

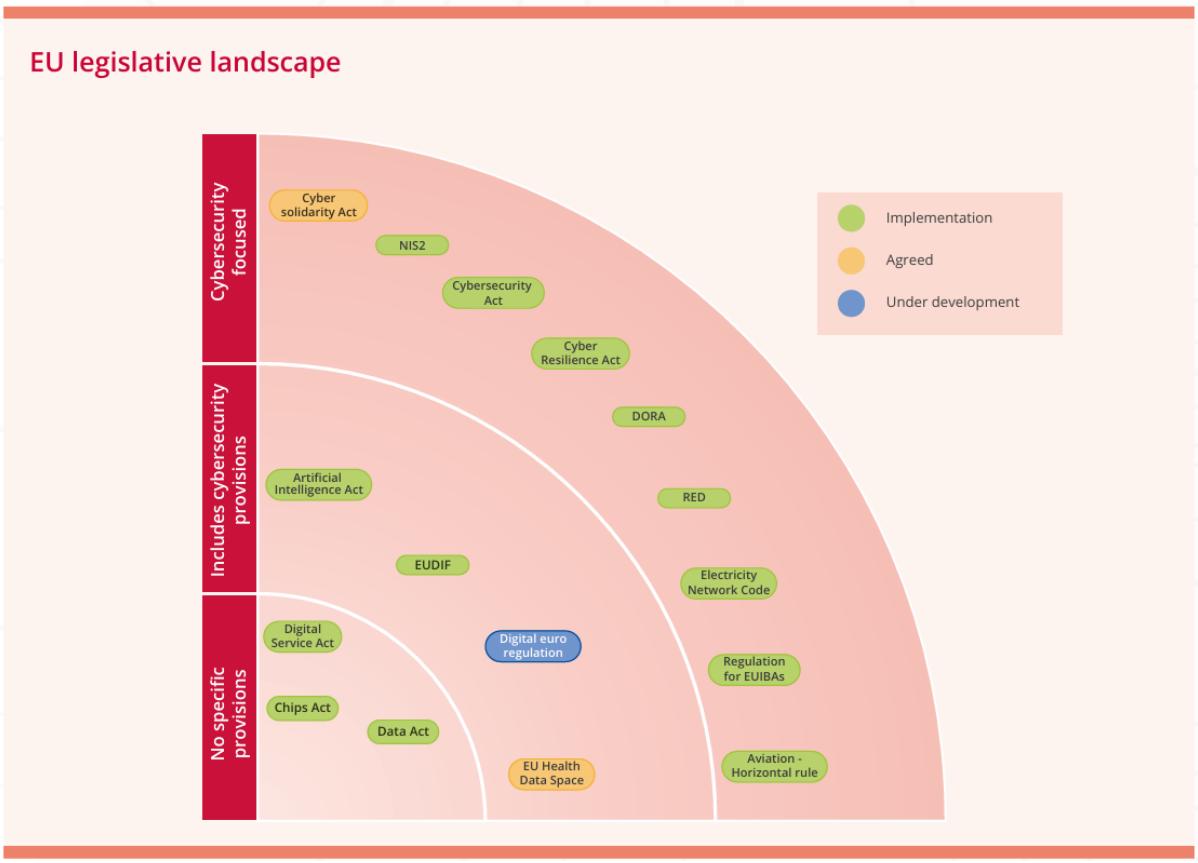

Figure 3. The EU legislative landscape - 2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION[10]

5.3.1. The "NIS Directive"

The NIS Directive was the first comprehensive EU legislation aimed at boosting cybersecurity of network and information systems to safeguard vital services for the EU's economy and society. More specifically, the NIS Directive required EU Member States to strengthen their overall cybersecurity posture by implementing several key measures. Each Member State was obligated to adopt a national cybersecurity strategy, designate one or more national competent authorities, and establish at least one Computer Security Incident Response Team (CSIRT).

The NIS Directive also imposed security and incident notification obligations on Operators of Essential Services (OES) in the sectors and sub-sectors defined in Annex II of the NIS Directive — such as those in energy, transport, banking, health, and water sectors—and on Digital Service Providers (DSPs), including cloud computing services, online marketplaces, and search engines.

These entities were required to take appropriate and proportionate technical and organisational measures to manage cybersecurity risks and report incidents that had a significant impact on the continuity of the services they provide. Additionally, the NIS Directive encouraged cross-border cooperation among Member States to improve collective EU cybersecurity resilience.

The Commission, in order to address the expanding cyber-threat landscape and emergence of new challenges, proposed in December 2020, the revising of the NIS Directive, which eventually led to the adoption of the Directive (EU) 2022/2555 (the "NIS 2 Directive"), which came into force in January 2023. The Member States had until 17 October 2024 to transpose the NIS 2 Directive into national law. The NIS 2 Directive repealed the NIS Directive as from 18 October 2024.[11]

[10] https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

[11] https://digital-strategy.ec.europa.eu/en/policies/NIS2-directive

5.3.2. The "NIS 2 Directive"

The NIS 2 Directive establishes a unified legal framework to uphold cybersecurity in 18 critical sectors across the EU. It also calls on Member States to strengthen their national cybersecurity strategies and enhance collaboration with the EU for cross-border reaction and enforcement. The NIS 2 Directive introduces major changes compared to the NIS Directive including, but not limited to, identification of the entities falling within the scope of the NIS 2 Directive to "essential" and "important" entities, introducing a size cap factor, expansion of the sectors and entities concerned, new selection and registration methods, stricter cybersecurity requirements, management responsibility for non-compliance, new deadlines for reporting incidents, strengthened supervision mechanisms and stricter administrative fines for non-compliance.

Cybersecurity involves protecting network and information systems (NIS), their users, and other affected individuals from cyber incidents and threats. To respond to the increased exposure of Europe to cyber threats, the Directive (EU) 2022/2555, also known as the NIS 2 Directive, replaced its predecessor, the Directive (EU) 2016/1148 or the NIS Directive. The NIS 2 Directive raises the EU's common level of cybersecurity, by expanding its scope, setting clearer cybersecurity requirements, and stronger supervision mechanisms. It requires Member States to enhance their cybersecurity capabilities, while introducing and strengthening risk management measures and reporting requirements to entities from more sectors and setting up rules for cooperation, information sharing, supervision, and enforcement of cybersecurity measures.

The NIS 2 Directive provides that each Member State must adopt a national cybersecurity strategy, which includes, among others, policies for supply chain security, vulnerability management, and cybersecurity education, training and awareness.

The NIS 2 Directive introduces three different states of notification reporting of a significant incident and more specifically provides for the submission of an early warning notification no later than within 24 hours of becoming aware of the significant incident, submission of an incident notification within 72 hours of becoming aware of the significant incident, submission of an intermediate report (if needed) and a final report no later than one month after the submission of the incident notification. The NIS 2 Directive also introduces the submission of a notification to the competent authorities for cyber threats and near miss incidents and voluntary incident notifications even from entities that do not fall within the scope of the NIS 2 Directive.

The NIS 2 Directive empowers the competent authorities with enhanced supervisory mechanisms and introduces a difference between important and essential entities as important entities are supervised "ex-post" and essential entities are supervised both "ex-post" and "ex-ante".

The NIS 2 Directive also introduces the mechanism of voluntary peer reviews with a view to learning from shared experiences, to enhance mutual trust and cybersecurity capabilities and policies across the EU. It also introduces accountability of the top management for non-compliance with cybersecurity risk management measures, thus bringing cybersecurity to the attention of the management of the entities concerned.

The NIS 2 Directive enhances the role of the national Computer Security Incident Response Teams (CSIRTs) and strengthens their duties, technical capabilities and tasks in order to effectively and efficiently detect and respond to incidents. The CSIRTs are crucial for maintaining situational awareness and providing assistance. To manage large-scale cybersecurity incidents or crises, the NIS 2 Directive provides for the establishment of a national cyber crisis management authority and for the establishment of the European cyber crisis liaison organisation network (EU-CyCLONe). The EU-CyCLONE supports coordinated management and ensures regular information exchange among Member States and EU institutions in case of large-scale incidents and crises.

In parallel, the NIS Cooperation Group is established by the NIS 2 Directive to support and facilitate strategic cooperation and information exchange among EU Member States, the European Commission, and the EU Agency for Cybersecurity (ENISA). The NIS Cooperation Group publishes non-binding guidelines and recommendations to support the implementation of the NIS 2 Directive by the Member States. [12]

5.3.3. Cybersecurity Act

The EU Cybersecurity Act, which came into effect on June 27, 2019, aims to enhance cybersecurity across the European Union by strengthening the role of ENISA (European Union Agency for Cybersecurity) and establishing

[12] https://digital-strategy.ec.europa.eu/en/policies/NIS2-directive

a European cybersecurity certification framework. This legislation was introduced to improve the EU's ability to prevent, detect, and respond to cybersecurity threats while fostering trust in digital services and products.

One of the key aspects of the Act is to strengthen ENISA. ENISA was granted a permanent mandate, ensuring its continued role in cybersecurity policy and operations across the EU. The agency was also provided with greater financial resources and staff to better support member states in handling cybersecurity threats. Additionally, ENISA plays a crucial role in advising policymakers, coordinating cyber crisis responses, and facilitating information-sharing between EU nations.

Another major element of the Cybersecurity Act is the establishment of a European Cybersecurity Certification Framework (ECCF), which provides common cybersecurity requirements and evaluation criteria for certification of **ICT products, ICT services** and **ICT processes**. [13]

On 15 January 2025, the Cybersecurity Act was amended to strengthen the EU's cyber resilience, particularly by introducing European certification schemes for **managed security services (MSS)**. This amendment recognizes the growing importance of services such as incident handling, penetration testing, security audits, and consulting.

5.3.4. The (EU) Cybersecurity Certification Framework[14]

The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. The framework will be based on agreement at EU level on the evaluation of the security properties of a specific ICT-based product or service. It will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements.

In particular, each European scheme should specify:

- The categories of products and services covered.
- The cybersecurity requirements, such as standards or technical specifications.
- The type of evaluation, such as self-assessment or third party.
- The intended level of assurance.

The certification framework defines the three assurance levels as basic, substantial, and/or high and are used to inform users of a product's cybersecurity risk. They are commensurate with the level of risk associated with the intended use of the product, service or process, in terms of probability and impact of an accident.

The **Basic** level ensures compliance with security requirements to minimize common cyber risks, primarily through a technical documentation review. The **Substantial** level offers stronger protection against cyber threats from attackers with limited skills and resources, requiring vulnerability reviews and security functionality testing. The **High** level provides the highest assurance against advanced cyberattacks by skilled actors, involving extensive security testing, vulnerability assessments, and penetration testing.

The resulting certificate will be recognised in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

5.3.5. The EUCC scheme

The European Cybersecurity Common Criteria (EUCC) scheme is the first cybersecurity certification framework developed under the EU Cybersecurity Act. Its primary aim is to provide a common European approach to evaluating the security of information and communication technology (ICT) products—such as software, hardware, and embedded systems. The scheme is designed to ensure these products meet standardized cybersecurity requirements and are trustworthy for use across the European Union.

The EUCC is based on the internationally recognized Common Criteria (ISO/IEC 15408), which defines a structured methodology for evaluating the security of ICT products. By leveraging this global standard, the EUCC

[13] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[14] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

enables a harmonized approach to product evaluation throughout EU member states, reducing fragmentation caused by individual national schemes. It is currently a voluntary scheme, though it plays a key role in the EU's broader efforts to enhance digital trust, sovereignty, and resilience.

Certification under the EUCC scheme demonstrates that an ICT product has undergone a rigorous third-party evaluation, ensuring its secure operation and resilience against vulnerabilities. This process aims to ensure the safe use of ICT products by verifying their compliance with the stringent security criteria and protection against cyber threats. It fosters trust between suppliers and users, while also enhancing cooperation and interaction at the European level to address cyber threats.

The scheme focuses on certifying the cybersecurity of ICT products in their lifecycle, including:

- Biometric systems
- Firewalls (both hardware and software)
- Detection and response platforms
- Routers
- Switches
- Specialized software (such as SIEM and IDS/IDP systems)
- Data diodes
- Operating systems (including mobile devices OS)
- Encrypted storage
- Databases
- Smart cards and secure elements, included in all sorts of products, such as in passports daily used by all citizens.

The EUCC was established through **Commission Implementing Regulation (EU) 2024/482**, adopted on 31 January 2024. This regulation was published in the Official Journal of the European Union on 7 February 2024 and entered into force on 27 February 2024, which is twenty days after its publication. According to the regulation, the EUCC scheme became fully applicable on 27 February 2025, one year after its entry into force. This milestone allowed Member States, through their National Cybersecurity Certification Authorities (NCCAs), to begin issuing EUCC certificates from that date onward. The **Commission Implementing Regulation (EU) 2024/3144**[15] of EUCC has been amended by Commission on December 18, 2024.

Under the EUCC scheme, two assurance levels are defined: Substantial and High, each representing a different depth of cybersecurity evaluation for ICT products. The EUCC Implementing Act sets out the procedures and requirements for issuing EUCC certificates at these assurance levels, including the necessary documentation. Conformity self-assessment as defined in Article 53 of Regulation (EU) 2019/881 is not permitted under EUCC.

A key element of the certification process is the vulnerability assessment (AVA_VAN), which determines how resistant a product is to exploitation based on the evaluation of flaws or weaknesses in its operational environment. For the Substantial assurance level, the product must undergo vulnerability analysis corresponding to AVA_VAN level 1 or 2, while at the High level, it must meet the more demanding criteria of AVA_VAN level 3, 4, or 5. These levels reflect the increasing rigor of testing and threat resistance required to achieve certification under each assurance tier.

5.3.6. Cyber Resilience Act

The Cyber Resilience Act entered into force on 10 December 2024. It establishes common standards for products with digital elements, including hardware and software. Such products must meet specific cybersecurity

[15] https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

requirements throughout their lifecycle, including automatic security updates and incident reporting. The Act also introduces a duty of care for manufacturers, ensuring that products are secure by design and by default. This regulation protects consumers and businesses from cyber threats by enabling a safer digital environment.

The Cyber Resilience Act enhances cybersecurity standards of products that contain a digital component, requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products.

From baby-monitors to smart-watches, products and software that contain a digital component are omnipresent in our daily lives. Less apparent to many users is the security risk such products and software may present.

The Cyber Resilience Act (CRA) aims to safeguard consumers and businesses buying software or hardware products with a digital component. The CRA addresses the inadequate level of cybersecurity in many products, and the lack of timely security updates for products and software. It also tackles the challenges consumers and businesses currently face when trying to determine which products are cybersecure and in setting them up securely. The new requirements will make it easier to take cybersecurity into account when selecting and using products that contain digital elements. It will be more straightforward to identify hardware and software products with the proper cybersecurity features.

The CRA introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the planning, design, development, and maintenance of such products. These obligations must be met at every stage of the value chain. The act also requires manufacturers to provide care during the lifecycle of their products. Some critical products of relevance for cybersecurity will also need to undergo a third-party assessment by an authorised body before they are sold in the EU market.

The regulation applies to all products connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules, which is the case for medical devices, aviation and cars. Products will bear the CE marking to indicate that they comply with the CRA requirements. The new rules will rebalance responsibility towards manufacturers, who must ensure their products with digital elements meet cybersecurity standards for the EU market. This will allow buyers to make more informed decisions, trusting the cybersecurity of CE-marked products.

The Cyber Resilience Act entered into force on 10 December 2024. The main obligations introduced by the CRA will apply from 11 December 2027.

5.3.7. The Union Rolling Work Programme for European cybersecurity certification (URWP)[16]

The EU Cybersecurity Act foresees that a URWP for European cybersecurity certification publishes a document setting out a strategic vision and reflections on possible areas for future European cybersecurity certification schemes, considering recent legislative and market developments.

Considering the Cyber Resilience Act (CRA) and other legislative developments, such as the European Digital Identity Regulation, the first URWP points to areas for future European cybersecurity certification schemes linked to legislative developments as well as areas for future reflection regarding cybersecurity certification. This might eventually lead to requests for new schemes where necessary and appropriate. Furthermore, it outlines the strategic priorities to be considered when preparing any European cybersecurity certification scheme.

The URWP stresses the following areas for future European cybersecurity certification linked to EU legislation:

- ID Wallets
- Managed security services
- Industrial Automation and Control Systems
- Security lifecycle development building on the CRA requirements
- Cryptographic mechanisms

[16] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

5.3.8. EU toolbox for 5G security[17]

The EU toolbox for 5G security is a set of robust and comprehensive measures for an EU coordinated approach to secure 5G networks.

Based on the EU coordinated risk assessment of 5G network security, the toolbox lays out a range of security measures aiming to mitigate risks (see Figure 4) effectively and ensure secure 5G networks are deployed across Europe. It sets out detailed mitigation plans for each of the identified risks and recommends a set of key strategic and technical measures (see Figure 5) which should be taken by all Member States and/or by the Commission.

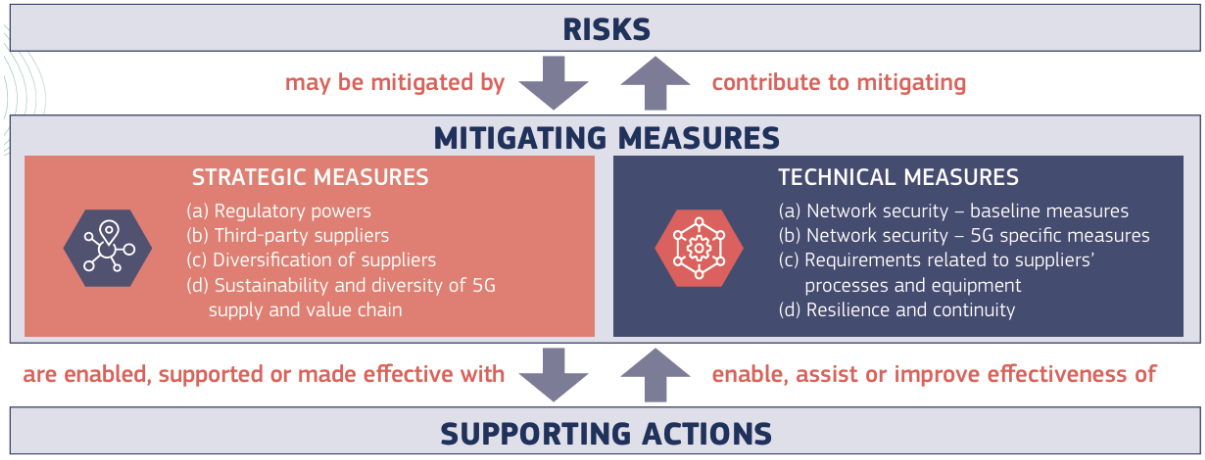

Figure 4. Relationship between risks, mitigating measures and supporting actions for 5G network security

[17] https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

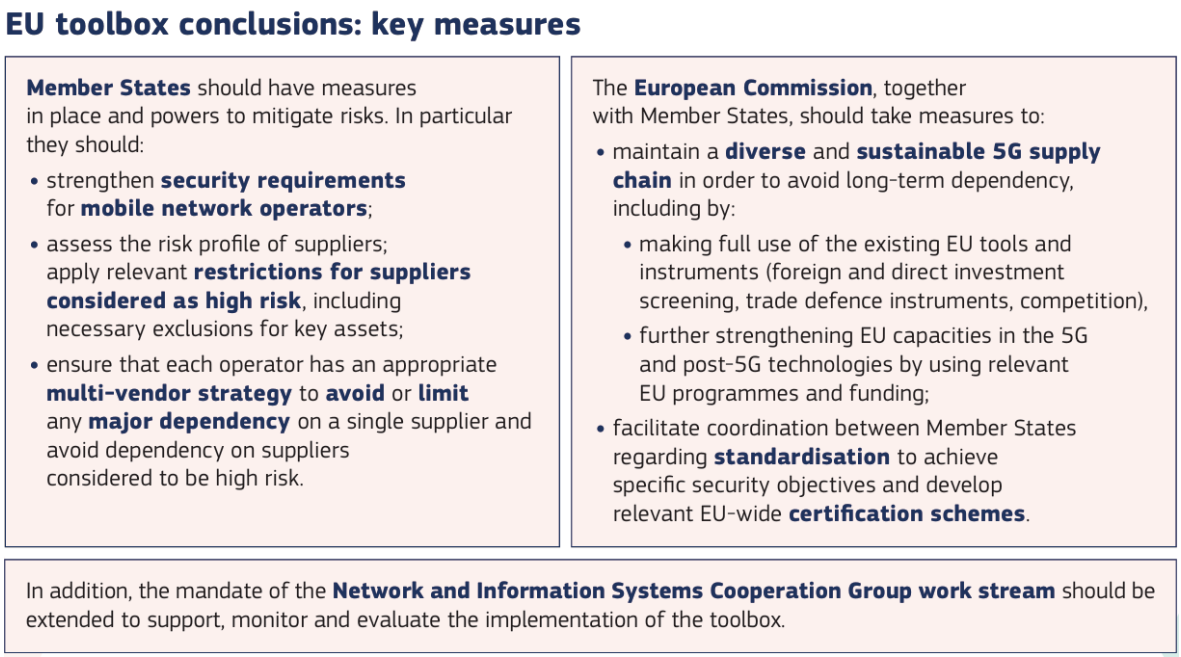

Figure 5. Conclusions on key measures – EU toolbox

5.3.9. Cyber Solidarity Act[18]

The EU Cyber Solidarity Act will improve the preparedness, detection and response to cybersecurity incidents across the EU.

The EU Cyber Solidarity Act aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The Act includes a European Cybersecurity Alert System, made of Security Operation Centres interconnected across the EU, and a comprehensive Cybersecurity Emergency Mechanism to improve the EU's cyber resilience.

The European Cyber Solidarity Act includes a proposal for a European Cybersecurity Alert System to improve the detection, analysis and response to cyber threats.

This system will be composed of national and cross-border Security Operations Centres (SOCs) across the EU, who will use advanced technology such as Artificial Intelligence (AI) and data analytics to detect and share warnings on threats with authorities across borders.

During a first phase, launched in November 2022, three consortia of cross-border Security Operations Centres (SOCs) were selected, bringing together public bodies from 17 Member States and Iceland, under the Digital Europe Programme.

The Cyber Emergency Mechanism will ensure that preparedness and response to cybersecurity incidents are improved. It will do this by acting in 3 areas:

- Supporting preparedness actions: Testing entities in crucial sectors such as finance, energy and healthcare for potential weaknesses that could make them vulnerable to cyber threats. The selection of sectors to be tested will be based on common risk assessment at the EU level.
- Creating an EU Cybersecurity Reserve: The EU Cybersecurity Reserve will consist of incident response services from private service providers (trusted providers'), that can be deployed at the request of Member States or Union Institutions, bodies and agencies to help them address significant or large-scale cybersecurity incidents.

[18] https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

- Ensuring mutual assistance: The mechanism will support a Member State that offers mutual assistance to another Member State affected by a cybersecurity incident.

The Cyber Solidarity Act also establishes the Cybersecurity Incident Review Mechanism to assess and review specific cybersecurity incidents. At the request of the Commission or of national authorities (the EU-CyCLONe or the CSIRTs network), the EU Cybersecurity Agency (ENISA) will be responsible for the review of specific significant or large-scale cybersecurity incident and should deliver a report that includes lessons learned, and where appropriate, recommendations to improve Union's cyber response.

5.3.10. DORA[19]

The Digital Operational Resilience Act (DORA), which is officially known as Regulation (EU) 2022/2554, is a comprehensive regulatory framework which aims to safeguard the financial services sector against Information and Communication Technology (ICT)-related incidents. This is achieved by enhancing how the organisations are going to handle (mitigate, document, react, etc.) potential vulnerabilities and threats.

DORA introduces rules that are designed to strengthen the operational resilience of financial entities. An organisation's management body is becoming responsible for ICT management and thus it has to define appropriate risk management frameworks and to be involved in the execution and oversight of the defined strategies.

DORA divides digital operational resilience into five different categories.

ICT risk management: It aims to shape the ICT risk management into a proactive process, changing it from the reactive one that it is now. It focuses on developing and implementing regular risk assessments, mitigation strategies, evaluation methods and incident response plans.

Incident reporting: Its scope is to standardise the incident report process for financial entities throughout the EU. Institutions are required to establish systems that have the ability to monitor, detect, describe, report and analyse the incidents. Due to DORA's emphasis on transparency, the incident reporting framework must include processes for reporting incidents to both internal and external stakeholders.

Digital operational resilience testing: It aims to ensure the financial institutions' resilience to cyber threats. The organisations are required to carry out regular testing to evaluate their cyber vulnerabilities and responses and then use the results to improve their practices.

Third-party risk management: This category reinforces the relationship between financial institutions and their critical third-party providers. The institutions are required to have detailed contracts with their ICT providers, conduct continuous due diligence and implement a robust process for offboarding. DORA seeks to ensure that third-party relationships do not compromise operational resilience.

Information sharing: It aims to raise the awareness of operational resilience and enhance the sharing of practices and lessons learned across the sector. The organisations are required to share information in a secure way in order to foster the collaboration and increase the resiliency among financial institutions.

5.3.11. Network Electricity Code[20]

EU is ensuring an interconnected internal electricity market. Regulatory frameworks have developed, allowing electricity to be traded across the Union, e.g. recently the Electricity Regulation (EC) No 2019/943 and the Directive (EU) No 2019/944 on common rules for the internal market for electricity.

In this regard, the European Commission has adopted also rules, known as network codes or guidelines for electricity for the integration of the electricity markets. Those network codes and guidelines contain provisions

[19] https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[20] https://energy.ec.europa.eu/topics/markets-and-consumers/wholesale-energy-market/electricity-network-codes-and-guidelines_en

on market rules, system operation and network connection. In the past, the grid operation and trading rules were drawn up nationally. As electricity is increasingly interconnected between countries, the EU-wide rules effectively manage these electricity flows in the internal energy market. These rules are legally binding European Commission implementing Regulations. They govern all cross-border electricity market transactions and system operations alongside the Regulation on conditions for accessing the network for cross-border electricity exchanges [(EC) 2019/943)].

The European Commission creates an annual priority list for developing electricity network codes based on public consultation. New rules may be adopted as guidelines instead of network codes, all legally binding regulations (they are adopted under a different provision of the Electricity Regulation (EC) No 2019/943 but they have the same status)[21].

5.3.12. Directive 2014/53/EU[22]

The Radio equipment directive 2014/53/EU (RED) establishes a regulatory framework for the placement of radio equipment on the market. It ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects. These include technical features for the protection of privacy, personal data and against fraud. Furthermore, additional aspects cover interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software.

Definition of 'radio equipment' based on 2014/53/EU (RED):

'Radio equipment' means an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination.

The RED shall not apply to equipment specified in Annex I of the Directive itself. Also, it does not apply to radio equipment exclusively used for activities related to public security, defence, state security, or activities concerning the economic well-being of the state in the context of state security matters. Additionally, it excludes radio equipment used for the activities of the state in the area of criminal law enforcement.

Radio equipment that falls within the scope of the RED shall not be subject to Directive 2014/35/EU (Low Voltage Directive), except as outlined in point (a) of Article 3(1) under the 'Essential Requirements' of the Radio Equipment Directive.

To ensure a unified market for radio equipment, several essential requirements have been established. These requirements aim to ensure the safety and health of users by protecting them from harm caused by the equipment, such as electric hazards or physical dangers. They also aim to ensure electromagnetic compatibility (EMC), preventing interference between devices that use the radio spectrum and ensuring that the equipment operates without disrupting other systems or communications. Another key goal is to promote the efficient use of the radio spectrum, minimizing interference and maximizing capacity for all users.

The essential requirements are as follows: Radio equipment shall be constructed to ensure the health and safety of persons, domestic animals, and the protection of property. These objectives are in line with the safety requirements set out in Directive 2014/35/EU, but without imposing a voltage limit. Radio equipment shall be constructed in a way that will ensure an adequate level of electromagnetic compatibility as specified in Directive 2014/30/EU (Electromagnetic Compatibility Directive). Furthermore, it shall be constructed to effectively use and support the efficient use of radio spectrum to avoid harmful interference.

[21] https://energy.ec.europa.eu/topics/markets-and-consumers/wholesale-energy-market/electricity-network-codes-and-guidelines_en#:~:text=These%20rules%2C%20known%20as%20network,EC)714%2F2009

[22] https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng

Additionally, radio equipment in specific categories or classes shall be constructed in a such a way that it complies with the following essential requirements: It must interwork with accessories, particularly common chargers, and it should interconnect via networks with other radio equipment. Radio equipment must be able to connect to interfaces of the appropriate type across the Union. It must avoid misusing network resources in a way that causes unacceptable degradation of service. Furthermore, radio equipment must incorporate safeguards to ensure the protection of the personal data and privacy of both users and subscribers. It must support features that protect against fraud and provide access to emergency services. Additionally, a key essential requirement is that the radio equipment shall support features to facilitate its use by users with disabilities. Finally, the radio equipment includes specific features to ensure that software can only be installed on the equipment when the compliance between the two (radio equipment, software) has been verified.

In 2021, the Commission adopted a Delegated Act of the Radio Equipment Directive activating Articles 3(3)(d), (e) and (f) for certain categories of radio equipment to increase the level of cybersecurity, personal data protection and privacy. [23] This act lays down new legal requirements for cybersecurity safeguards, which manufacturers will have to take into account in the design and production of the concerned products. It will also protect citizens' privacy and personal data, prevent the risks of monetary fraud as well as ensure better resilience of our communication networks. The new measures will help to

- **Improve network resilience**: Wireless devices and products will have to incorporate features to avoid harming communication networks and prevent the possibility that the devices are used to disrupt website or other services functionality.
- **Better protect consumers' privacy**: Wireless devices and products will need to have features to guarantee the protection of personal data. The protection of children's rights will become an essential element of this legislation. For instance, manufacturers will have to implement new measures to prevent unauthorised access or transmission of personal data.
- **Reduce the risk of monetary fraud:** Wireless devices and products will have to include features to minimise the risk of fraud when making electronic payments. For example, they will need to ensure better authentication control of the user in order to avoid fraudulent payments.

This delegated act is complemented by the Cyber Resilience Act.

5.3.13. Regulation for EUIBAs

European Union institutions, bodies, offices, and agencies (EUIBAs), encompassing the EU's seven core institutions (European Commission, European Parliament, European Council, Council of the European Union, Court of Justice of the European Union, European Court of Auditors, and European Central Bank) and its decentralized agencies, rely heavily on interconnected digital systems to perform critical functions such as policymaking, financial oversight, and judicial processes. These entities vary widely in scope and capacity, from the European Parliament's legislative operations to smaller agencies like ENISA, making a uniform cybersecurity approach impractical.

The Regulation (EU, Euratom) 2023/2841[24], adopted on 13 December 2023, establishes measures to ensure a high common level of cybersecurity across these EUIBAs. This regulation is a direct outcome of the EU Cybersecurity Strategy launched in 2020 (see section 5.2), which seeks to secure essential services and enhance collective resilience against cyber threats. In the context of this regulation, prevention is defined as a proactive, systematic approach to identifying, assessing, and mitigating cyber risks before they materialize into incidents. This preventive focus is reinforced by the recognition that EUIBAs are high-value targets for cyberattacks due to their role in managing sensitive political, economic, and operational data. A breach in one entity, such as the European Commission's legislative drafting systems or the European Central Bank's financial oversight tools, could disrupt Union-wide services and undermine public trust.

[23] https://single-market-economy.ec.europa.eu/document/download/492e4668-f9c2-495c-ac11-4379dd2533d9_en

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2841

Prevention under Regulation 2023/2841[25] is operationalized through a multi-layered framework:

- **Risk-based governance:** EUIBAs must conduct regular cybersecurity risk assessments to map vulnerabilities in their digital systems, from cloud-based platforms to on-premises hardware, ensuring that security measures are proportionate to identified threats.
- **Baseline security measures:** Each entity is required to implement technical and organizational safeguards, such as encryption, access controls, and staff training, to prevent breaches.
- **Early warning and coordination:** The regulation mandates rapid incident reporting to CERT-EU[26] (Cybersecurity Service for EUIBAs) within 24 hours of detecting a significant threat, reducing the cascading effects of cyberattacks across EUIBAs.

This contrasts with reactive measures by prioritizing resilience and preparedness, aligning with the EU Cybersecurity Strategy's goal of safeguarding essential services (such as those provided by EUIBAs) against the growing sophistication of cyberattacks (like ransomware, state-sponsored espionage, etc.). The regulation's flexibility accommodates the diversity of EUIBAs, allowing tailored implementation that balances security with operational efficiency.

5.3.14. Commission Implementing Regulation (EU) 2023/203 of 27 October 2022[27]

Commission Implementing Regulation (EU) 2023/203, establishes requirements for organizations and competent authorities in the aviation sector/industry to manage information security risks that could affect aviation safety. This regulation applies to various entities, including those involved in aircraft maintenance, air operations, pilot training, and air traffic management. It mandates that relevant organizations and authorities implement robust information security risk management practices to maintain the integrity and safety of aviation operations.

The regulation aims to:

- Identify and Manage Risks: Ensure that organizations recognize and address information security risks that could impact aviation safety.
- Mandates the implementation of ISMS by various aviation organizations.
- Detect and Respond to Incidents: Establish capabilities to detect information security events, identify incidents, and implement appropriate responses and recovery actions.
- Strengthen the cyber-resilience of the aviation sector within the EU.
- Maintain Safety Standards: Integrate information security risk management into existing safety management systems to uphold high levels of aviation safety.

The regulation entered into force in February 2023. Organizations are required to comply with its provisions by 22 February 2026, except for the EGNOS air navigation service provider, which must comply by 1 January 2026.

5.3.15. Regulation (EU) 2019/2144[28]

The UNECE R155 regulation (United Nations Economic Commission for Europe Regulation No. 155) establishes cybersecurity requirements for vehicles, ensuring that automotive manufacturers implement robust cybersecurity management systems (CSMS). It mandates that passenger cars, trucks, buses, and other vehicle types integrate cybersecurity risk management throughout the vehicle lifecycle, covering design, production, and post-market monitoring. Compliance with UNECE R155 is required for type approval in the EU and other UNECE member countries.

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302841

[26] https://cert.europa.eu/about-us

[27] https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj/eng

[28] https://eur-lex.europa.eu/eli/reg/2019/2144/oj/eng

EU regulation - 2019/2144, also known as the General Safety Regulation (GSR), aligns with UNECE R155 and makes cybersecurity and software update requirements mandatory for vehicles in the EU. It requires that all new vehicles meet cybersecurity and over-the-air (OTA) update security standards by July 2024, ensuring enhanced protection against cyber threats in modern connected and autonomous vehicles. The main points are cybersecurity by design principles, cybersecurity compliance are prerequisite for market access in the EU, collaboration within stakeholders, risk assessment and management, as well as software update.

6. Breakdown of the requirements of the CRA regarding products with digital elements.

The CRA introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the planning, design, development, and maintenance of such products. These obligations must be met at every stage of the value chain. The act also requires manufacturers to provide care during the lifecycle of their products. Some critical products of particular relevance for cybersecurity will also need to undergo a third-party assessment by an authorised body before they are sold in the EU market.

The regulation applies to all products connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules, which is the case for medical devices, aviation and cars. Products will bear the CE marking to indicate that they comply with the CRA requirements. The new rules will rebalance responsibility towards manufacturers, who must ensure their products with digital elements meet cybersecurity standards for the EU market. This will allow buyers to make more informed decisions, trusting the cybersecurity of CE-marked products.

6.1. Structure of the CRA

The enacting terms of the CRA are split into Chapters and Articles and are complemented by Annexes.

The CRA contains 8 (eight) Chapters with a total of 71 (seventy-one) Articles and 8 (eight) Annexes.

The titles of each one as well as the structure is presented below.

Chapter I: General Provisions

- Article 1 – Subject Matter
- Article 2 – Scope
- Article 3 – Definitions
- Article 4 – Free movement
- Article 5 - Procurement or use of products with digital elements
- Article 6 - Requirements for products with digital elements
- Article 7 - Important products with digital elements
- Article 8 - Critical products with digital elements
- Article 9 - Stakeholder consultation
- Article 10 - Enhancing skills in a cyber resilient digital environment
- Article 11 - General product safety
- Article 12 - High-risk AI systems

CHAPTER II: Obligations of economic operators and provisions in relation to free and open-source software

- Article 13 – Obligations of Manufacturers
- Article 14 - Reporting obligations of manufacturers
- Article 15 - Voluntary reporting
- Article 16 - Establishment of a single reporting platform
- Article 17 - Other provisions related to reporting
- Article 18 - Authorised representatives
- Article 19 - Obligations of importers
- Article 20 - Obligations of distributors
- Article 21 - Cases in which obligations of manufacturers apply to importers and distributors

Article 22 - Other cases in which obligations of manufacturers apply

Article 23 - Identification of economic operators

Article 24 - Obligations of open-source software stewards

Article 25 - Security attestation of free and open-source software

Article 26 - Guidance

CHAPTER III: Conformity of the product with digital elements

Article 27 - Presumption of conformity

Article 28 - EU declaration of conformity

Article 29 - General principles of the CE marking

Article 30 - Rules and conditions for affixing the CE marking

Article 31 - Technical documentation

Article 32 - Conformity assessment procedures for products with digital elements

Article 33 - Support measures for microenterprises and small and medium-sized enterprises, including start-ups

Article 34 - Mutual recognition agreements

CHAPTER IV: Notification of conformity assessment bodies

Article 35 – Notification

Article 36 - Notifying authorities

Article 37 - Requirements relating to notifying authorities

Article 38 - Information obligation on notifying authorities

Article 39 - Requirements relating to notified bodies

Article 40 - Presumption of conformity of notified bodies

Article 41 - Subsidiaries of and subcontracting by notified bodies

Article 42 - Application for notification

Article 43 - Notification procedure

Article 44 - Identification numbers and lists of notified bodies

Article 45 - Changes to notifications

Article 46 - Challenge of the competence of notified bodies

Article 47 - Operational obligations of notified bodies

Article 48 - Appeal against decisions of notified bodies

Article 49 - Information obligation on notified bodies

Article 50 - Exchange of experience

Article 51 - Coordination of notified bodies

CHAPTER V: Market surveillance and enforcement

Article 52 - Market surveillance and control of products with digital elements in the Union market

Article 53 - Access to data and documentation

Article 54 - Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk

Article 55 - Union safeguard procedure

Article 56 - Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk

Article 57 - Compliant products with digital elements which present a significant cybersecurity risk

Article 58 - Formal non-compliance

Article 59 - Joint activities of market surveillance authorities

Article 60 - Sweeps

CHAPTER VI: Delegated powers and committee procedure

Article 61 - Exercise of the delegation

Article 62 - Committee procedure

CHAPTER VII: Confidentiality and penalties

Article 63 - Confidentiality

Article 64 - Penalties

Article 65 - Representative actions

CHAPTER VIII: TRANSITIONAL AND FINAL PROVISIONS

Article 66 - Amendment to Regulation (EU) 2019/1020

Article 67 - Amendment to Directive (EU) 2020/1828

Article 68 - Amendment to Regulation (EU) No 168/2013

Article 69 - Transitional provisions

Article 70 - Evaluation and review

Article 71 - Entry into force and application

Annex I: Essential Cybersecurity Requirements

Annex II: Information and Instructions to the User

Annex III: Important products with digital elements

Annex IV: Critical products with digital elements

Annex V: EU Declaration of Conformity

Annex VI: Simplified EU Declaration of Conformity

Annex VII: Content of the technical documentation

Annex VIII: Conformity Assessment Procedures

6.2. Scope of the CRA

The Cybersecurity Act (CRA) establishes (article 1) rules for ensuring the cybersecurity of products with digital elements in the market. It sets essential requirements for the design, development, production, and vulnerability handling processes of products with digital elements. In this respect, the economic operators are obligated to comply with these rules and requirements concerning cybersecurity. Within this framework, CRA also includes provisions for market surveillance, including monitoring and enforcement.

In general, the scope of the CRA (article 2) is to set out requirements and exemptions for products with digital elements, ensuring alignment with existing regulations and cybersecurity standards while safeguarding security interests. In this regard, the Commission has the authority to issue delegated acts to specify limitations or exclusions.

Specifically, according to article 2 of CRA, the Regulation applies to products with digital elements that are connected to a device or network, covering those with direct or indirect data logical or physical connections.

However, **it does not apply** to

- products falling under specific EU legal acts **such as** regulations related to **medical devices, in vitro diagnostic medical devices**, and **motor vehicle type-approval requirements** (Regulations (EU) 2017/745, 2017/746, 2019/2144 respectively).
- products that have been certified under the common rules in **civil aviation** (Regulation (EU) 2018/1139) or fall within the scope of marine equipment Directive are also exempt (2014/90/EU).
- (may not apply to) products covered by **other Union rules addressing cybersecurity risks** if those rules provide equal or higher protection.
- spare parts for digital products if they match original components' specifications for replacement. Furthermore, spare parts for products with digital elements and those designed for national security, defense purposes, or handling classified information are also excluded.

Further information on the exclusions is provided in Section 6.3.

Lastly, the Regulation does not entail the disclosure of information that could jeopardize national security, public security, or defense of essential interests of Member States.

Digital Products play a crucial role in digital security, network management, and privacy protection. According to the definition provided by the CRA (art. 3, definitions)

A "**product with digital elements**" refers to a "**software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately**".

Where, remote data processing' means **data processing at a distance** for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions.

Examples of such devices include:

smartphones, laptops, smart home products, smart watches, internet connected toys, but also microprocessors, firewalls and smart meters.

In simpler terms, a product with digital elements can be:

- A **Software** that has or is able to have a **data** or **network connection** during use, e.g. accounting software, software firewalls, security information and event management (SIEM)
- **Hardware** that has or is able to have a **data** or **network connection** during use, e.g. smartphones, laptops, home cameras, smartwatches, connected toys, but also modems, firewalls, and smart meters
- A **hardware** product requiring a **direct or indirect logical** or **physical data connection** to a device or network, e.g. industrial control systems, sensors.

The CRA **classifies** the digital products into **categories**.

6.2.1. Important products with digital elements

Products with digital elements which have **the core functionality** of a product category set out in Annex III of the CRA shall be considered to be **important products** with digital elements and shall be subject to the **conformity assessment procedures referred to in Article 32(2) and (3)** of the CRA. The integration of a product with digital elements which has the core functionality of a product category set out in Annex III of the CRA shall not in itself render the product in which it is integrated subject to the conformity assessment procedures referred to in Article 32(2) and (3) of the CRA.

Annex III of the published versions of the CRA[29], provides a list of 23 types of products which should be classified as Important products with digital elements split into two Classes (Class I and Class II).

[29] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847#anx_III

Class I

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
2. Standalone and embedded browsers
3. Password managers
4. Software that searches for, removes, or quarantines malicious software
5. Products with digital elements with the function of virtual private network (VPN)
6. Network management systems
7. Security information and event management (SIEM) systems
8. Boot managers
9. Public key infrastructure and digital certificate issuance software
10. Physical and virtual network interfaces
11. Operating systems
12. Routers, modems intended for the connection to the internet, and switches
13. Microprocessors with security-related functionalities
14. Microcontrollers with security-related functionalities
15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities
16. Smart home general purpose virtual assistants
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
18. Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council (1) that have social interactive features (e.g. speaking or filming) or that have location tracking features
19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children

Class II

1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
2. Firewalls, intrusion detection and prevention systems
3. Tamper-resistant microprocessors
4. Tamper-resistant microcontrollers

Between, 13 March 2025 - 18 April 2025, the European Commission published a proposal for the Technical Description of important and critical products with digital elements and received feedback from various interested parties, including the CURIUM project.

The proposal was related to the requirement of the CRA for the Commission to specify the technical description of the categories of important and critical products with digital elements listed in Annex III and IV to the Regulation. Such products may be subject to more stringent conformity assessment procedures, as set out in Article 32. The documents provided were 1) a Draft implementing regulation – Ares (2025)2037850 and 2) an Annex of descriptions of products with digital elements.

This proposal for an implementing regulation, notes further on the definition of products:

Pursuant to Article 7(1) and Article 8(1) of Regulation (EU) 2024/2847, the **core functionality of a product with digital elements determines** whether that product with digital elements fits into the technical description of a **category of important or critical products with digital elements** and therefore the applicable conformity assessment procedures. A **product's core functionality refers** to its **fundamental features and capabilities that fulfil the primary purpose** for which the product with digital elements has been made available on the market and without which the product would not be able to meet its **intended purpose or reasonably foreseeable use**.

Whereas the fact that a product with digital elements **performs functions other than or additional to those detailed in the technical descriptions** set out in the Annexes **does not in itself mean that the product with digital elements does not have the core functionality** of a product category set out in the Annexes.

The proposal does not introduce new categories of products (the 19+4 presented above) but rather provides technical description of these categories as the fall within the scope of the CRA.

Table 6-1Table 6-1 Example of proposed Annex I for the technical descriptions of important products with digital elements shows an example of these technical descriptions.

Table 6-1 Example of proposed Annex I for the technical descriptions of important products with digital elements

Category of product	Technical description
1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers	Identity management systems are products with digital elements that provide mechanisms for identity lifecycle management, such as identity provisioning, maintenance, authentication, authorisation and deprovisioning, and including associated metadata. Privileged access management hardware and software are products with digital elements that authenticate and authorise users or devices, granting or denying access to digital resources or to physical locations. This category includes but is not limited to products with digital elements that have the core functionality of either or both identity management and privileged access management; authentication and access control readers; biometric readers; single sign-on software; federated identity management software and multi-factor authentication software.
2. Standalone and embedded browsers	Standalone browsers are standalone applications that fulfil the functions of browsers.
	Embedded browsers are browsers that are intended for integration into another system or application.
	In the context of this category of products, browsers are software products with digital elements that enable end users to access and interact with web content hosted on servers that are connected to networks such as the Internet.

These technical descriptions are expected to be finalized within 2025, since based on the CRA (Article 7), "By 11 December 2025, the Commission shall adopt an implementing act specifying the technical description of the categories of products with digital elements under classes I and II as set out in Annex III and the technical description of the categories of products with digital elements as set out in Annex IV".

6.2.2. Critical products with digital elements

The categories of critical products with digital elements set out in this Regulation have a cybersecurity-related functionality and perform a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements through direct manipulation. The categories of critical products with digital elements set out in Annex IV of the CRA, due to their criticality, already widely use various forms of certification, and are also covered by the European Common Criteria-based cybersecurity certification scheme (EUCC) set out in Commission Implementing Regulation (EU) 2024/482.

Annex IV of the published version of the CRA[30], provides a list of 3 types of products which should be classified as Critical products with digital elements. These products are:

1. Hardware Devices with Security Boxes

2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council[31] and other devices for advanced security purposes, including for secure crypto processing

3. Smartcards or similar devices, including secure elements

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847#anx_IV

[31] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).

As presented in Section A. on Important products above, the proposal for the technical description of the categories of important and critical products with digital elements listed in Annex III and IV to the Regulation also covers Critical products.

Table 6-2 Table 6-1 Example of proposed Annex I for the technical descriptions of important products with digital elements shows an example of these technical descriptions.

Table 6-2 Example of proposed Annex I for the technical descriptions of critical products with digital elements

Category of product	Technical description
1. Hardware Devices with Security Boxes	Hardware products with digital elements that incorporate a hardware physical envelope providing countermeasures against physical attacks, including tamper evidence, resistance or response, and that are designed to securely store, process, and manage sensitive data and cryptographic operations. This category includes but is not limited to payment terminals, hardware security modules, and tachographs that meet the above definition.
2. Smart meter gateways within smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944 of the European Parliament and of the Council[4] and other devices for advanced security purposes, including for secure cryptoprocessing	Products with digital elements that control communication between components in smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944 and authorised third parties, such as utility providers, as well as other devices within the smart grid infrastructure, that collect, process and store meter data, and that also protect data and information flows by supporting specific cryptographic needs, such as encryption and decryption of data, and by firewalling between the wider network and the local network. This category includes but is not limited to smart meter gateways related to smart metering systems measuring electricity as defined in Article 2(23) of Directive (EU) 2019/944. It may also include other smart metering systems measuring consumption of other sources of energy such as gas or heat.

6.2.3. Products with digital elements belonging to the "Default" category

This category, usually referred to as Default, includes all products with digital elements that are not explicitly listed as either important or critical. This category is the largest one and is estimated to represent approximately 90% of all products with digital elements. **Products falling under the default category should use the self-assessment method to demonstrate compliance with CRA.**

6.2.4. High-risk AI systems

Products with digital elements which are classified as high-risk AI systems[32], are considered to be within the scope of the CRA. For these products, the requirement for fulfilling the essential requirements set out in Part I of Annex I of the CRA and the processes put in place by the manufacturer to comply with the essential cybersecurity requirements set out in Part II of Annex I of the CRA persist. Additionally, for these products, the achievement of the level of cybersecurity protection required under Article 15 of the AI Act is demonstrated in the EU declaration of conformity issued under the CRA. To fulfil the conformity assessment requirements for these products, notified bodies which are competent to control the conformity of the high-risk AI systems under the AI Act shall also be competent to perform these assessment procedures provided they follow the required evaluation and notification processes.

6.3. CRA scope exclusions

The CRA does not apply to products with digital elements, which are:

- **Medical devices** as defined and regulated by the Regulation (EU) 2017/745. Meaning any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, or diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, or investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, or providing information by means of in vitro examination of specimens derived from the human body, including

[32] Article 6 of the AI Act. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

organ, blood and tissue donations and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

Exception to the above are: personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children, which are within the scope of the CRA.

- **In vitro diagnostic medical devices** as defined and regulated by the Regulation (EU) 2017/746. meaning any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on a physiological or pathological process or state or concerning congenital physical or mental impairments or concerning the predisposition to a medical condition or a disease or to determine the safety and compatibility with potential recipients or to predict treatment response or reactions or to define or monitoring therapeutic measures.
- **Motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles** as defined and regulated by the Regulation (EU) 2019/2144. Meaning vehicles of categories M, N and O, as defined in Article 4 of Regulation (EU) 2018/858, and to systems, components and separate technical units designed and constructed for such vehicles (Vehicles having at least four wheels and used for the carriage of passengers, power-driven vehicles having at least four wheels and used for the carriage of goods, trailers).
- **Products certified under the Regulation (EU) 2018/1139.** Meaning products, parts and equipment to control aircraft remotely, covering also the esign, production, maintenance and operation of aircraft, as well as their engines, propellers, parts, non-installed equipment and equipment to control aircraft remotely, safety-related aerodrome equipment used or intended for use at the aerodromes, ATM/ANS in the Single European Sky airspace.

  Exception to the above are: aircrafts, and their engines, propellers, parts, non-installed equipment and equipment to control aircraft remotely, while carrying out military, customs, police, search and rescue, firefighting, border control, coastguard or similar activities , which are within the scope of the CRA.
- **Equipment that falls within the scope of Directive 2014/90/EU** of the European Parliament and of the Council. Meaning equipment placed or to be placed on board an EU ship and for which the approval of the flag State administration is required by the international instruments
- **Spare parts** that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace;
- **Products with digital elements** developed or modified exclusively for **national security or defence** purposes or to products specifically designed to process classified information;
- **Websites** that do not support the functionality of a product with digital elements, or **SaaS / PaaS / IaaS services cloud services** designed and developed outside the responsibility of a manufacturer of a product with digital elements;
- Products with digital elements qualifying as **free and open-source software** that are not **monetized by their manufacturers**. Free and open-source software (FOSS) presents a unique challenge: it is widely

used and critical to many products yet often developed outside traditional commercial models. The CRA recognizes that securing such software cannot fall solely on manufacturers who integrate it, the communities developing and maintaining it must also play a role. Articles 24 and 25 reflect a thoughtful approach, integrating FOSS into this framework (specifically FOSS intended for commercial activities, not all open-source software) while balancing cybersecurity with the need to foster innovation. Article 25 of the CRA empowers the European Commission to establish voluntary security attestation programs for FOSS to support manufacturers integrating such software into their products with digital elements. These programs assist manufacturers integrating such software into their products by offering an optional security validation mechanism.

6.4. CRA interested parties (including Economic Operators)

As mentioned already, the CRA introduces a comprehensive regulatory framework aimed at enhancing cybersecurity across the supply chain of products with digital elements and thus it affects various stakeholders.

The stakeholders can be split into two groups: Economic operators and other stakeholders.

The term '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.

In this section, a short overview is provided of different stakeholders related to the CRA.

- **Manufacturer:** A natural or legal person that designs, develops, or produces products with digital elements and markets them under their own name or trademark, whether for payment, monetisation or free of charge.
- **Importer:** A natural or legal person established within the EU that place products with digital elements on the market which carry the name or trademark of a natural or legal person established outside the EU.
- **Distributor:** A natural or legal person, other than the manufacturer or the importer, that makes a product with digital elements available in the EU market without modifying it.
- **Authorised Representative:** A natural or legal person established within the EU who has received a written mandate from a manufacturer to act on its behalf concerning specific tasks.
- **Open-Source Software Steward:** A legal person, other than a manufacturer, that provides sustained support for the development and viability of specific open-source products with digital elements intended for commercial activities.
- **Market Surveillance Authority:** Each EU Member State designates one or more market surveillance authorities responsible for ensuring the effective implementation of the CRA. Where relevant, it shall cooperate with the national cybersecurity certification authorities and exchange information on a regular basis. It should also cooperate and exchange information on a regular basis with the CSIRTs designated as coordinators and ENISA
- **Consumer:** A natural person purchasing or using the product for personal reasons (end user).

6.5. Obligations of Economic operators

The CRA establishes specific responsibilities for economic operators, which include manufacturers, authorised representatives, importers, distributors, or other natural or legal persons who are 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. These responsibilities are mainly described in Articles 13, 14, 15, 18, 19, 20, and 24.

6.5.1. Manufacturers (Articles 13, 14, 15)

Manufacturers must ensure that their products are designed, developed, and produced to meet essential cybersecurity requirements, as specified in Annex I, Part I. This involves conducting a cybersecurity risk assessment throughout the product lifecycle—during planning, design, development, production, delivery, and maintenance. The results of this assessment must be documented and updated as necessary. The risk assessment should consider factors like the intended use, environment, and assets the product aims to protect.

Manufacturers are also responsible for ensuring that third-party components, including free and open-source software, do not compromise the product's cybersecurity. If any vulnerabilities are found, whether in the product itself or in third-party components, manufacturers must report them and implement remedial actions. They should also share relevant information with the component's suppliers when a fix is developed.

Before market placement, manufacturers must conduct conformity assessments, draw up technical documentation and an EU declaration of conformity, and affix the CE mark. Additionally, they must define a support period for the product, which should last at least five years. During this period, vulnerabilities must be effectively handled, and security updates must remain available for a minimum of 10 years or for the duration of the support period, whichever is longer.

Clear instructions on secure installation, operation, and use must be provided to users, along with information about updates, vulnerabilities, and the end of the support period. Manufacturers must also take immediate corrective measures if they discover that a product or process does not comply with the cybersecurity requirements. If necessary, they must withdraw or recall the product from the market.

Manufacturers are required to cooperate with market surveillance authorities by providing all relevant documentation and evidence of compliance when requested. If a manufacturer ceases operations and is unable to meet these obligations, they must inform both market surveillance authorities and users. Furthermore, manufacturers may need to provide a Software Bill of Materials (SBOM) listing all components used in the product, especially open-source software, to ensure transparency and security.

Moreover, the dedicated Administrative Cooperation group (ADCO) may conduct assessments to understand the dependency on software components, and manufacturers may be asked to supply relevant information to assist in this process. Throughout, the regulations emphasise transparency, accountability, and ongoing vigilance to manage cybersecurity risks effectively.

Furthermore, taking into consideration the reporting obligations regarding vulnerabilities and incidents affecting the security of products with digital elements, manufacturers are required to notify the Computer Security Incident Response Team (CSIRT) designated as coordinator and ENISA when they become aware of any actively exploited vulnerabilities. The notifications must be made through a single reporting platform and include several details, such as early warning notifications within 24 hours, vulnerability notifications within 72 hours, and a final report within 14 days after a corrective measure is available. Similarly, manufacturers must report severe security incidents impacting their products, with initial notifications within 24 hours, followed by incident notifications within 72 hours, and a final report within one month.

The definition of a "severe incident" includes situations where the product’s ability to protect sensitive data is compromised or malicious code is introduced. Manufacturers may also be asked to submit intermediate reports to update authorities on the status of a vulnerability or incident. If the manufacturer has no main establishment in the EU, they must report to the CSIRT designated as coordinator in the Member State with the highest number of impacted products or users.

After learning of a vulnerability or security incident, manufacturers must inform impacted users and provide guidance on corrective measures. If the manufacturer fails to notify users in time, the CSIRTs may step in to share the information.

Finally, manufacturers, as well as other natural or legal persons, are encouraged to voluntarily report any vulnerabilities in a product or potential cyber threats that could impact the product's risk profile to a CSIRT designated as coordinator or to ENISA. Similarly, they may report incidents affecting the security of the product or near misses that could have resulted in such incidents.

6.5.2. Authorized Representatives (Articles 18, 15)

A manufacturer may appoint an authorised representative through a written mandate. However, the authorised representative is not responsible for the obligations outlined in Article 13(1) to (11), (12) first subparagraph, and (14).

The authorised representative's duties are defined by the mandate received from the manufacturer. They must, upon request from market surveillance authorities, provide a copy of this mandate. The representative's mandate must include at least three core responsibilities:

- maintaining the EU declaration of conformity (Article 28) and technical documentation (Article 31) for a minimum of 10 years after the product with digital elements is placed on the market, or for the product's support period, whichever is longer.
- providing any necessary information and documentation to authorities to demonstrate the product's conformity with regulatory requirements.
- cooperating with market surveillance authorities in actions aimed at mitigating risks posed by the product.

6.5.3. Importers (Articles 19, 15)

Importers are responsible for ensuring that the products they place on the market comply with essential cybersecurity requirements set out in Annex I, Part I & II. Before distributing a product, they must ensure that the manufacturer has completed the appropriate conformity assessments (Article 32), prepared the required technical documentation, affixed the CE marking (Article 30), and provided the necessary EU declaration of conformity (Article 13(20)), user instructions, and language requirements as set out in Annex II. Importers must also verify that the manufacturer has met specific obligations, such as those related to risk assessments and vulnerability management (Article 13(15), (16) and (19)).

If an importer believes that a product or its manufacturing processes do not comply with the regulation, they are prohibited from placing it on the market until the product is in conformity. If the product presents a significant cybersecurity risk, the importer must notify the manufacturer and market surveillance authorities. Importers must also assess non-technical risk factors that could affect cybersecurity and inform the authorities if they believe the product poses a significant risk.

Importers are required to provide their contact details on the product or its packaging, ensuring they are easily understood by users and market surveillance authorities. If a product placed on the market is found to be non-compliant, the importer must take corrective measures, including withdrawal or recall if necessary. If a vulnerability is discovered, the importer must inform the manufacturer and notify authorities if the product poses a significant risk. Importers must also retain the EU declaration of conformity and technical documentation for at least 10 years or for the product's support period, whichever is longer, and make them available to market surveillance authorities upon request.

In the event that the manufacturer ceases operations and can no longer fulfil its regulatory obligations, the importer must inform the relevant market surveillance authorities and, if possible, alert users of the affected product.

6.5.4. Distributors (Articles 20, 15)

Distributors are required to act with due care to ensure compliance with the regulation when making such products available on the market. Before distributing a product, they must verify that the product carries the CE marking and that the manufacturer and importer have met all obligations specified in the regulation (Article 13(15), (16), (18), (19) and (20) and Article 19(4)), providing the necessary documentation. If a distributor believes, based on available information, that a product does not meet essential cybersecurity requirements, they must refrain from distributing the product until the necessary corrections are made. If a product poses a significant cybersecurity risk, they must promptly inform the manufacturer and relevant market surveillance authorities.

Distributors are also obligated to take corrective measures if they discover that a product or its manufacturing processes do not comply with the regulation. They must ensure that appropriate steps are taken to rectify the issue or, if necessary, withdraw or recall the product. If a vulnerability is identified in the product, the distributor must inform the manufacturer immediately and notify the market surveillance authorities if the product poses a significant cybersecurity risk. They must provide the necessary information to the authorities, in an easily understandable format, and cooperate with them on any actions taken to mitigate cybersecurity risks.

Additionally, if a distributor learns that the manufacturer has ceased operations and can no longer meet the regulation’s obligations, the distributor must inform the relevant market surveillance authorities and, as far as possible, alert users of the affected products

6.5.5. Open-Source Software Stewards (Articles 24,15)

Open-source software stewards must establish and document a cybersecurity policy to ensure the development of secure digital products and manage vulnerabilities effectively. This policy should encourage the voluntary reporting of vulnerabilities by developers, address the documentation, remediation, and sharing of vulnerabilities within the open-source community, and consider the specific characteristics of the steward's legal and organisational structure. Furthermore, open-source software stewards are required to cooperate with market surveillance authorities to mitigate cybersecurity risks in free and open-source software products. Upon a justified request from these authorities, stewards must provide relevant documentation in a format that is easily understandable, either in paper or electronic form. Open-source stewards must comply with obligations from Article 14(1), related to the development of products with digital elements, and follow specific provisions from Articles 14(3) and (8) when severe cybersecurity incidents impact the security of these products or related network systems.

6.6. Essential Cybersecurity Requirements

The CRA mandates that the products with digital elements fulfil a set of requirements named as "Essential Cybersecurity Requirements". These requirements are included in Annex A of the regulation and are split into two parts. The first part related to requirements relating to the properties of products with digital elements and the second one to the handling of vulnerabilities by the manufacturers.

Part I:

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities.

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access.

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means.

(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions.

(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation).

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks.

(j) be designed, developed and produced to limit attack surfaces, including external interfaces.

(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.

(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.

(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Part II

(1) identify and document 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.

(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates.

(3) apply effective and regular tests and reviews of the security of the product with digital elements.

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(5) put in place and enforce a policy on coordinated vulnerability disclosure.

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements.

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner.

(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

6.7. Technical Documentation

One more of the requirements imposed by the CRA, as stated in Article 31, is for technical documentation to be drawn up/written before the product with digital elements is placed on the market and be continuously updated, where appropriate, at least during the support period.

The technical documentation shall contain at least the following information, as applicable to the relevant product with digital elements:

1. a general description of the product with digital elements, including:

   (a) its intended purpose.

   (b) versions of software affecting compliance with essential cybersecurity requirements.

(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout.

(d) user information and instructions as set out in Annex II;

2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:

   (a) necessary information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing.

   (b) necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates.

   (c) necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes.

3. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained pursuant to Article 13, including how the essential cybersecurity requirements set out in Part I of Annex I are applicable.

4. relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements.

5. a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 27 of this Regulation or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 pursuant to Article 27(8) of this Regulation, and, where those harmonised standards, common specifications or European cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential cybersecurity requirements set out in Parts I and II of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or European cybersecurity certification schemes, the technical documentation shall specify the parts which have been applied.

6. reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential cybersecurity requirements as set out in Parts I and II of Annex I.

7. a copy of the EU declaration of conformity.

8. where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for that authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I.

The above ensure that all necessary technical details for verifying compliance with the Cyber Resilience Act are documented and available for market surveillance and regulatory review.

Furthermore, products with digital elements must be accompanied by the following user information:

1. Manufacturer details (name, address, and contact email).
2. Contact information for reporting cybersecurity vulnerabilities.
3. Identification of the product (e.g., batch or serial number) and corresponding instructions.
4. The intended use and security environment for the product, including essential functions.
5. Known or foreseeable cybersecurity risks during normal or misuse conditions.
6. Access information for the software bill of materials (if applicable).

7. Access details for the EU declaration of conformity.
8. Technical support availability and details about security updates.
9. Detailed instructions on secure commissioning, data security during use, updating processes, and secure decommissioning of the product, including data removal.

6.8. Proof of conformity

A critical component of any compliance process is the “proof of conformity”, which is the evidence ensuring that products meet security standards requirements before they are placed on the market. The “proof of conformity” is demonstrated through conformity assessments procedure, the EU Declaration of Conformity.

The CRA mandates that manufacturers, importers, and distributors to prove conformity based on self-assessment for lower-risk products (default, non-critical category) and obligate third-party evaluation for important and critical products (Annex III and Annex IV- Class I and Class II).

These obligations are detailed, and explained and proof of conformity relies on them in next CRA Articles:

- Article 27 (Presumption of conformity),
- Article 28 (EU Declaration of Conformity),
- Article 29 (CE Marking), and
- Article 32 (Conformity Assessment Procedures).

Article 27 introduces the presumption of conformity, which allows manufacturers to assume compliance if their product adheres to:

- Harmonized Standards (HS)—These are official EU cybersecurity standards adopted under Regulation (EU) 1025/2012. If a product meets these standards, it is presumed to comply with the CRA.
- Common Specifications (CS) – If harmonized standards do not exist or are not sufficient, the European Commission may issue common specifications as an alternative. Products meeting these specifications are also presumed to be compliant.
- European Cybersecurity Certification (under Regulation (EU) 2019/881) – If a product has been certified under an EU cybersecurity certification scheme at a "substantial" or "high" assurance level, it is presumed to conform to the CRA’s security requirements.

This presumption of conformity simplifies the compliance process for manufacturers who follow recognized cybersecurity standards. Manufacturers also must ensure that conformity assessments are conducted before the product is placed on the market and that they remain valid throughout the product lifecycle.

Article 28 requires from manufacturers to create and issue an EU Declaration of Conformity, a legally binding document confirming that the product complies with the CRA's requirements. This declaration must:

- Be structured according to the template in Annex V.
- Include product identification details (model, version, unique identifier).
- State compliance with harmonized standards or common specifications.
- Be signed by a representative of the manufacturer.
- Be kept for at least 10 years after the product is placed on the market.

This declaration ensures traceability and accountability, making it easier for market authorities to verify compliance.

Article 29 of the Cyber Resilience Act (CRA) states that the CE marking must comply with the general principles outlined in Article 30 of Regulation (EC) No 765/2008.

Regulation (EC) No 765/2008, which establishes the CE marking framework, defines in Article 30 that:

- The CE marking is a declaration by the manufacturer that the product complies with all applicable EU legal requirements (not just the CRA but also other relevant regulations, such as the Low Voltage Directive or the Machinery Regulation).
- The CE marking must be visibly, legibly, and permanently affixed to the product, its packaging, or accompanying documents.
- No additional markings may mislead users about the meaning or form of the CE marking.
- If third-party certification (notified body) is required, the notified body's identification number must be placed next to the CE marking.
- Member States must ensure the correct use of the CE marking and prevent misuse.

This means that the CE marking under the CRA follows the same strict rules as in other EU legislation, ensuring uniform application across industries and preventing fraudulent or misleading markings.

Article 32 details the specific procedures manufacturers must follow to assess compliance. These are further outlined in Annex VIII, which defines three main approaches:

Internal Control (Module A) – Self-Assessment

- Used for non-critical products.
- Manufacturers internally ensure compliance and prepare technical documentation.

EU-Type Examination (Modules B & C) – Third-Party Certification

- Required for critical products in Annex III or IV.
- A notified body reviews the product's technical design, cybersecurity measures, and vulnerability handling processes.
- After approval, the manufacturer ensures conformity in production (Module C).

Specifically, the conformity to type based on internal production control (based on module C) is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations related to the "Production" and "Conformity marking and declaration of conformity". This procedure ensures and declares that the products with digital elements are in conformity with the type described in the EU-type examination certificate and satisfy the essential cybersecurity requirements (Part I, Annex I) and that the manufacturer meets the essential cybersecurity requirements (Part II, Annex I).

The manufacturers shall take all necessary actions and measures that both the product and its monitoring ensure conformity of the manufactured products with digital elements with the approved type mentioned in the EU-type examination certificate, as well as with the essential cybersecurity requirements (Part I, Annex I). Additionally, the manufacturer shall ensure it meets the essential cybersecurity requirements (Part II, Annex I).

Upon ensuring that each product with digital elements conforms to the type described in the EU-type examination certificate and satisfies all applicable requirements, the manufacturer shall then proceed to affix the CE marking to each product.

Furthermore, the manufacturer shall proceed with the preparation of the declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product with digital element has been placed on the market or for the support period, whichever is longer. This declaration of conformity shall clearly identify the product model it pertains to. Also, upon request, a copy of this declaration of conformity shall be made available to the relevant authorities.

The manufacturer's above-mentioned obligations may be fulfilled by its authorized representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

Full Quality Assurance (Module H)

- The most stringent procedure.

- A notified body audits the manufacturer's entire design, production, and cybersecurity management system.
- Used for high-risk products that require ongoing oversight.

For critical products, third-party assessment is mandatory, while less critical products may follow self-assessment procedures.

6.9. EU Declaration of Conformity

Annex V of the CRA provides the official template for the EU Declaration of Conformity (referred to in Article 28). It ensures that the declaration includes essential information such as: Name and type and any additional information enabling the unique identification of the product with digital elements. Elements which must be included are: Name and address of the manufacturer or its authorised representative, a statement that the EU declaration of conformity is issued under the sole responsibility of the provider, Object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate), A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation, References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued and Additional information like: Signature, place and date of issue, name, function. An example of the EU Declaration of Conformity is provided in this document in Section 11.

This document must be kept on file for at least 10 years and must be made available to market surveillance authorities upon request.

7. Analysis of related certification policies, standards and developments on standardization.

7.1. Standardization and the CRA

As shown in Section 5, CRA sets out essential cybersecurity requirements for manufacturers and economic operators and applies to all products connected, either directly or indirectly to another device or network except for specified exclusions. In addition, CRA lays down rules and requirements, which constitute the core obligations imposed on manufacturers and economic operators: a) rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products, b) essential cybersecurity requirements for the design, development, and product of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity, c) essential cybersecurity requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the products are expected to be in use, and obligations for economic operators in relation to those processes. These essential requirements apply to any product with digital elements placed on the EU internal market.

It is critically important, in order to support the effective implementation of the CRA, the essential cybersecurity requirements to be translated into harmonized standards, providing a clear and consistent path for manufacturers to demonstrate compliance. To achieve this, the essential requirements should be addressed through a standardization process carried out by European Standardisation Organizations (ESOs), with the goal of developing 41 harmonized standards [33]. A relevant standardization request was sent by the European Commission to the ESOs, in April 2024, requesting the development of Horizontal standards for security requirements relating to the properties of products with digital elements (14), Horizontal standards for vulnerability handling requirements (1) and Vertical standards for security requirements relating to the properties of products with digital elements (26). The standardization request describes the type of standard request as well as a deadline for the adoption of the standard by the ESOs.

The standards should include detailed technical specifications of the essential cybersecurity requirements, with respect to the design, development and production of products with digital elements as well as to the processes for vulnerability handling. They should also indicate clearly the correspondence between technical specifications and the essential cybersecurity requirements they aim to cover. The standards should ensure that the developed European Standards and European standardisation deliverables are consistent with the EU legal framework. Furthermore, the European Standardisation Organisations, recognized by both the industry and scientific communities, are considered particularly relevant to the specific area covered by this Regulation. As such, they are responsible for developing the corresponding standards to be established under the Cyber Resilience Act.

The European Standardization Organizations referred to above are:

- **CEN**: European Committee for Standardization
- **CENELEC**: European Committee for Electrotechnical Standardization
- **ETSI**: European Telecommunications Standard Institute
- **ISO**: International Organization for Standardization
- **IEC**: International Electrotechnical Commission
- **ITU**: International Telecommunication Union

For each of the organizations listed above, the relevant committees involved in the development of the CRA standards have been identified. These committees are tasked with developing European standards on designing, developing, and producing products with digital elements in such a way that they ensure an appropriate level of

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

cybersecurity based on the risks. For each committee, its standardization activities include ongoing activities, with potential relevance for the mapping have been identified, drafting a list of respecting standards. For example, one of the committees contributing to the development of standards for CRA is JTC13/WG9, which stands for Joint Technical Committee 13 on "Cybersecurity and Data Protection", Working Group 9.

In April 2024, a Joint Analysis was published on the Cyber Resilience Act Requirements Standards Mapping by the Joint Research Centre and ENISA. In this document, each CRA requirement is mapped against relevant standards. For each standard the level of coverage offered for the requirement and possible gaps to be considered are discussed.

The following table, presents the summary of the identified standards and their suitability regarding specific requirements of the CRA

Table 7-1 Overall list of the identified standards with their respective mapping towards the security requirements

Standard	1	2	3a	3b	3c	3d	3e	3f	3g	3h	3i	3j	3k
EN ISO/IEC 27002:2022	X		X					X			X	X	X
EN ISO/IEC 27005:2022	X												
EN IEC 62443-3-2:2020	X											X	
EN IEC 62443-4-1:2018	X	X											
ISO/IEC 18045:2022		X										X	
ITU-T X.1214 (03/2018)		X											
ETSI EN 303 645 V2.1.1 (2020-06)	X	X	X	X	X	X	X	X	X	X	X	X	X
ISO/IEC 18031:2011			X										
ISO/IEC 9798, Parts 1 to 6				X									
ISO/IEC 24760, Parts 1 to 3				X									
ISO/IEC 29146:2016				X									
ITU-T X.1253 (09/2011)				X									
ITU-T X.812 (11/1995)				X									
EN IEC 62443-4-2:2019				X	X	X		X		X		X	X
ITU-T X.805 (10/2003)					X			X					
ISO/IEC 18033, Parts 1 to 7					X								
ITU-T X.814 (11/1995)					X								
ISO/IEC 9796, Parts 2 and 3						X							
ISO/IEC 9797, Parts 1 to 3						X							
ISO/IEC 14888, Parts 1 to 3						X							

Standard	1	2	3a	3b	3c	3d	3e	3f	3g	3h	3i	3j	3k
ITU-T X.815 (11/1995)						X							
ISO/IEC 27701:2019							X						
ISO/IEC 29100:2011							X						
ETSI TS 103 485 V1.1.1 (2020-08)							X						
ISO/IEC 22237-1:2021								X					
ITU-T Y.4810 (11/2021)									X				
ISO/IEC TS 19249:2017										X			
ISO/IEC 15408-2:2022										X			
ISO/IEC 27001:2022											X		
ISO/IEC 27034-1:2011											X		
EN ISO/IEC 15408-3:2022											X		
ISO/IEC 13888-1:2020												X	
ISO/IEC 30111:2019													X
IEC 62443-2-1:2010													X

Where:

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.
(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities.
(3a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state.
(3b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems.
(3c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms.
(3d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions.
(3e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data').
(3f) protect the availability of essential functions, including the resilience against.
and mitigation of denial of service attacks.
(3g) minimise their own negative impact on the availability of services provided by other devices or networks;
(3h) be designed, developed and produced to limit attack surfaces, including external interfaces.
(3i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.
(3j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions.
(3k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

There are several security standards published by different Standards Developing Organizations (SDOs) including ISO and NIST related to products with digital elements. The main aim of such standards is to provide a framework

to manage security from all aspects of the product with digital elements. This section provides an overview of the existing standards to identify cybersecurity requirements, security properties and evaluation criteria of products with digital elements that are widely used across the sectors.

Table 7-2 Overall list of the identified standards with their respective mapping towards the vulnerability handling requirements

Standard	1	2	3	4	5	6	7	8
ISO/IEC 27036, Parts 1 to 3	X							
ISO/IEC 27001:2022		X	X					
ISO/IEC 27002:2022		X	X				X	X
EN ISO/IEC 30111:2020		X		X	X	X		X
EN ISO/IEC 29147:2020		X		X	X	X		
IEC 62443-4-1:2018		X		X			X	X
ISO/IEC TS 27034-5-1:2018								
ETSI EN 303 645 V2.1.1 (2020-06)			X					

Where:

Manufacturers of the products with digital elements shall:
(1) identify and document vulnerabilities and components contained in the product, including 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 product
(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates.
(3) apply effective and regular tests and reviews of the security of the product with digital element.
(4) once a security update has been made available, publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities.
(5) put in place and enforce a policy on coordinated vulnerability disclosure.
(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements.
(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner.
(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken

The conclusion of the analysis is summarized as follows:

There is already at least one document (standard) that can be considered as an initial reference offering some coverage to each of the identified requirements. However, there is not a single standard capable of covering all the requirements expressed in the proposed legislative act, even if some of the standards do partially cover all of the requirements. The analysis offers re-assurance that a good international cybersecurity standardisation base is already in place for serving the scope of the Cyber Resilience Act requirements, but harmonisation is needed to ensure a homogeneous horizontal coverage, and some gaps, as highlighted in this report, need still to be addressed.

Within the work program of CEN/CLC/JTC 13/WG 9, the following three projects are referenced as being under drafting:

Table 7-3 Projects, their description and status being developed by CEN/CLC/JTC 13/WG 9

Project reference	Status	Initial Date	Current Stage	Next Stage	Forecasted voting date
prEN XXX (WI=JT013089) **Cybersecurity requirements for products with digital elements - Principles for cyber resilience**	Under Drafting	2025-03-05	2025-05-13	2025-09-09	2026-10-27
This document (standard) provides a framework covering all elements defined in section 1 of Annex II of the standardization request and sets out principles and specifications for the planning, design, development, production, delivery and maintenance of products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks, in accordance with the manufacturers' obligations under article 13 of the CRA and in support of the compliance with the essential requirements of Annex I of the CRA. In addition, this standard will, amongst others, include general principles terminology on product security addressing the full life cycle, risk management concepts – including threat modelling – and an abstract, high-level description of processes related to compliance to the extent that they support compliance with the CRA essential cybersecurity requirements, including but not limited to the manufacturers' obligations within the intended context under article 13 of the CRA.					
prEN XXX (WI=JT013091) **Cybersecurity requirements for products with digital elements – Generic Security Requirements**	Under Drafting	2025-03-05	2025-03-05	2025-07-25	2026-09-20
This document provides generic technical cybersecurity requirements for products with digital elements including their remote data processing solutions to fulfil the Essential Requirements of Annex I, Part I, (2)(a) through (2)(m) of the CRA. Where appropriate, multiple alternative requirements are provided that can be chosen from on a risk basis. The standard will include generic assessment criteria to support compliance of products with digital elements with the essential requirements of the CRA as listed above. Guidance will be provided to support the user of the standard in selecting the appropriate requirements to address the identified risks demonstrating the relation between cybersecurity threats and requirements. The EN 18031 series will be used as an input.					
prEN XXX (WI=JT013090) **Cybersecurity requirements for products with digital elements – Vulnerability Handling**	Under Drafting	2025-03-05	2025-03-05	2025-07-03	2025-06-06
This standard shall provide specifications applicable to vulnerability handling processes, covering all relevant product categories, to be put in place by manufacturers of the products with digital elements. Those processes shall at least allow to: (a) identify and document vulnerabilities and components contained in the product, 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 product; (b) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates; (c) apply effective and regular tests and reviews of the security of the product with digital elements; (d) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch; (e) put in place and enforce a policy on coordinated vulnerability disclosure; (f) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a standardised contact address for the reporting of the vulnerabilities discovered in the product with digital elements; (g) provide for mechanisms to securely distribute updates for products with digital elements to					

Project reference	Status	Initial Date	Current Stage	Next Stage	Forecasted voting date
ensure that vulnerabilities are fixed or mitigated in a timely manner, and, where applicable for security updates, in an automatic manner; (h) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.					

7.2. Support to standardization

During the recent years, European funded projects have commenced activities related to the support of CRA standardization.

7.2.1. Cyberstand.eu

CYBERSTAND.eu[34] aims to empower European stakeholders to engage in the development of standards and conformity in relation to the Cyber Resilience Act (CRA).

In order to reach this goal, the work of CYBERSTAND will be based on the following activities:

- Support EU experts in the contribution to standardisation 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 harmonised 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 standardisation
- Foster the development on harmonised standards in conformity with the CRA: CYBERSTAND.eu will contribute to +10 standardisation work items, showcasing +30 use cases and supporting the contents of cybersecurity chapter in the Rolling Plan for ICT standardisation
- Deliver a series of events and publications: CYBERSTAND.eu will increase the European influence and leadership in international cybersecurity standardisation through stakeholder consultations, policy briefs and events, aiming at improving the general awareness of cybersecurity standards in Europe.

The project is currently at its 7th Specific Service Procedure and a number of experts have been funded in the previous procedures to contribute in the development of standards for the CRA.

7.2.2. STAN4CR2

The STAN4CR2[35] project supports and accelerates EU standardization efforts, fostering collaboration to prevent security incidents and mitigate their impact, including on users' health and safety.

Building on the STAN4CR project, funded by the EC and EFTA, STAN4CR2 ensures coordination between both initiatives. It will focus on developing vertical standards to complement the horizontal standards under WG-9 of the CEN-CENELEC Joint Technical Committee 13 (CEN-CLC/JTC 13) on "Cybersecurity and Data Protection." Given the broad scope and cybersecurity expertise shortage, multiple Technical Groups from CEN, CENELEC, and ETSI will collaborate, with rapporteurs playing a key role in ensuring smooth coordination and communication.

STAN4CR2 will provide essential coordination through CEN, CENELEC, and ETSI, ensuring alignment across horizontal and vertical workstreams. Additionally, stakeholder consultations will foster greater inclusivity, gather diverse feedback, and increase public awareness and engagement in standardization activities.

European standardization efforts will be dedicated to developing the necessary horizontal and vertical (product specific) standards:

[34] https://cyberstand.eu/project

[35] https://www.cencenelec.eu/news-and-events/news/2025/call-for-tender/2025-03-07-stan4cr2/

- The WG-9 within the CEN-CENELEC Joint Technical Committee 13 (CEN-CLC/JTC 13) "Cybersecurity and Data Protection" is currently developing the deliverables linked to the horizontal standards.
- The vertical standards will be developed in different technical committees in specific working groups within CEN, CENELEC and/or ETSI, depending on the scope.

The goal of the STAN4CR2 project is to facilitate a seamless and inclusive standardization process, while ensuring appropriate coordination and alignment across horizontal and vertical standards. Maintaining cohesion between various workstreams and engaging in comprehensive stakeholder consultations will be key for the project's success. These consultations aim to broaden stakeholder participation, gather diverse perspectives, and enrich the standardization discussions and development process. The project also seeks to raise public awareness of standardization activities and promote greater dissemination and engagement with relevant stakeholders, fostering broader involvement and helping achieve the project's objectives. The timely development of standards will benefit industries, policymakers, and society at large by providing a solid foundation for the integration of state of art standards into everyday applications of many digital products placed in the EU market. Furthermore, the developments of standards to support the CRA will contribute to the resilience and competitiveness of the EU Single Market by enhancing cybersecurity measures, promoting innovation, and fostering trust among consumers and businesses alike.

7.3. Certification aspects of the CRA

As already mentioned above, the Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for products with digital elements, ensuring that both hardware and software are secure throughout their lifecycle. Although these requirements are horizontally mandatory and applied to all categories of products with digital elements (Important, Critical, Default), the conformity assessment processes to be followed to provide evidence that the product with digital elements and the processes put in place by the manufacturer meet these essential cybersecurity requirements are different.

These options (based on Article 32 of the CRA) are the following:

a) the **internal control procedure** (based on *module A*) set out in Annex VIII of the CRA. In this case the **manufacturer ensures and declares on its sole responsibility** (self-assessment) that the products with digital elements satisfy all the essential cybersecurity requirements, and the manufacturer meets the essential cybersecurity requirements.

b) the **EU-type examination** procedure (based on *module B*) set out in Annex VIII of the CRA **followed** by **conformity to EU-type based on internal production control** (based on *module C*) set out in Annex VIII of the CRA. EU-type examination is the part of a conformity assessment procedure in which a **notified body** examines the technical design and development of a product with digital elements and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential cybersecurity requirements set out in Part I of Annex I and that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I. EU-type examination shall be carried out by assessing the adequacy of the technical design and development of the product with digital elements through the examination of the technical documentation and supporting evidence referred to in point 3 of Annex VIII – Point II, and the examination of specimens of one or more critical parts of the product (combination of production type and design type). **Conformity to type based on internal production control** is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2 and 3 of this Part, and ensures and declares that the products with digital elements concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential cybersecurity requirements set out in Part I of Annex I and that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.

c) a **conformity assessment based on full quality assurance** (based on *module H*) set out in Annex VIII of the CRA. Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2 and 5 of this Part, and ensures and declares on its sole responsibility that the products with digital elements or product categories concerned satisfy the essential cybersecurity requirements set out in Part I of Annex I and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Part II of Annex I.

d) where available and applicable, a **European cybersecurity certification scheme** pursuant to Article 27(9).

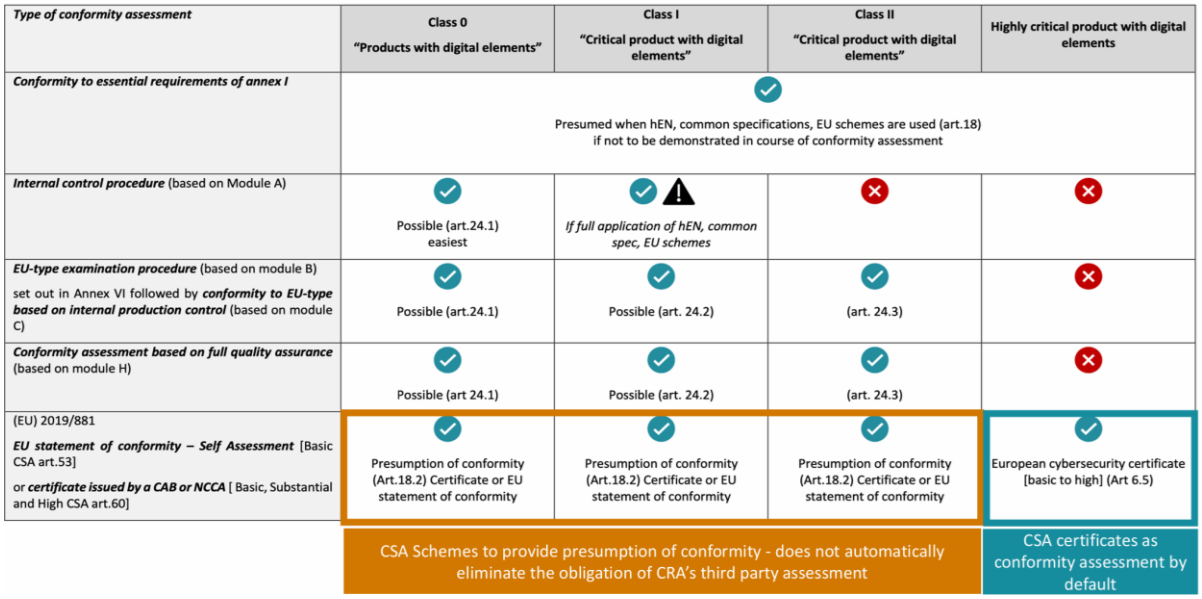

Figure 6. Relationship between conformity assessment options and different categories of products with digital elements[36]

7.4. EUCC and CRA interplay

As shown above (option d) the CRA establishes a "presumption of conformity" for products that have been certified under a recognized European cybersecurity certification scheme, such as the EUCC, provided the certification meets at least a "substantial" assurance level[37]. Although the subject may seem straight forward, the usage of EUCC for "proving" compliance to the essential requirements of the CRA faces several challenges. ENISA has recently (January 2025) a final version of the report on the Cyber Resilience Act implementation via EUCC and its applicable technical elements, and concluded that gaps and challenges exist, but there is possibility of finding solutions and practically using the certification schemes under the EU CSA to support CRA compliance. Table 7-4 shows the results of the gap analysis between the critical products with digital elements and the coverage afforded by existing Protection Profiles, the scope of the assessment, the requirements for remote data processing solutions (not typically covered by a EUCC certification) and the coverage of the Security Functional Requirements (SFRs) / Security Assurance Requirements (SARs) for CRA conformance[31].

Table 7-4 Summary of conclusions on the EUCC | CRA interplay for critical products

Type of critical product	PP conformance required in typical PPs	Scope of the EUCC assessment vs CRA product with digital elements	Requires remote data processing solutions (General case)	Coverage of required SFRs /SARs for CRA conformance
Hardware devices with security boxes	Strict	full product	NO	Direct coverage: low Indirect coverage: high but not complete With gaps in vulnerability management-

[36] https://eucyberact.org/wp-content/uploads/2023/03/B12b-FeraudA-VerrandoPJ.pdf , EUROSMART, CRA's impact on the CSA's EU cybersecurity certification framework

[37] https://certification.enisa.europa.eu/document/download/b51f00ee-d2c3-47e7-af85-059b5e06acef_en?filename=CRA%20implementation%20via%20EUCC.pdf

Type of critical product	PP conformance required in typical PPs	Scope of the EUCC assessment vs CRA product with digital elements	Requires remote data processing solutions (General case)	Coverage of required SFRs /SARs for CRA conformance
				related requirements.
Smart Meter Gateways	Strict	Full product (as a part of a non-certifiable complex system)	NO	Direct coverage: low Indirect coverage: high but not complete With gaps
Smartcards and similar devices	Strict Demonstrable (depending on the PP)	Full product (with composite evaluations for layers on HW, e.g., applets)	NO	Direct coverage: low Indirect coverage: high but not complete With gaps

Further information on the interplay is expected soon, as ENISA in collaboration with the European Commission, is organising two dedicated webinars to present and discuss the interplay between the European Common Criteria-based cybersecurity certification scheme (EUCC) and the Cyber Resilience Act (CRA).[38]

[38] https://certification.enisa.europa.eu/news/enisa-launches-global-series-webinars-interplay-between-eucc-and-cyber-resilience-act-cra-2025-05-16_en

8. Results

The methodology presented in Section 4, has provided a number of outcomes / results. These results are depicted within this section, at a high level, to facilitate readability. The detailed requirements and how they are connected with the different components of the CURIUM Continuum are included in deliverable D.2.2.

8.1. Analysis of legal, regulatory and standards requirements

This section contains a high-level overview of the functional requirements group (FRG) to be fulfilled by the CURIUM Continuum tools. The requirements, as depicted here, do not offer details as they have already been analysed within Section 6 above. Furthermore, they are depicted in a grouped manner, as seen from the perspective of the user of the CURIUM Continuum. These requirements can be classified as functional stakeholder's requirements as they stem from the analysis of the legal and regulatory frameworks.

Table 8-1 Identification of Functional Requirements (FRs)

Requirements regarding the scope of the CRA	**FRG1. A stakeholder needs to be able to identify if they, for one or more products, are within the scope of the CRA.** [*Articles 2, 3, 7, 8 of the CRA* and *Section 6.2 of this document*]Scope of the CRA The system should allow them to identify: - 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.
Requirements imposed to the economic operators	**FRG2. A stakeholder, needs to be informed on the requirements for products with digital elements.** [*Articles 6, 13, 18, 19, 20, 24, Annex I of the CRA* and *Sections 6.5, 6.6, 6.8, 6.9, 7.3, 5.3.4 and 5.3.5 of this document*] The system should be able to tell them, based on the identification of the type of economic operator - 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.

	FRG3. A stakeholder, needs to be guided in the performance of some of the essential requirements imposed by the CRA. [*Annex I of the CRA* and *Section 6.6 of this document*] The system should be able to provide them tools, to support them in - Assessing the cybersecurity risks associated with a product with digital elements; - Extracting an outcome (documented) on cybersecurity risks associated with a product with digital elements; - Identifying controls (measures) for treating cybersecurity risks based on their desired level of residual risk; - 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;
	FRG4. A stakeholder, needs to be supported in the creation of some of the technical documentation imposed by the CRA. [*Annex VIII of the CRA* and *Section 6.7 of this document*] The system should guide them in determining - Which are the contents of the technical documentation that need to be drafted - How the documentation already produced by the stakeholder, maps to the requirements of the CRA (Annex VIII) - Which type of conformity assessment process they should follow - How to draft the EU statement of Conformity

8.2. SWOT analysis

The SWOT analysis was conducted as a brainstorming exercise between the project partners. **Error! Reference source not found.**, presents the results of this analysis split into the four key aspects (Strengths, Weaknesses, Opportunities, Threats).

Table 8-2 Results of the SWOT analysis

Favourable for achieving objectives	**Unfavourable for achieving objectives**
Strengths	**Weaknesses**
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. **S2.** Some of the partners of the project are already involved in the ongoing standards developing activities related to the CRA. **S3.** Highly knowledgeable partners that support the provision of the tools.	**W1.** The project duration is limited. **W2.** Key issues related to the implementation of the CRA are still currently being defined by the European Policy makers. This could mean that something incorporated as part of the tools of the CURIUM continuum could become obsolete when a change or a clarification is provided. **W3.** Limited information about the CRA and its requirements is known by the affected economic operators, especially the ones that fall within the

Favourable for achieving objectives	Unfavourable for achieving objectives
S4. A key role in the project regarding capacity building and validation is undertaken by EIT Digital. EIT Digital's innovation ecosystem is a dynamic and collaborative network that plays a pivotal role in shaping the digital landscape across Europe. **S5.** The tools comprising the CURIUM Continuum are based on standards.	SME definition. As such, they may be unable to fully articulate their needs at this stage. **W4.** The CRA shall apply from the 11th of December 2027, which for some seems very far away, making engagement of the interested parties more difficult. **W5.** The CURIUM Continuum is not a fully integrated platform of tools. It is a compilation of 5 components not interlinked. **W6.** There is a great dependence on third-party systems (e.g. NIST NVD, SBOM parsers etc…).
Opportunities **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. **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. **O3.** Since the CRA implementation is in early stages, and the need of the market seems to be great, maybe a logical step in the future would be to scale the CURIUM platform into a cyber-security and resilience service ecosystem. **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.	**Threats** **T1.** Key issues related to the implementation of the CRA are still currently being defined by the European Policy makers. **T2.** Other projects on the same call exist, possibly providing similar tools with different implementation, fragmenting the market. **T3.** The CRA is still evolving and there is potential for shifting/changing requirements or even delayed harmonization. **T4.** The requirements of the CRA and the activities related to conformity assessment are not straight forward and, in some cases, difficult to understand. **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.

8.3. The Stakeholder questionnaire results

The survey was deployed via the EU Survey platform and remained open for nearly a month, during which each partner was responsible for promoting it within their respective countries. The survey targeted a broad audience, including manufacturers and developers of products with digital elements, authorized representatives, national authorities, European bodies, government or regulatory entities, the academic community, and other relevant stakeholders. A total of 91 completed responses were received.

The analysis of the 91 responses yielded valuable quantitative and qualitative insights that reflect the current state of preparedness, awareness, and support needs among the diverse stakeholder groups. The following sections present the main results of the survey using both numeric data and graphical visualizations. These

findings provide a clear picture of stakeholders' existing knowledge of the CRA, perceived challenges in achieving compliance, and preferences for training, tools, and support mechanisms. This evidence base is instrumental in shaping the CURIUM Compliance Continuum to be both relevant and responsive to the real-world needs of the target audience, especially SMEs and micro enterprises operating in critical digital product domains.

Figure 7Figure 7 below presents the number of organizations and entities from various industry sectors in each country that participated in and responded to the survey. As illustrated in the graph below, Greece, Cyprus and Germany are among the countries with the highest responses to this survey. Greece has the highest representation (38.46%), followed by Germany and Cyprus (both at 15.38%). Responses were also received from Italy (8.79%), Croatia (7.69%), Spain (3.3%), France (3.3%), and Romania (3.3%), as well as from Austria, Belgium, Ireland, and Sweden, each representing (1.10% each) of the total.

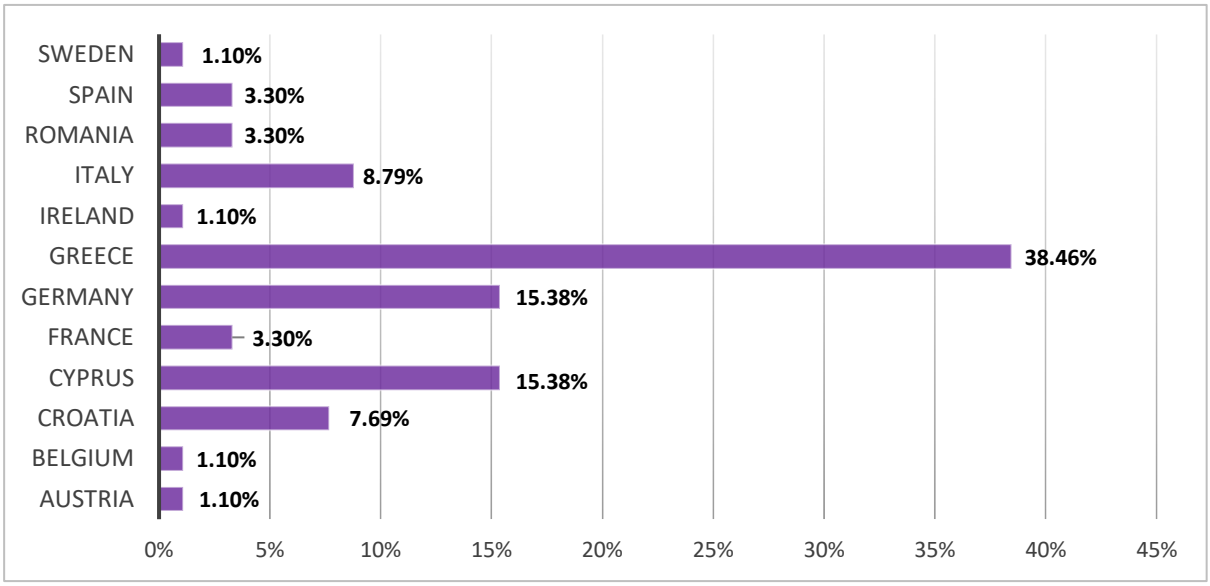

Figure 7. Number of respondents per country

Figure 8. below shows how the responses to the survey were distributed among various types of organizations and entities. The majority of responses came from Manufacturers/Developers of products with digital elements (31%), followed by Government and/or Regulatory bodies (15%), and Academic Community (13%), End users of products with digital elements (11%), National authorities (8%), Other (8%), Distributors of products with digital elements (4%), Natural or legal persons who are subject to obligations in relation to the manufacture or market availability of products with digital elements under the CRA (3%), Authorized representatives of manufacturers of products with digital elements (2%), Cyber Insurance (2%). Smaller contributions came from open-source communities (1%) and industry associations (1%).

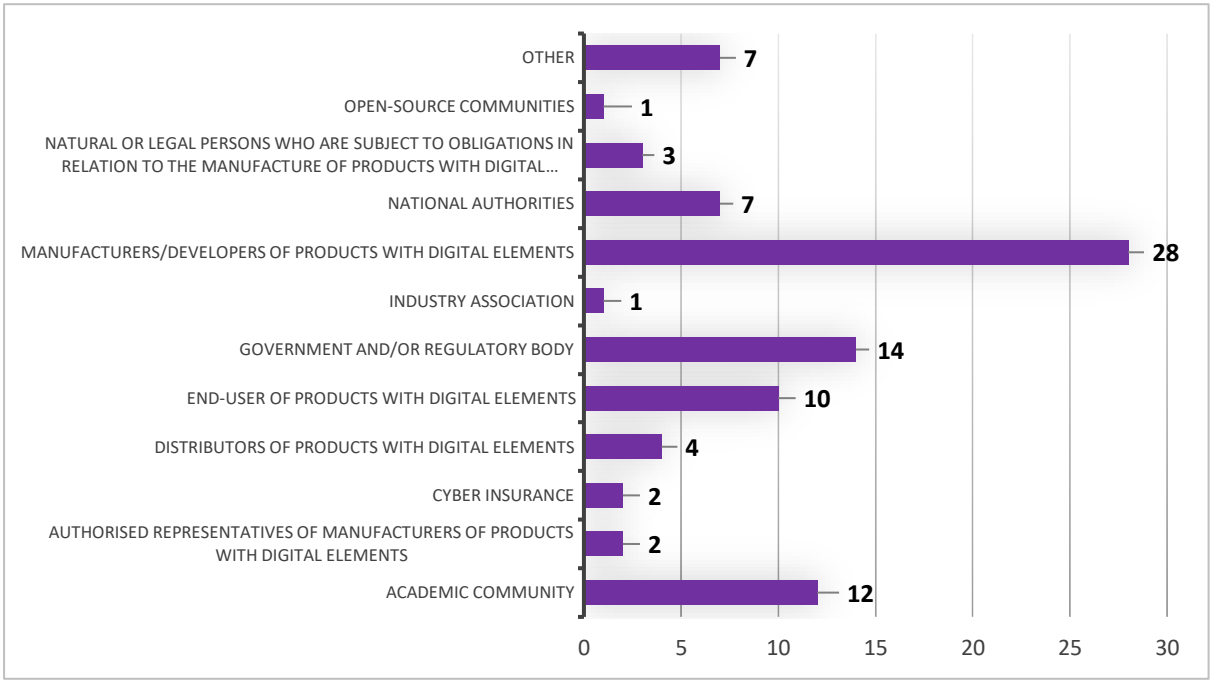

Figure 8. Number of responses by Organization/Entity Type

Error! Reference source not found., illustrates how surveyed organizations or entities perceive their overall knowledge of the CRA, based on a weighted scoring system applied after the survey. Respondents were grouped into three categories according to their calculated knowledge scores. The **Low** knowledge group (0–33%), includes the largest number of respondents—approximately 40—indicating limited or no awareness of CRA-related topics. The **Moderate** group (34–66%), comprises around 35 respondents who demonstrate some familiarity but still require further support to navigate the CRA effectively. Finally, the **High** knowledge group (67–100%), includes about 15 respondents who show strong or expert-level understanding of the CRA's scope and requirements.

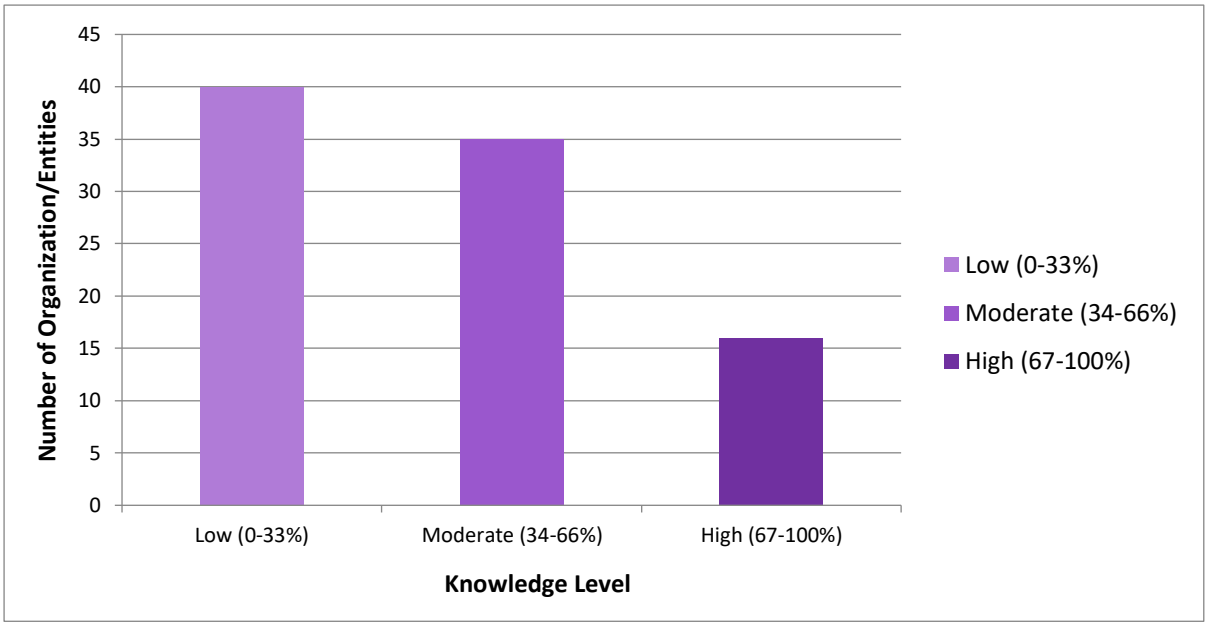

Figure 9. Knowledge level of CRA

This indicates that while a significant number of respondents have some awareness of the CRA, there is still a large portion who would benefit from foundational training and guidance to effectively engage in CRA compliance efforts

Further information on the results of the questionnaire per type of stakeholder are included in D2.2.

Kind of support	Total Number
Training on the CRA	77 / 91
Technical assistance (for the implementation of relevant security controls)	49 / 91
Policy guidance and legal support	48 / 91
Access to technical and organizational tools to guide you through the requirements	46 / 91
Access to technical and organizational tools to help you implement the requirements	41 / 91
Consulting services	50 / 91
Other	2 / 91

Table 8-3 Kind of support for CRA requirements

9. Conclusions

The purpose of this document was to present the methodology and the results of the analysis performed by the CURIUM project for the elicitation of the requirements for the tools and activities of the CURIUM project.

The methodology for the elicitation of the requirements was split into three distinct steps and resulted in the identification of concrete requirements, functional requirements groups, obstacles and opportunities presented to the project.

A State of the Art Analysis regarding current legal, regulatory, standardization and certification policies was performed. This analysis provided the requirements of the different regulatory documents as they relate to the scope of the CURIUM project. These requirements are extensive and are presented in a grouped manner (FRGs) within Section 8.1. 4 FRGs have been identified and will be further analysed and correlated to the components of the CURIUM Continuum as part of Deliverable D2.2..

A SWOT analysis was performed. This analysis provides an overview of the strengths, weaknesses, opportunities and threats to the project. Through this analysis a number of circumstances that could be exploited and avoided by the project have been identified. Specifically, the analysis revealed 4 Strengths and 3 Opportunities of the project, which the project team will endeavour to exploit and 4 Weaknesses and 4 Threats of the project which the project team will try to mitigate to the degree possible.

Finally, a Stakeholder questionnaire was provided and answers were collected from 91 respondents from 12 different countries. The stakeholder questionnaire allowed for the identification of the needs of the various categories of stakeholders, in relation to the scope of the project. The full results of the questionnaire are presented in Deliverable D2.2.. Specifically, D2.2. 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.

10. Annex I

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

Who we are

The CURIUM project aims to enhance the resilience, security, privacy, and accountability of all hardware and software products with digital elements, through the design and development of a novel Compliance Continuum provided via a set of cybersecurity-oriented tools and services information, guidance, trustworthy Security Testing and essential requirements fulfilment facilitation. The proposed approach is well-positioned to meet the emerging cybersecurity challenges posed by highly interconnected digital products, as well as to simplify and automate the compliance processes ensuring alignment with the cybersecurity requirements outlined in the Cyber Resilience Act (CRA). Ultimately, the project seeks to support European SMEs, particularly micro and small enterprises, in completing effective self-assessment processes or preparing their products for third-party assessments, reducing costs and time to certification.

Term "Compliance Continuum": *The Compliance Continuum serves as a framework for organizations to assess their current level of compliance, identify areas for improvement, and develop strategies to enhance their overall compliance posture.*

The Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) aims to safeguard consumers and businesses buying software or hardware products with a digital component. The CRA addresses the inadequate level of cybersecurity in many products, and the lack of timely security updates for products and software. It also tackles the challenges consumers and businesses currently face when trying to determining which products are cybersecure and in setting them up securely. The new requirements will make it easier to take cybersecurity into account when selecting and using products that contain digital elements. It will be more straightforward to identify hardware and software products with the proper cybersecurity features.

The Cyber Resilience Act entered into force on 10 December 2024. The main obligations introduced by the CRA will apply from 11 December 2027, giving affected organizations time to prepare.

Why this survey

The *Compliance Continuum* as mentioned above, aims to become a useful tool for various interested parties. To achieve this goal, we need your opinion, on what you believe would be most useful to you, to begin your CRA compliance journey.

Privacy Notice:

The survey does not process personal data by default. The CURIUM project has activated the "Anonymous survey mode" of the EU Survey. This means that by default contributions to this survey will be anonymous as EUSurvey will not save any personal data such as IP addresses.
There is a question within this survey, where we ask you if you wish to participate and contribute to our events and round tables (and thus be a member of our stakeholder database). If your answer is yes, then we ask you to fill in your email address as means of communication.
In this case, the following privacy policy applies:

I have read, understood and agree to the above-mentioned privacy policy.

(Possible answers: Yes | No)

Demographics (Profile of the respondent)

Please indicate the type of organization / entity you represent by filling in this survey:

Manufacturers / **Developers** of products with digital elements

Authorised representatives of manufacturers of products with digital elements

Importers of products with digital elements

Distributors of products with digital elements

Natural or legal persons who are 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 the CRA

National authorities

European Bodies, Institutions or Agencies (e.g. ENISA, EC etc)

End user of products with digital elements

Government and/or Regulatory body

Academic Community

Industry Association

Open-source communities

Cyber Insurance

Consumer Associations

Other

Which is the industry your organization belongs to?

Digital infrastructure (electronic communications, trust services, domain name services, top level domain registries, cloud services, data centers, internet exchange points, content delivery networks);

Energy (electricity, district heating, oil, gas and hydrogen);

Transport (air, rail, water, road);

Banking and Financial market infrastructures;

Health (healthcare providers, EU reference labs, research and manufacturing of pharmaceuticals and medical devices);

Drinking water and waste water;

Public administrations;

Space;

Postal and courier services;

Waste management;

Manufacture, production and distribution of chemicals;

Manufacturing;

Digital providers;

Research;

Other

Please indicate the size of the organization / entity you represent by filling in this survey, utilizing the SME definition of the European Union (https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en)

Large: Staff headcount >250 | Turnover > € 50m **or** Balance sheet total > € 43m

Medium-sized: Staff headcount < 250 | Turnover ≤ € 50 m **or** Balance sheet total ≤ € 43 m

Small: Staff headcount < 50 | Turnover ≤ € 10 m **or** Balance sheet total ≤ € 10 m

Micro: Staff headcount < 10 | Turnover ≤ € 2 m **or** Balance sheet total ≤ € 2 m

Please indicate your role within the organization

Management (Non IT/ IS)

Management (IT/IS)

Member of the IT / IS team

Member of the Procurement team

Member of the product design / development / implementation team

Compliance Officer

Member of a Regulatory Authority / National or European Institution, Agency or Body

Member of an Academic Institution

Other

Which is the country you reside / best represents your viewpoint?

Austria (AT)	Germany (DE)	Other (OTH)
Belgium (BE)	Greece (EL)	Poland (PL)

Bulgaria (BG)	Hungary (HU)	Portugal (PT)
Croatia (HR)	Ireland (IE)	Romania (RO)
Cyprus (CY)	Italy (IT)	Slovak Republic (SK)
Czechia (CZ)	Latvia (LV)	Slovenia (SI)
Denmark (DK)	Lithuania (LT)	Spain (ES)
Estonia (EE)	Luxembourg (LU)	Sweden (SE)
Finland (FI)	Malta (MT)	
France (FR)	Netherlands (NL)	

Existing knowledge of the CRA

Please select the response that best suits you, to the statements mentioned below.

I know what is the Scope and Requirements of the Cyber Resilience Act (CRA)

I don't know anything about it

I have heard of it, but would need effort or help to know its details

I have read it and have understood the main concepts

I have a deep understanding of the subject and, if needed, I can support/guide others

I know the definition and can distinguish between products with digital elements

I don't know anything about it

I have heard of it, but would need effort or help to know its details

I have read it and have understood the main concepts

I have a deep understanding of the subject and, if needed, I can support/guide others

I know the exceptions to the application of the CRA

I don't know anything about it

I have heard of it, but would need effort or help to know its details

I have read it and have understood the main concepts

I have a deep understanding of the subject and, if needed, I can support/guide others

I know about the classification of products under the CRA and can assign products to the different classes

I don't know anything about it

I have heard of it, but would need effort or help to know its details

I have read it and have understood the main concepts

I have a deep understanding of the subject and, if needed, I can support/guide others

I understand the concept and details of the essential cybersecurity requirements mandated for products with digital elements

I don't know anything about it

I have heard of it, but would need effort or help to know its details

I have read it and have understood the main concepts

I have a deep understanding of the subject and, if needed, I can support/guide others

I understand the concept and details of conformity assessment options for a product with digital elements

I don't know anything about it

I have heard of it, but would need effort or help to know its details

I have read it and have understood the main concepts

I have a deep understanding of the subject and, if needed, I can support/guide others

I understand the concept and know of the contents of the technical documentation for a product with digital elements according to the CRA

I don't know anything about it

I have heard of it, but would need effort or help to know its details

I have read it and have understood the main concepts

I have a deep understanding of the subject and, if needed, I can support/guide others

Challenges

At this current stage, rate the following challenges as they relate to your organization. The scale to be used is: 1) Strongly disagree 2) Disagree 3) Neither agree nor disagree 4) Agree 5) Strongly agree.

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
***We do not know** whether our company currently develops or sells "product(s) with digital elements"					
***We have limited** knowledge of the CRA scope and requirements					
***We do not know** if our organization is in scope of the CRA					

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
***We do not know** which are the actual / practical requirements of the CRA					
***We do not have access** to tools which would assist us in the risk assessment process					
***We do not have access** to tools which would assist us in the identification of our exposure to risk					
***We do not have access** to tools to perform vulnerability analysis					
***We do not have access** to tools to perform penetration tests					
***We do not have** an understanding what is an EU declaration of conformity and how this could be extracted					
***We do not know** which are the essential requirements that the product with digital elements needs to comply with					
***We do not know** which options exist in relation to the conformity assessment of products with digital elements					
***We do not know** of any training / capacity building activity that focuses on the CRA					
***We do not know** how to construct the technical documentation of the product with digital elements					
***We find it very difficult** to locate / get expert advice or direction on CRA compliance					
*There is **limited** or **no funding** available to us, to prepare for CRA compliance					
*The tools provided by different organizations, are **very costly**					
*Preparing for CRA compliance **requires expert knowledge**					

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
***I have never** participated in any training activities regarding the CRA					
***We have not** assessed whether our "product with digital elements" complies with CRA's security-by-design principles".					

Offerings

What kind of support would help you understand and comply with CRA requirements? Choose all that would be desirable for you.

Training on the CRA

Technical assistance (for the implementation of relevant security controls)

Policy guidance and legal support

Access to technical and organizational tools to guide you through the requirements

Access to technical and organizational tools to help you implement the requirements

Consulting services

Other

Which type of training would be most useful for you? You may select multiple answers.

Hands-on workshops using a testing environment

Live online courses

Self-paced online courses

One-to-one advisory sessions

Self-assessment guides and documentation

Other

Which roles in your organisation should receive CRA-related training?(free text)

Do you think that any training provided should be differentiated based on the audience? (for example different trainings for technical and non technical personnel)

Yes

	No
Which would be your preferred host for such training? You can make one or more selections	The national Cybersecurity Authority
	ENISA
	The EC
	An SME related association
	Any one
	Other

Are there any additional regulatory aspects that should be taken into consideration during the compliance to the CRA?

Yes

No

I do not know

11. Annex II

A template for the EU Declaration of Conformity.

EU Declaration of Conformity (DoC)

We:

Company name:	
Postal address:	
Postal code:	
City:	
Telephone number:	
E-Mail Address:	

Declare that the DoC is issued under our sole responsibility and belongs to the following product:

Product:	
Type:	
Batch:	
Serial number:	

Object of the declaration (identification of the product allowing traceability, may include color images, where necessary for the identification of the product):

Identification of the product	Image(s)

The object of the DoC described above is in conformance with the relevant EU harmonized legislation:

e.g. Low Voltage Directive (LVD) 2014/35/EU	

…..	

The following harmonized standards and technical specifications have been applied:

e.g. IEC 62443-4-1	
….	

Notified body (if and where applicable):

Additional information (if needed):

Signed from and on behalf of:

Place of Issue	*yyyy-mm-dd*	*Name, function, signature*