Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

OCCTET

Open Source Compliance Comprehensive tools and resources designed to simplify and streamline the CRA compliance process for SME, allowing them to tackle the complexities of OSS compliance.

Project Title: Open Source Compliance Comprehensive tools and resources designed to simplify and streamline the CRA compliance process for SME, allowing them to tackle the complexities of OSS compliance.
Project Acronym: OCCTET
Grant Agreement / Contract No.: 101190474
Program: DIGITAL Europe Programme; DIGITAL-ECCC-2024-DEPLOY-CYBER-06
Instrument: DIGITAL JU SME Support Action
Granting Authority: European Cybersecurity Industrial, Technology and Research Competence Centre
Project Start Date: 1 November 2024
Project Duration: 24 months

Deliverable Number: D2.1
Deliverable Title: CRA SME Requirement Document
Deliverable Type (DOA): R — Document, report
Deliverable Type (content): A comprehensive CRA Compliance Framework Report, detailing SME and FOSS-specific requirements, challenges, and best practices for CRA compliance. This document will include insights from direct engagements with SME owners and FOSS contributors, analysis of existing compliance literature, and expert consultations.
Work Package: WP2 – Define and support compliance procedures
Task Number(s): T2.1; T2.2
Dissemination Level: PU – Public
Due Date (DoA): 31 March 2025
Actual Submission Date: 30 April 2025
Version: 1.1 (PR1 Revision)

Lead Beneficiary: EXP- Expertware SRL
Main Author(s): Augustin Alexandrovici - EXP; Ayman Khalil - RAL
Contributing Partner(s): RAL, ECL, BS, EXP, ABCD;DSME
Reviewer: ECL - Eclipse Foundation Europe
Licensing (public Deliverable)

Legal Notice

This deliverable has been produced within the OCCTET project (Grant Agreement No. 101190474) funded under the Digital Europe Programme.
Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Document History

Version	Date	Issued By	Status	Comments
0.1	10-02-2025	Andreea Galbau	Draft	Initial draft for D2.1
0.2		Augustin Alexandrovici	Draft	Adapted after CRA Nov 2024
0.3		Stefan Teodor Pop	Draft	Adapted based on consortium comments
0.4		Nataël COUTURIER	Draft	Global review
0.5		Paul GEDEON	Draft	Global review
0.6		Ayman KHALIL	Draft	- Global review - Integration of initial results of FOSS Survey - Integration of Risk related to FOSS ecosystem
1.0		Augustin Alexandrovici	Final	Version for publication
1.2		Ayman KHALIL	Update	Version integrating latest SMEs survey results Integrating additional clarifications following the commission's feedback during the review phase.
1.3	18-02-2026	EXP-ECL	Final review	PR1 Revision - strengthened stakeholder validation narrative, methodological clarification, and formatting alignment

Executive Summary

Deliverable D2.1 presents the CRA SME Requirements Framework developed under Work Package 2 (WP2) of the OCCTET project. The objective of this document is to consolidate regulatory obligations stemming from the Cyber Resilience Act (CRA) and translate them into structured compliance requirements tailored to Small and Medium-sized Enterprises (SMEs) and the Free and Open Source Software (FOSS) ecosystem.

The framework is grounded in a structured methodological approach combining regulatory analysis, stakeholder engagement, survey results from SMEs and FOSS contributors, desk research, and expert consultation within the consortium. The survey instruments were aligned with the structure of the CRA, enabling direct mapping between stakeholder realities and regulatory domains, including essential cybersecurity requirements, role-based responsibilities, vulnerability handling, lifecycle management, and conformity assessment pathways.

During RP1, targeted consultation activities generated initial qualitative insights from SMEs and FOSS contributors across multiple European countries. While the dataset reflects an early consultation phase and does not constitute a statistically representative sample, it provides consistent patterns regarding compliance awareness gaps, documentation challenges, vulnerability management limitations, and the need for accessible, automation-friendly tooling adapted to SME constraints.

These findings have directly informed the design priorities of the OCCTET compliance toolkit and the self-assessment model developed under WP2 and WP4. In accordance with the Description of Action, broader and more systematic validation is foreseen under WP4 (Validation – Use Cases), supported by continued stakeholder mobilisation and dissemination activities under WP5.where progressive feedback collection and real-world SME participation will support iterative refinement of the compliance framework.

D2.1 therefore provides the foundational requirements baseline for the OCCTET project, ensuring regulatory alignment, methodological transparency, and operational relevance for SMEs and FOSS communities seeking to navigate CRA compliance in a structured and scalable manner.

Keywords: Cyber Resilience Act (CRA), SMEs, FOSS, Open Source Compliance, SME Requirements, Self-Assessment Checklist, Vulnerability Handling, Product Classification, Conformity Assessment, Digital Elements

Table of contents

1 Introduction

Across the European Union (EU), both citizens and organizations increasingly depend on connected technologies for their day-to-day operations. Small and medium-sized enterprises (SMEs) are particularly reliant on digital systems that power critical workflows across multiple platforms and devices.

In response, the EU Cyber Resilience Act (CRA) has established a regulatory framework aimed at bolstering cybersecurity standards. The accompanying requirements and self-assessment checklist help organizations navigate these regulations efficiently. This framework highlights essential elements such as policy documentation, risk management, security controls, and product criticality assessments.

By offering flexibility based on specific product features and target audiences, the CRA allows businesses to satisfy regulatory demands while tailoring their security strategies to unique operational contexts. Regular updates and the incorporation of stakeholder feedback ensure that the checklist remains relevant and current, enabling organizations to sustain a strong cybersecurity posture in line with evolving EU standards

1.1 CRA introduction

Current business processes span across multiple industries and make use of various “digital components”. While the CRA scope is obvious for the SMEs developing hardware and software products it might not be so obvious for other companies where the inclusion of ‘digital components' is less evident.

SMEs need first to assess if their business creates products or services which use/embed/integrate other “digital elements”. Even if the “digital components” are delivered by other suppliers the SMEs must ensure that CRA obligations are respected end-to-end.

There are multiple scenarios where the use of “digital components” is not obvious hence we would like to provide various examples which help the SMEs with the process of CRA applicability self-qualification.

The Cyber Resilience Act (CRA) proposes cybersecurity requirements for **products or services with digital elements**. The regulation applies to products whose **intended, or reasonably foreseeable use** includes a **direct or indirect logical or physical data connection** to a device or network.

CRA rules categories:

(a) rules for the taking 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 production 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.

Dependent on classification:

1. **Default products** → internal assessment generally sufficient.
2. **Important products Class I** → internal assessment if **fully** applying relevant harmonized standards/certification schemes; otherwise third-party assessment.
3. **Important products Class II** → Always require **third-party** assessment.
4. **Critical products** → Always require **third-party** assessment and in some cases, commission through delegated act can specify schemes that can be used to demonstrate conformity.

1.2 CRA Scope Exemptions

Products with digital elements exempted by CRA:

(a) Medical Devices: Regulation (EU) 2017/745 and Regulation (EU) 2017/746;
(b) Motor Vehicles: Regulation (EU) 2019/2144
(c) Civil Aviation: certified according to Regulation (EU) 2018/1139
(d) Marine Equipment: covered by Directive (EU) 2014/90
(e) Products developed or modified exclusively for national security or defence purposes.
(f) Spare parts which replace identical components for products already certified.
(g) Products complying with other EU legislation of frameworks (sectoral or functional) that achieve the same or higher level of protections.
(h) Certain products are excluded if covered by **specific sectoral regulations** or purely **SaaS** (unless they are integrated into a remote data processing solution for a physical product).
(i) **Free, not-for-profit open-source software** is excluded if it is not part of a commercial arrangement although the open-source software stewards have specific responsibilities.
(j) Covered products are classified as **non-critical** or **critical**, with critical split into **Class I** (lower risk) and **Class II** (higher risk) as per Annex III.

1.3 CRA Applicability Timeline

Obligation	Enter into force
Provision on notification of conformity assessment bodies	11 June 2026
Reporting obligations concerning actively exploited vulnerabilities or severe incidents concerning manufactured or distributed products containing digital elements.	11 September 2026
Full CRA Regulation Applicability	11 December 2027

1.4 CRA Risks for FOSS Ecosystem

Under the Cyber Resilience Act, open source developers and project stewards face distinct but interconnected risk profiles. While independent, non-commercial open source developers are explicitly out of scope, they may still face indirect pressures related to vulnerability disclosure, project trust, and downstream integration into commercial products.

In contrast, FOSS project stewards (e.g. foundations or coordinated maintainer groups), may fall within CRA scope if they engage in monetized activities or manage structured release cycles, potentially being treated as economic operators. Their responsibilities could include lifecycle security practices, vulnerability handling, and documentation obligations.

Meanwhile, manufacturers or commercial integrators who embed FOSS into CRA-regulated products bear full compliance responsibility, including ensuring that FOSS components do not compromise cybersecurity.

1.5 CRA Risks for SMEs

Despite widespread reliance on connected products, many of these devices continue to exhibit weak cybersecurity standards, including default passwords that are easily breached, unencrypted data transmission, and complex or infrequent update mechanisms. These vulnerabilities leave both end users and SME’s vulnerable to cyber-attacks that can compromise sensitive information, disrupt operations and damage reputations. Given that users often lack the necessary awareness or tools to safeguard themselves, the EU Cyber Resilience Act (CRA) imposes obligations on manufacturers to elevate security measures at the design stage.

Under the CRA, manufacturers must ensure that products are developed and deployed with robust security controls in place, while also streamlining the processes required for ongoing updates and patches. This means taking a proactive approach to risk mitigation from the outset by embedding strong cryptographic protocols, replacing or securing default passwords, and establishing user-friendly mechanisms for deploying critical software updates. The aim is to enhance cybersecurity across the entire product lifecycle—from initial design to end-of-life management.

For SMEs, this legislative push serves both as a challenge and an opportunity. On the one hand, meeting heightened security requirements can demand additional resources, specialized expertise, and increased operational complexity—areas where smaller organizations often face constraints. On the other hand, SMEs that successfully adopt CRA-aligned practices can strengthen their market position by demonstrating robust security credentials and fostering greater trust with customers and partners. By aligning product development and maintenance processes with CRA guidelines, SMEs can not only fulfill their regulatory obligations but also enhance their competitive edge and resilience in an increasingly threat-intensive digital landscape.

Penalties for non CRA compliance

The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 13, 14 shall be subject to administrative fines of up to 15 000 000 EUR or, if the offender is an undertaking, up to 2.5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.

The non-compliance with Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53 shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to 5 000 000 EUR or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Administrative fines do not apply to microenterprises or SMEs for a failure to meet the 24-hour deadline for the early warning notification of actively exploited vulnerabilities or severe cyber security incidents impacting their products.

1.6 SMEs Challenges

The list has been compiled based on the SMEs customers of consortium members. The results for the CRA readiness survey will be incorporated.

Lack of Technical Knowledge

SMEs frequently lack in-house cybersecurity expertise, making it difficult to understand and implement the complex technical requirements mandated by the CRA.

- **Example:** An SME may struggle to configure secure authentication methods or perform code reviews if they do not have a dedicated IT security team.
- **Impact:** This knowledge gap can result in overlooked vulnerabilities, incomplete risk assessments, and higher exposure to cyberattacks.

Complexity of Legal and Regulatory Requirements

Interpreting extensive and evolving regulations, such as the CRA, can be overwhelming for smaller organizations.

- **Example:** An SME might find it challenging to keep track of different national guidelines, especially if they operate or sell products across multiple EU member states.
- **Impact:** Confusion or misinterpretation of legal obligations can lead to non-compliance, potential fines, and reputational damage.

Limited Resources

SMEs typically have tighter budgets and fewer personnel, making it challenging to dedicate sufficient time and funds to cybersecurity initiatives.

- **Example:** A small business may not be able to invest in specialized security software or frequent third-party audits, even if those tools and services would significantly reduce cyber risk.
- **Impact:** Insufficient resource allocation can cause security projects to be deprioritized, potentially increasing the risk of security incidents.

Supply Chain Complexity

Many SMEs rely on third-party vendors for critical components or services—ranging from software libraries to cloud hosting platforms.

- **Example:** If a vendor’s code includes an unpatched vulnerability, it can compromise the security of the SME’s final product.

- **Impact:** A lack of robust due diligence or clear contractual obligations around cybersecurity can create weak links that attackers exploit, jeopardizing compliance with the CRA's requirements for secure supply chains.

Integration with Existing (Often Legacy) Systems

Small businesses may have inherited older IT systems that were not designed with modern cybersecurity standards in mind.

- **Example:** A legacy CRM platform might store customer data in an unencrypted format, making it incompatible with newly recommended encryption protocols.
- **Impact:** Upgrading or replacing legacy systems to align with CRA standards can be costly and time-consuming, creating operational disruptions.

Cultural and Organizational Resistance

Embracing a security-focused mindset often requires a cultural shift—from leadership to frontline employees.

- **Example:** Employees accustomed to convenience might resist strict password policies or frequent mandatory training sessions.
- **Impact:** Without organization-wide buy-in, even well-designed security policies can falter in practice, undermining compliance and creating internal friction.

Balancing Innovation with Compliance

SMEs often drive innovation by rapidly iterating product features, but cybersecurity regulations can slow development cycles.

- **Example:** A fast-growing startup aiming to capture market share may neglect security testing in favor of pushing features to market.
- **Impact:** Cutting corners on cybersecurity to meet tight timelines can result in vulnerabilities that jeopardize compliance and trust.

Cost-Effective Implementation of Best Practices

Maintaining strong cyber hygiene—like regular patching, encryption, or multi-factor authentication—can be resource-intensive.

- **Example:** Implementing role-based access controls across multiple systems might require significant software investments and staff training.
- **Impact:** SMEs may find it difficult to justify these costs, especially if immediate ROI is not apparent, yet lack of investment can lead to heightened risk.

Risk of Reputational Damage

Although larger enterprises can sometimes absorb the fallout from security incidents, SMEs might face existential threats from bad publicity.

- **Example:** A small tech firm that suffers a data breach affecting a niche market might lose critical customer trust and see sales plummet.
- **Impact:** Negative publicity can overshadow an SME's brand, hampering growth, investor relations, and market opportunities.

1.7 Goals

This document aims to provide support to open-source communities, microenterprises and small and medium-sized enterprises, including start-ups, in the implementation of CRA Regulation, aims to raise their awareness, to offer a concise process for self-assessing their CRA applicability, their strengths and weaknesses in relation the obligations introduced by CRA regulation as well as to guide them reaching compliance in an efficient manner.

2 Stakeholder Engagement and Requirements Derivation

As part of Task T2.1 "Gather SMEs and FOSS Requirements", OCCTET conducted targeted stakeholder engagement activities aimed at collecting concrete insights from key communities affected by the Cyber Resilience Act (CRA): the Free and Open Source Software (FOSS) community and Small and Medium-sized Enterprises (SMEs).

This section presents the initial findings from the first round of stakeholder input and explains how these findings were structured, interpreted, and integrated into the development of the OCCTET compliance framework.

2.1 Stakeholder Engagement Design and Structuring Methodology

The stakeholder engagement activities were designed as a structured consultation process aligned with the CRA regulatory framework.

2.1.1 Survey Design and Regulatory Anchoring

The survey instruments were drafted by Red Alert Labs (RAL), drawing on its regulatory expertise and ongoing involvement in European cybersecurity regulatory discussions. The draft was reviewed with consortium partners to ensure clarity, accessibility, and consistency with project objectives before distribution.

The questionnaire was deliberately grounded in the structure of the CRA. Its content reflected:

- The essential cybersecurity requirements set out in Annex I,
- The differentiation of economic operator roles (manufacturer, importer, distributor),
- Obligations related to third-party components and FOSS integration,
- Lifecycle management and vulnerability handling expectations.

This anchoring ensured that stakeholder responses could later be mapped directly to regulatory domains and conformity assessment pathways.

2.1.2 Structured Consultation Logic

The consultation was not conducted as an open exploratory survey, but as a structured assessment organised around three analytical pillars:

1. CRA Applicability (market placement, role identification, product classification awareness)
2. Operational Readiness (secure development, vulnerability handling, documentation, lifecycle practices)
3. Gap Identification (resource constraints, tooling needs, governance challenges)

This structure created a solid analytical foundation for mapping findings to the compliance journey and tooling architecture under WP4.

2.1.3 Processing and Cross-Work Package Consolidation

Following data collection, RAL conducted an initial analysis of responses. Findings were subsequently discussed in WP2, WP4, and WP5 coordination meetings, as well as transversal consortium sessions.

Responses were grouped according to CRA obligation domains, including essential requirements, vulnerability handling, role-based responsibilities, and conformity assessment considerations. This enabled progressive mapping of stakeholder realities to the emerging compliance tooling framework.

2.1.4 Representativeness Strategy

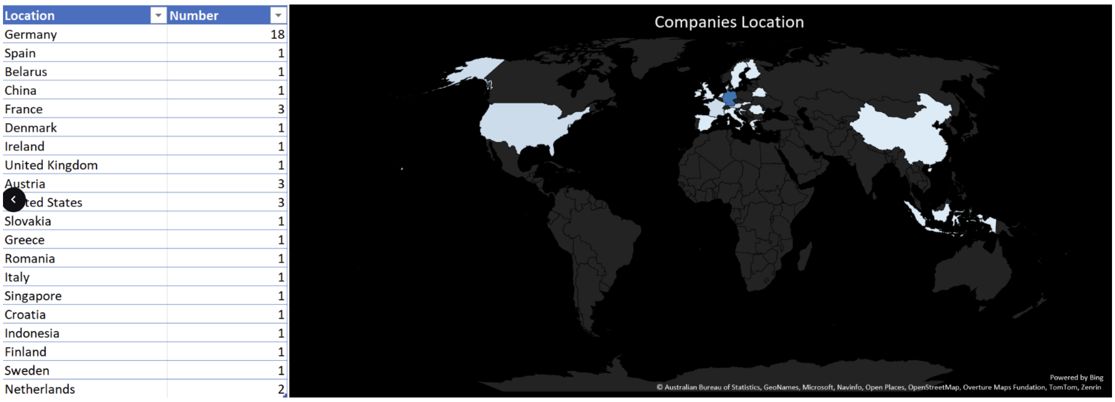
Stakeholder outreach was conducted through:

- DSME networks,
- Eclipse Foundation communication channels,
- Partner ecosystems and workshops,
- Open calls via the OCCTET website.

SMEs were intentionally targeted as a primary audience due to their high representation within European digital ecosystems and their potentially disproportionate compliance burden as well as the OCCTET ambition to support them.

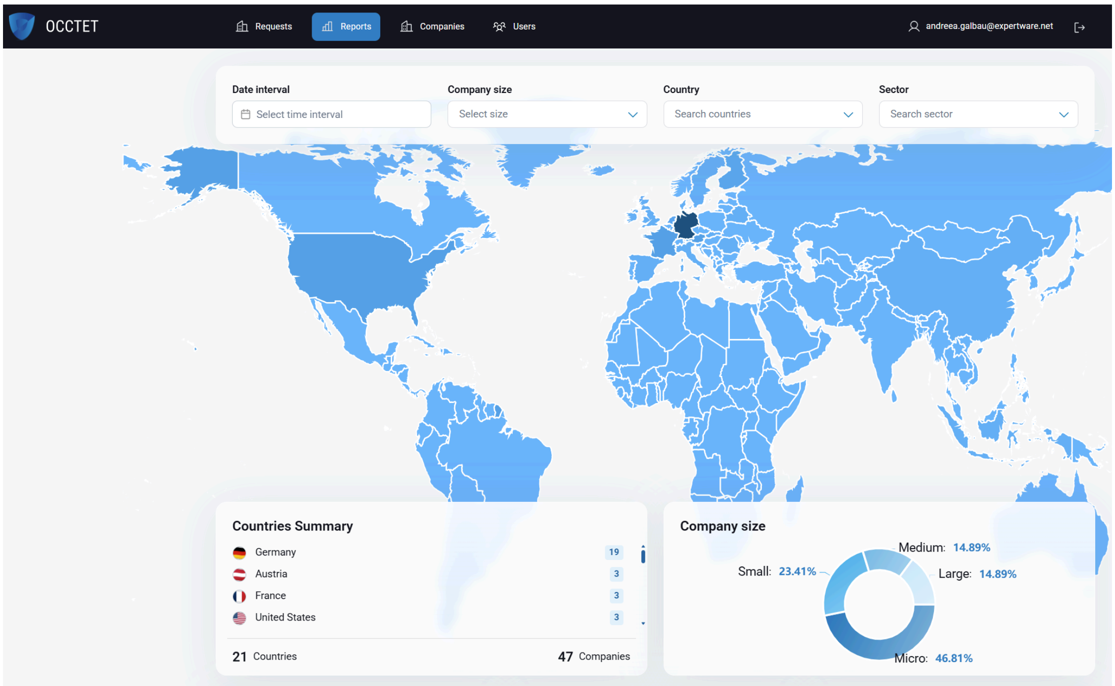
Future survey iterations embedded within the OCCTET platform started enabling more systematic tracking of geographical and sectoral distribution through the OCCTET self-assessment portal (https://cra.occtet.eu/)

The figure below shows an example of how geographic distribution is being monitored through the new assessment portal.



Location	Number
Germany	18
Spain	1
Belarus	1
China	1
France	3
Denmark	1
Ireland	1
United Kingdom	1
Austria	3
ted States	3
Slovakia	1
Greece	1
Romania	1
Italy	1
Singapore	1
Croatia	1
Indonesia	1
Finland	1
Sweden	1
Netherlands	2

Companies Location
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin



Date interval: Select time interval

Company size: Select size

Country: Search countries

Sector: Search sector

Countries Summary

Germany	19
Austria	3
France	3
United States	3

21 Countries

47 Companies

Company size

2.1.5 Ongoing Regulatory Alignment

Through RAL extensive involvement in European cybersecurity landscape and CRA initiatives, interpretation of stakeholder input has been continuously aligned with evolving European regulatory developments, including but not limited to:

- CRA FAQs:

  (https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions)

- Standardisation efforts for horizontal and vertical standards

  (https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions)

- CRA Expert Group

  (https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3967): Red Alert Labs is also part of the members of the CRA expert group and started a recurrent newsletter for the OCCTET partners related to the main topics that could impact the consortium work and the major orientations that could be needed.

- Ongoing connected topics such as the “Cyber Resilience Act implementation via EUCC and its applicable technical elements” :

  https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en

This ongoing regulatory alignment allowed up to now to ensure solid alignment with up to date information and initiatives related to the CRA, including strategic orientation and exploitation of the surveys.

2.2 FOSS Community Engagement : Initial Survey Results

An online survey titled "Shaping CRA Compliance for the FOSS Ecosystem" was launched in March 2025 via Framaforms and distributed through Eclipse Foundation committers' mailing list and the OCCTET linkedin and Bluesky accounts.

To date, 10 responses have been collected. Respondents include contributors, project leads, committers, and researchers from FOSS projects such as Eclipse ESCET, Jakarta Servlet, Eclipse GEF, Tomcat, ATL, Linux Foundation OpenSSF, Php Core,Tractus-X and Debian, operating in countries like Belgium, Netherlands, Germany, and the UK.

2.2.1 Summary of Product Types and CRA Applicability

Most respondents develop or maintain open-source tools, libraries, or middleware used in larger software or embedded systems. Common types include:

- Web server components and APIs
- Control logic generation tools
- Model transformation utilities
- Eclipse RCP-based IDE plugins or platforms

A majority of these tools are either:

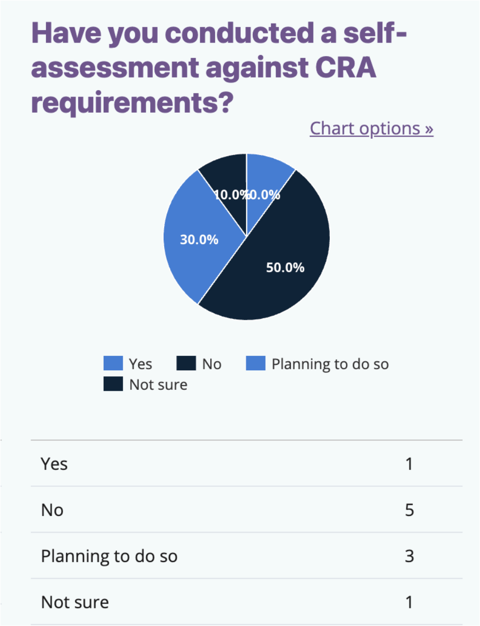
- Directly integrated into products with digital elements, or
- Distributed via ecosystems where their code ends up in commercial offerings, especially in the EU.

Although not all respondents were certain about the placement of their components on the EU market, several confirmed that their projects are part of product stacks commercially distributed in the EU. This suggests that many of the tools developed by these FOSS contributors may fall within the scope of the CRA, even if unintentionally.

This result highlights a core challenge: contributors often do not see themselves as "manufacturers" under the CRA, yet the downstream use of their components can trigger obligations. This gap reinforces the need for role clarification guidance, particularly around responsibility boundaries when OSS is embedded in digital products.

2.2.2 Awareness and Understanding

The survey highlights varying levels of awareness among FOSS contributors regarding the CRA. While a majority described themselves as "somewhat familiar" or "very familiar" with the regulation, only a small fraction had actually incorporated CRA requirements into their development workflows. Crucially, none of the participants had performed a self-assessment against CRA obligations, suggesting that awareness has not yet translated into operational readiness.

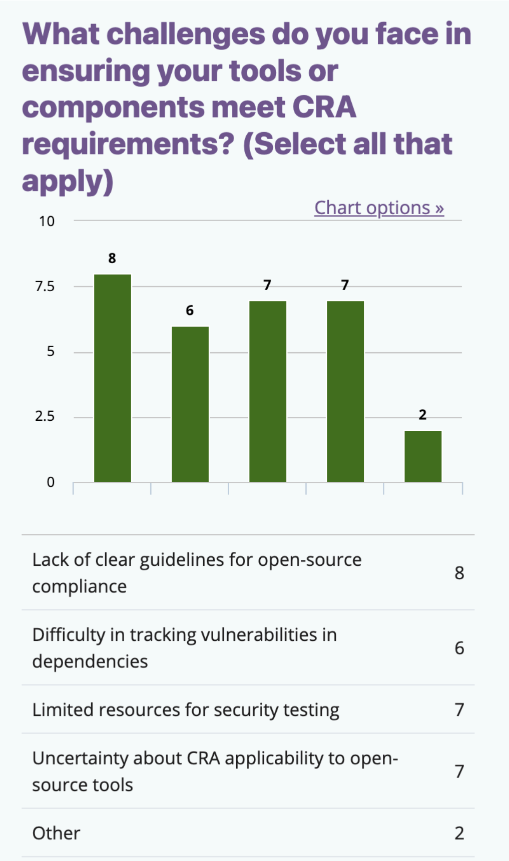


Have you conducted a self-assessment against CRA requirements?

Yes	1
No	5
Planning to do so	3
Not sure	1

2.2.3 Challenges Identified for FOSS community

Several consistent pain points emerged across responses. The most prevalent challenge cited was the lack of clear guidance specific to the open-source context as well as difficulties in vulnerability tracking across dependencies. Particularly around when obligations apply, and what concrete steps are expected. Participants also flagged limited access to security testing resources, and general confusion about how CRA applies to community-driven or indirectly commercialized tools.



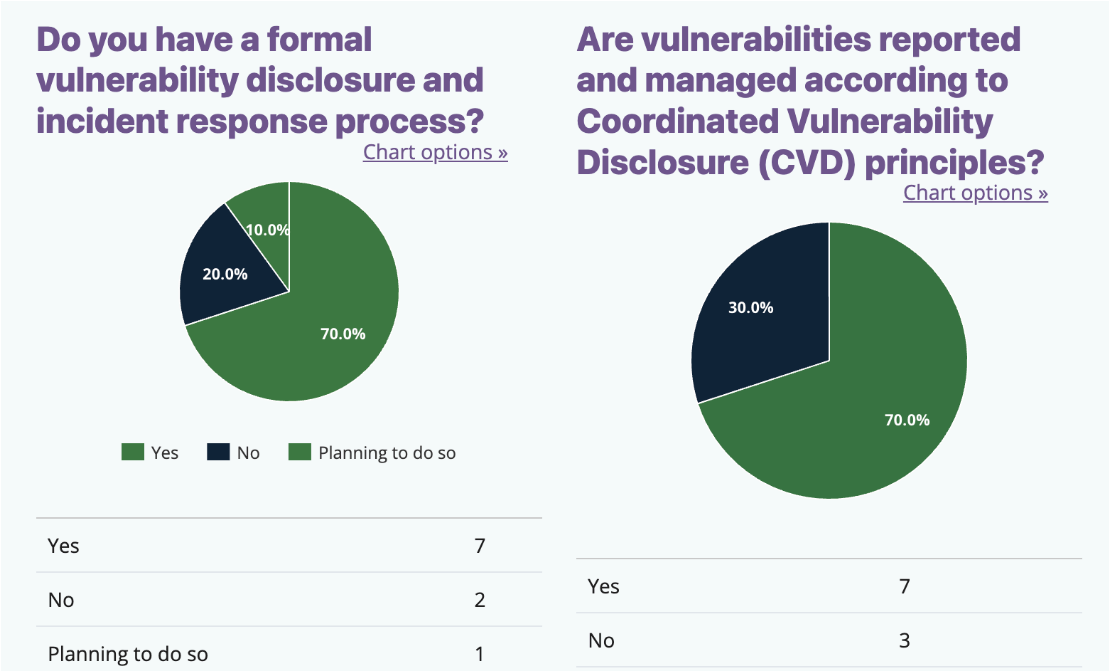
What challenges do you face in ensuring your tools or components meet CRA requirements? (Select all that apply)

Chart options »

Lack of clear guidelines for open-source compliance	8
Difficulty in tracking vulnerabilities in dependencies	6
Limited resources for security testing	7
Uncertainty about CRA applicability to open-source tools	7
Other	2

2.2.4 Cybersecurity Practices

The range of security practices among respondents varied significantly. Some projects employed static code analysis, GitHub security scans, automated testing, or peer reviews. However, only half had a formal vulnerability disclosure and incident response process in place. While there was evident initiative in improving security hygiene, there was also a lack of structured or standardized implementation aligned with CRA expectations (e.g. formal risk assessment, security support period communication, SBOM generation, …).



Do you have a formal vulnerability disclosure and incident response process?

Chart options »

Yes	7
No	2
Planning to do so	1

Are vulnerabilities reported and managed according to Coordinated Vulnerability Disclosure (CVD) principles?

Chart options »

Yes	7
No	3

2.2.5 Documentation and Support Needs

Documentation readiness remains a major gap. Most contributors do not currently publish documentation that would satisfy CRA's transparency and security support period requirements. The survey revealed a strong interest in templates, checklists, and example documentation. Resources that could lower the barrier to compliance.

2.2.6 Need for Tooling

Respondents expressed a clear preference for lightweight, automation-friendly tools that integrate with existing Git-based workflows. Suggestions included CVE tracking dashboards, SBOM generators, and modular documentation builders. Importantly, several contributors explicitly stated that they were seeking open-source or low-cost options rather than enterprise compliance platforms.

2.2.7 Direct Quotes and Open Feedback Highlights

The survey included open-ended questions that offered participants space to freely express their needs and concerns. Below are some of the responses that provided valuable insight into the community's real-world mindset:

- *"I don't know if I need to document my SBOM if I'm not selling anything…"* ⇒ this indicates some confusion around when CRA applies.
- *"A checklist with concrete examples is probably the best support you can offer."* ⇒ this indicates the necessity of having practical tools to guide the community.
- *"In the scope of Eclipse RCP application, showing the list of CVEs in an Eclipse RCP target platform with warning for instance."* ⇒ this points to a clear tooling request for Eclipse developers.

- *“Don't know if we comply [with standards]”* ⇒x this reflects uncertainty about existing cybersecurity posture.
- *“Automated tools would help the most.”* ⇒ repeated by several respondents as a core need.

2.3 SME Engagement Plan (Initial Survey Results)

An online survey titled “Shaping CRA Compliance for SMEs with OCCTET” was launched in March 2025 via Framaforms and distributed through OCCTET’s website and partner networks. The goal of the survey was to gather structured feedback from EU-based small and medium-sized enterprises (SMEs) on their awareness, challenges, and support needs to comply with the Cyber Resilience Act (CRA).

To date, 10 responses have been collected. Respondents include founders, technical leads, and compliance managers from SMEs operating in software development, digital product manufacturing, and service provision. Participants were based across Western, Northern, Southern, Central, and Eastern Europe, with some companies also active outside the EU.

2.3.1 Summary of Product Types and CRA Applicability

Most respondents represent organizations developing or integrating software components into digital products, including IoT systems, industrial control software, or cloud-based services. These products are either commercially distributed within the EU or preparing to enter the market. In several cases, companies perform multiple roles in the supply chain developing, importing, distributing, or maintaining digital elements.

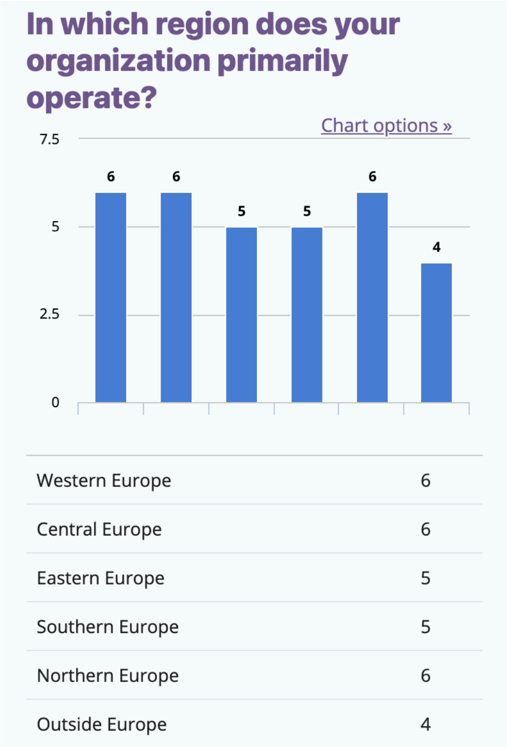

In which region does your organization primarily operate?

Chart options »

Western Europe	6
Central Europe	6
Eastern Europe	5
Southern Europe	5
Northern Europe	6
Outside Europe	4

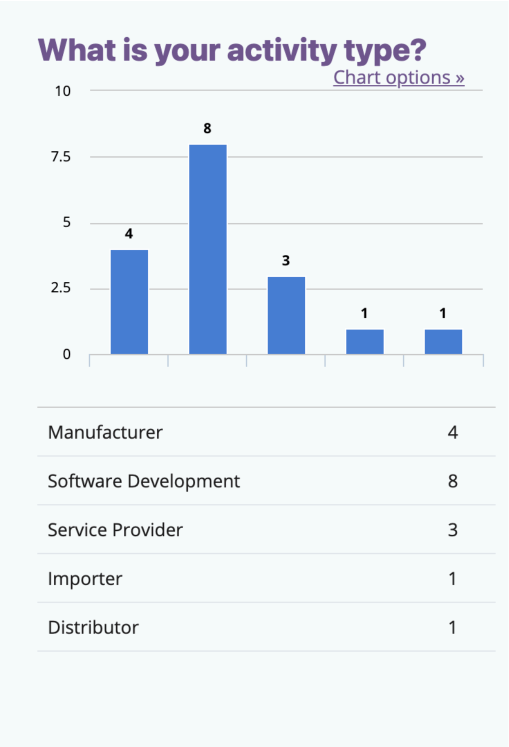
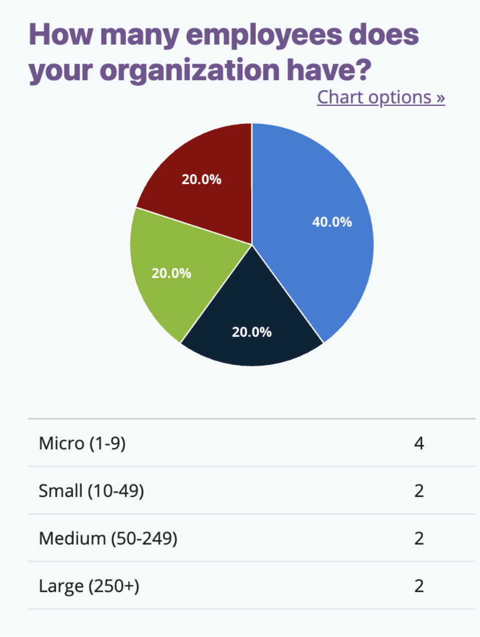

What is your activity type?

Chart options »

Manufacturer	4
Software Development	8
Service Provider	3
Importer	1
Distributor	1

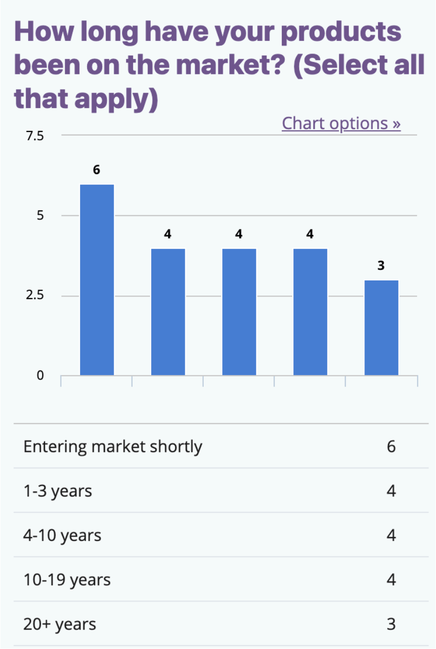
The companies varied in size, with micro- and medium-sized organizations most represented. Although two companies were part of larger structures, their cybersecurity activities aligned more with SME-level capabilities.

Several respondents stated that their products are either about to enter or are already present on the EU market. Product maturity ranged from new launches to over 20 years of commercialization, suggesting that both early-stage and mature SMEs may fall within the CRA scope. While most participants considered their products to be commercialized in the EU, there remains some ambiguity around the precise applicability of the regulation and the roles each SME must assume.



How many employees does your organization have?

Micro (1-9)	4
Small (10-49)	2
Medium (50-249)	2
Large (250+)	2

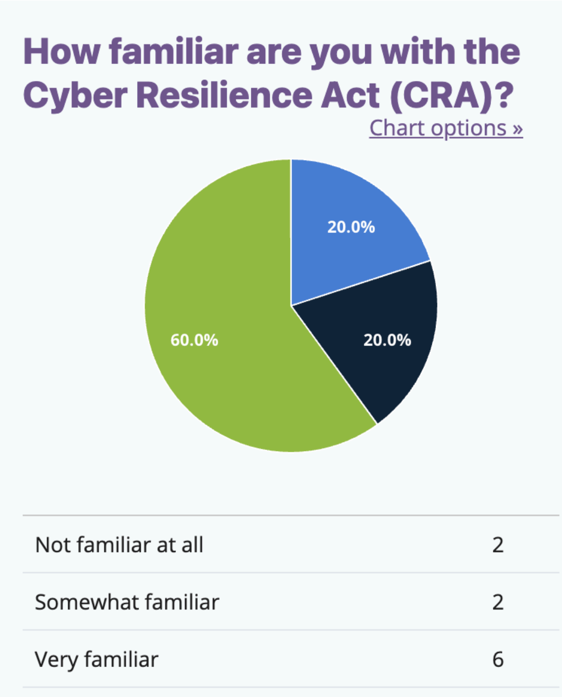


How long have your products been on the market? (Select all that apply)

Entering market shortly	6
1-3 years	4
4-10 years	4
10-19 years	4
20+ years	3

2.3.2 Awareness and Understanding

The survey highlighted relatively strong awareness of the CRA among SME respondents. Most described themselves as either “somewhat familiar” or “very familiar” with the regulation. However, despite this self-reported familiarity, none of the respondents had yet conducted a CRA self-assessment or implemented CRA-aligned processes within their development workflows. A few indicated that such evaluations were being planned, but the majority had not translated awareness into operational procedures.



How familiar are you with the Cyber Resilience Act (CRA)?

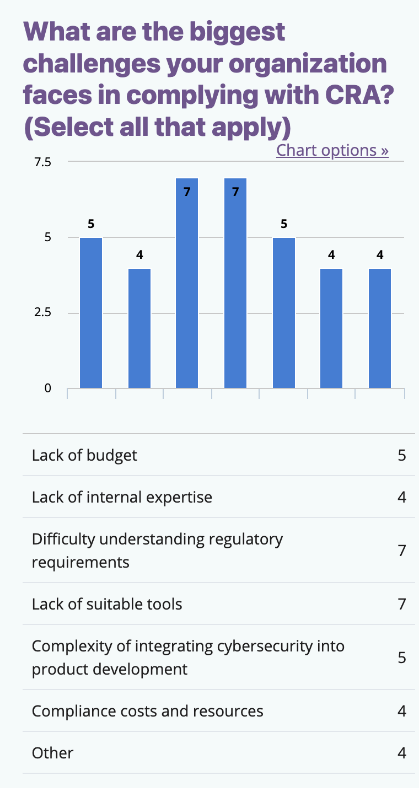
Not familiar at all	2
Somewhat familiar	2
Very familiar	6

This result underscores a challenge similar to that observed in the FOSS community: while SMEs recognize the relevance of the CRA, they lack clear direction on how to implement it and who within their organization should be responsible. This reinforces the need for actionable guidance and lightweight onboarding strategies tailored to SME environments.

2.3.3 Challenges identified for SMEs

SMEs consistently pointed to a lack of clarity regarding CRA requirements. Key challenges reported included: insufficient internal resources, difficulty identifying applicable obligations, the absence of accessible tools, and uncertainty around documentation and vulnerability management expectations. The most cited barriers were:

- Difficulty understanding regulatory requirements,
- Lack of suitable tools for SME-scale implementation,
- Limited staffing or dedicated cybersecurity functions,
- Budget constraints.



What are the biggest challenges your organization faces in complying with CRA? (Select all that apply)

Lack of budget	5
Lack of internal expertise	4
Difficulty understanding regulatory requirements	7
Lack of suitable tools	7
Complexity of integrating cybersecurity into product development	5
Compliance costs and resources	4
Other	4

These challenges mirror those reported by FOSS contributors but are further amplified in SMEs by resource limitations and time constraints. SMEs also noted that existing CRA resources appear oriented toward large enterprises, with few practical tools available to smaller players.

2.3.4 Cybersecurity Practices

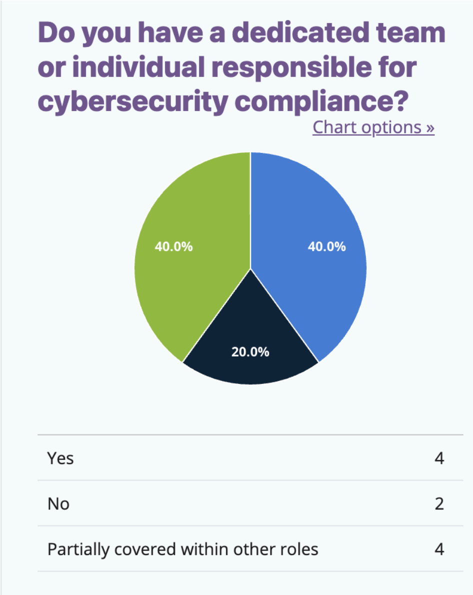
The range of security practices among SMEs varied significantly. Some companies had already begun implementing basic controls such as secure coding guidelines, automated code reviews, and use of code analysis tools. Others relied on informal reviews or external consultants. A small subset had established threat modeling or vulnerability tracking mechanisms, but only a few had formalized these processes.

Only a minority of SMEs reported having a dedicated person or team in charge of cybersecurity compliance. In most cases, cybersecurity responsibilities were either partially distributed across multiple roles or not formally assigned at all.

When asked about secure design integration, most SMEs described partial consideration of cybersecurity during product development, while only a few followed systematic approaches. Obstacles mentioned included limited engineering time, insufficient knowledge of secure development, and difficulty identifying and remediating vulnerabilities at the design stage.

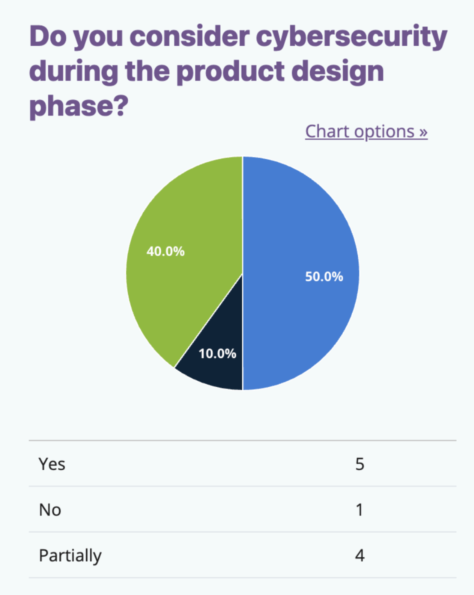
Still, several respondents indicated they already use tools such as secure coding checklists, GitHub CodeQL, static analysis tools, and in some cases threat modeling frameworks like

STRIDE or PASTA. However, these practices were usually informal or limited in scope, and rarely tied to CRA compliance objectives.



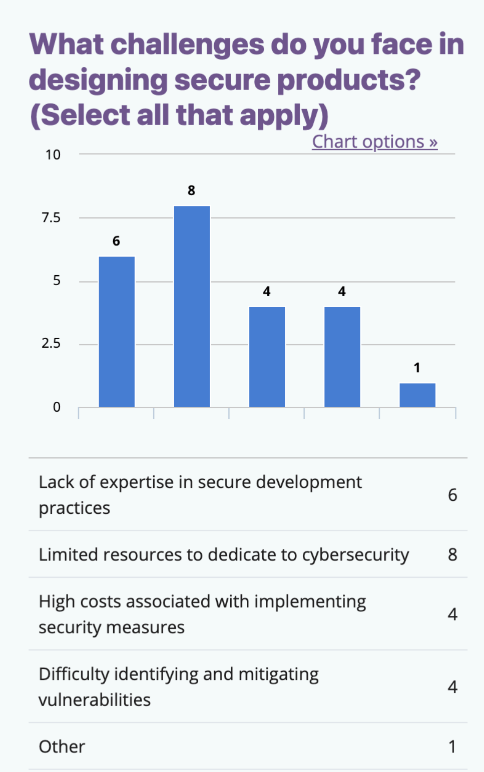
Do you have a dedicated team or individual responsible for cybersecurity compliance?

Yes	4
No	2
Partially covered within other roles	4



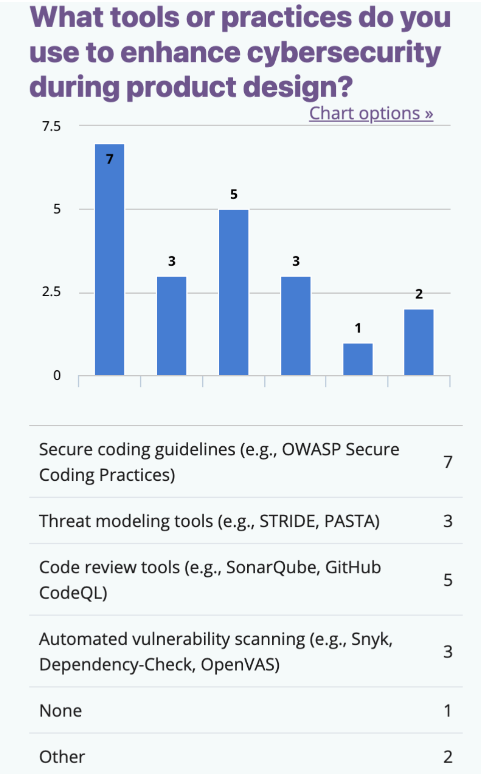
Do you consider cybersecurity during the product design phase?

Yes	5
No	1
Partially	4



What challenges do you face in designing secure products? (Select all that apply)

Lack of expertise in secure development practices	6
Limited resources to dedicate to cybersecurity	8
High costs associated with implementing security measures	4
Difficulty identifying and mitigating vulnerabilities	4
Other	1



What tools or practices do you use to enhance cybersecurity during product design?

Secure coding guidelines (e.g., OWASP Secure Coding Practices)	7
Threat modeling tools (e.g., STRIDE, PASTA)	3
Code review tools (e.g., SonarQube, GitHub CodeQL)	5
Automated vulnerability scanning (e.g., Snyk, Dependency-Check, OpenVAS)	3
None	1
Other	2

2.3.5 Lifecycle management and vulnerability handling

Few SMEs had implemented lifecycle practices aligned with CRA expectations. Only one respondent reported having a formal process for managing security updates. Several others were in the process of establishing such procedures, while two had no plans in place. Security update management was often dependent on customer feedback or reactive fixes rather than structured monitoring.

The situation was similar for vulnerability tracking. Most SMEs relied on manual tracking methods. A few used SBOM generation tools or dependency monitoring solutions, but coverage was inconsistent. In one case, vulnerability tracking was not performed at all.

These responses highlight the lack of scalable tools that can be integrated into existing SME workflows, tools that would enable automated tracking, update scheduling, and documentation aligned with CRA post-market obligations.

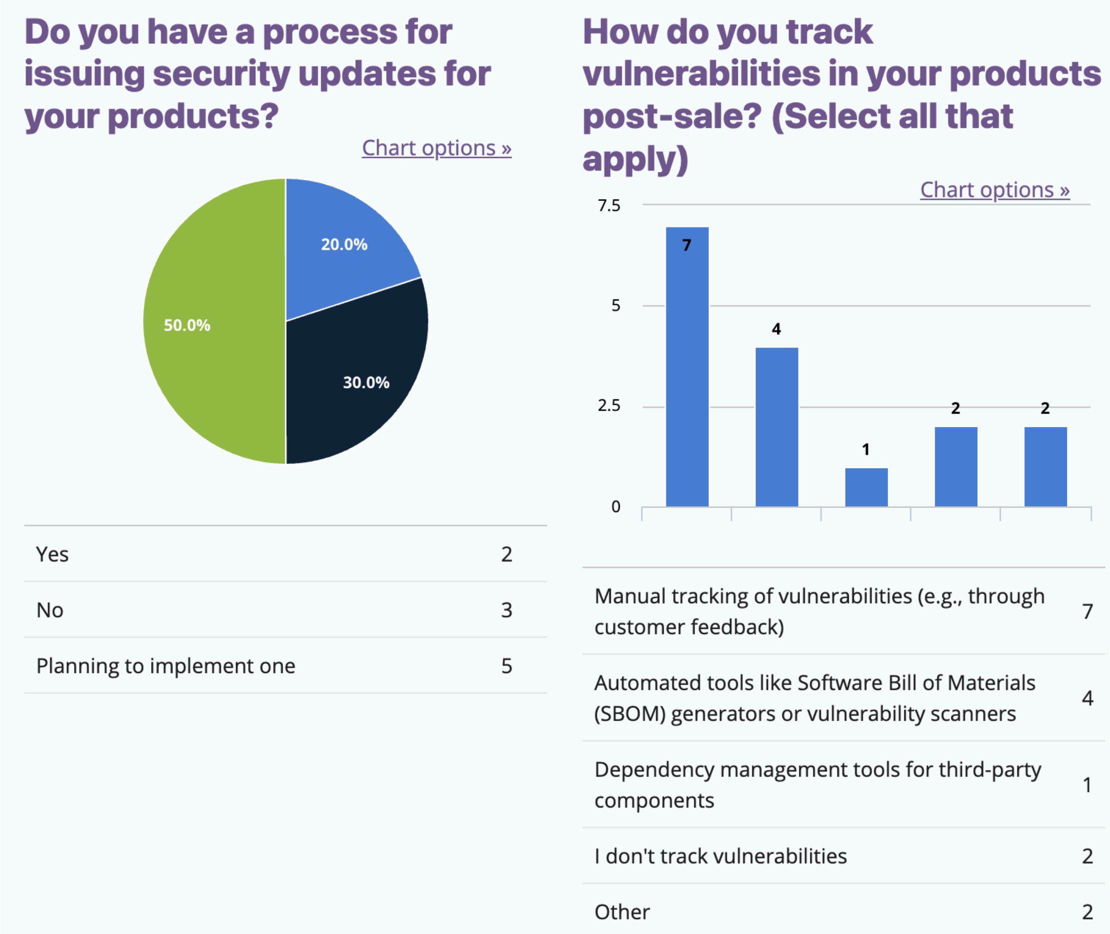

Do you have a process for issuing security updates for your products?

Chart options »

Yes	2
No	3
Planning to implement one	5

How do you track vulnerabilities in your products post-sale? (Select all that apply)

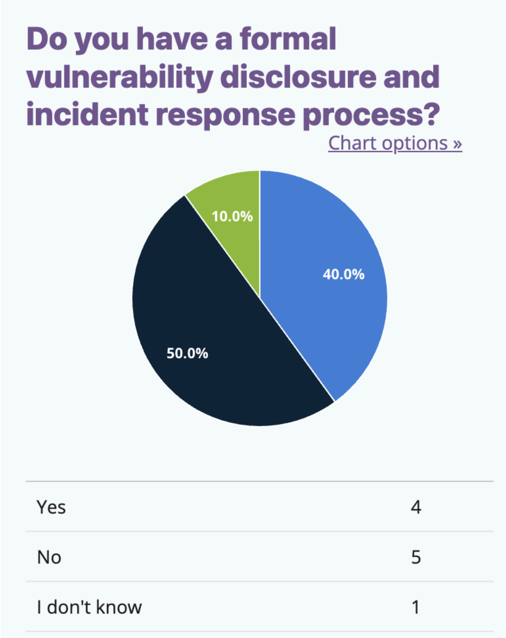
Chart options »

Manual tracking of vulnerabilities (e.g., through customer feedback)	7
Automated tools like Software Bill of Materials (SBOM) generators or vulnerability scanners	4
Dependency management tools for third-party components	1
I don't track vulnerabilities	2
Other	2

2.3.6 Vulnerability Disclosure and Incident Response

As with FOSS projects, formal vulnerability disclosure and incident response procedures were not yet widely implemented among SMEs. Three respondents reported having formal processes, three did not, and one was unsure. Similarly, only three stated that their current practices follow Coordinated Vulnerability Disclosure (CVD) principles.

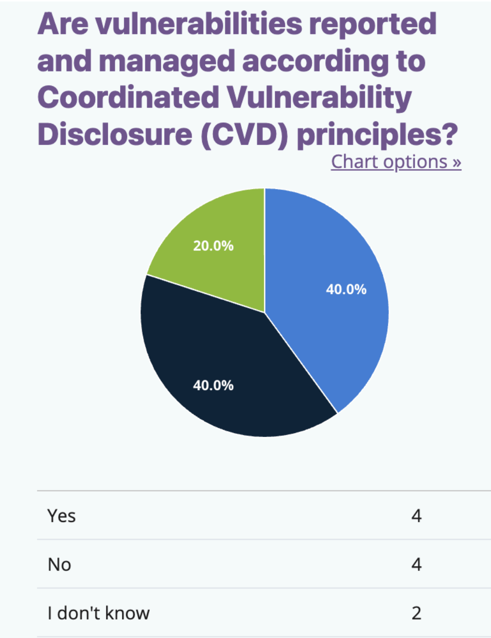
This result suggests that while SMEs are aware of the importance of vulnerability handling, many have not translated that awareness into structured or CRA-aligned processes. There is a clear opportunity for lightweight disclosure policy templates and pre-approved messaging workflows.



Do you have a formal vulnerability disclosure and incident response process?

Chart options »

Yes	4
No	5
I don't know	1



Are vulnerabilities reported and managed according to Coordinated Vulnerability Disclosure (CVD) principles?

Chart options »

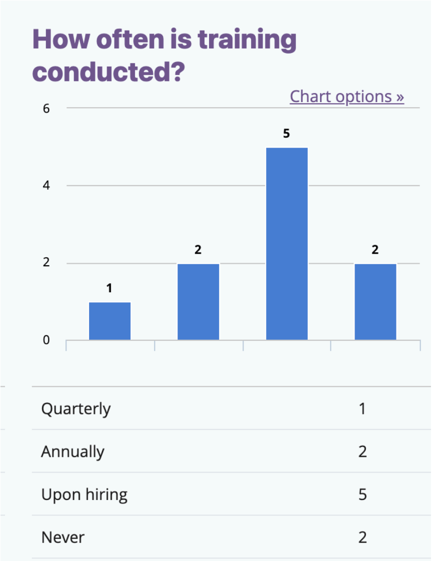
Yes	4
No	4
I don't know	2

2.3.7 Risk Assessments, Training, and Documentation

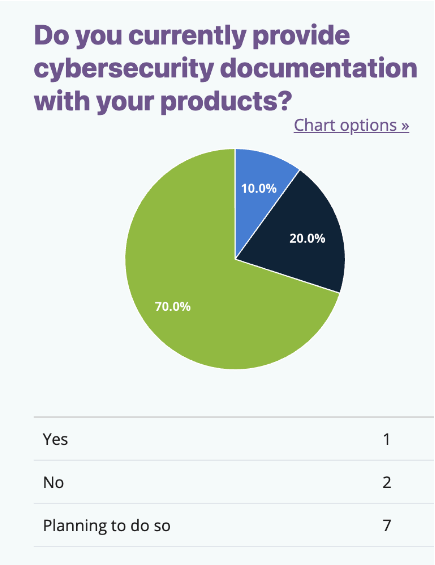
Although CRA-specific processes are rarely in place, many SMEs demonstrated positive trends in broader cybersecurity governance. Most provide cybersecurity training for staff, primarily during onboarding but also through annual or quarterly refreshers. Five SMEs conduct risk assessments on a regular basis, though these are typically general in scope and not explicitly tied to CRA requirements.

Documentation remains a significant gap. Only two SMEs currently provide cybersecurity documentation with their products, and five indicated plans to do so in the future. None currently publish material that would satisfy CRA’s transparency or security support period requirements.

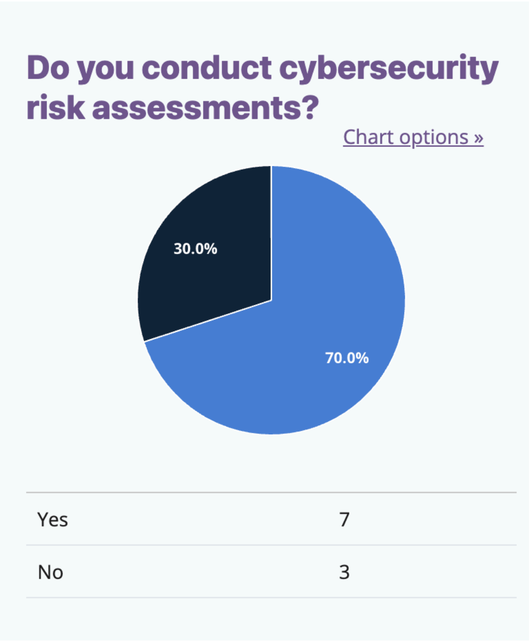
Respondents consistently expressed a desire for documentation templates, self-assessment guidance, and examples of what CRA-aligned product documentation should include.



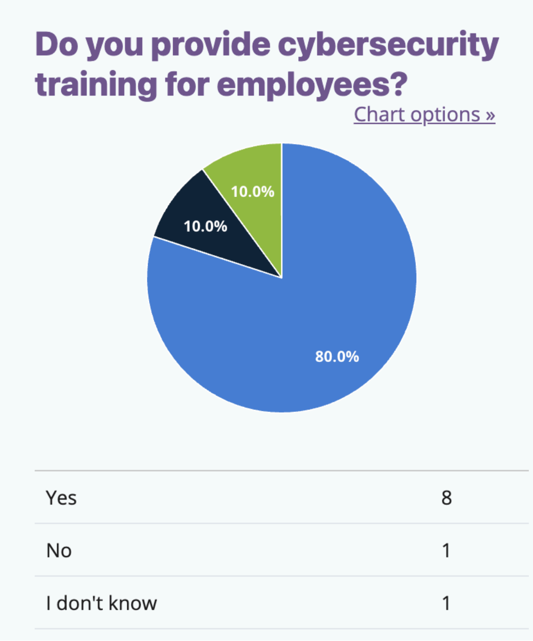
Quarterly	1
Annually	2
Upon hiring	5
Never	2


Do you currently provide cybersecurity documentation with your products?
Chart options »
10.0%
20.0%
70.0%

Yes	1
No	2
Planning to do so	7



Yes	7
No	3



Yes	8
No	1
I don't know	1

2.4 Cross-Cutting Observations and Project Implications

The findings presented in the previous subsections reveal consistent patterns across both FOSS contributors and SMEs. While awareness of the Cyber Resilience Act is developing, structured self-assessment and formal alignment of cybersecurity practices with regulatory requirements remain limited.

Across both groups, uncertainties persist regarding role identification and scope interpretation, particularly in complex supply chain and open-source integration contexts. Vulnerability handling and lifecycle practices often exist but are not consistently formalised in a compliance-oriented manner. Documentation and transparency requirements represent a significant readiness challenge, especially for smaller organisations with constrained resources.

These cross-cutting observations have directly informed the prioritisation of the OCCTET compliance framework and tooling development.

2.5 Methodological Note on Representativeness

The survey findings presented in this section reflect the results of an initial consultation round conducted during RP1. While the responses provide valuable qualitative insight into recurring challenges and patterns across SMEs and FOSS contributors, the dataset is not intended to constitute a statistically representative sample of the broader European ecosystem.

In line with the project lifecycle described in the Description of Action (DoA), these results serve as a structured baseline informing the development of the OCCTET compliance framework. Broader and more systematic validation is foreseen under WP4 (Validation – Use Cases) during RP2, where the OCCTET toolkit — including the self-assessment portal and associated compliance instruments — will be tested with participating SMEs. Continued stakeholder mobilisation and ecosystem outreach under WP5 (Dissemination and Community Engagement) will further support expanded participation and progressive refinement of the framework. This phased approach ensures that the compliance model evolves based on cumulative real-world evidence and structured engagement.

2.6 Translation into Tools and Iterative Validation

Stakeholder input has been systematically integrated into the design of the OCCTET compliance instruments.

Identified uncertainties regarding scope and role identification informed the structure of the Self-Qualification Questionnaire. Operational readiness gaps shaped the Technical Maturity and Process Assessment. Recurrent weaknesses in vulnerability handling and documentation influenced the compliance journey logic under WP4.

In addition, stakeholder feedback oriented the refinement of the digital platform developed by EXP. Observations concerning usability expectations, need for clearer onboarding, role-based guidance, and preference for lightweight workflows have influenced workflow sequencing, explanatory content structure, and feature prioritisation within the website tool.

Stakeholder engagement under WP2 represents the first phase of an iterative validation process. Survey findings are informing tool refinement under WP4 and workshop targeting under WP5. Future survey iterations embedded within the OCCTET platform will allow structured maturity data collection and progressive refinement of guidance materials based on aggregated usage patterns.

3 Open-source community obligations

The European Commission wants to encourage innovation without adding too many regulatory obligations which might be difficult to fulfill by individuals, small and medium organisations or open-source communities. In line with European Commission guidance, open-source software developed outside of a commercial context may fall outside the scope of certain CRA obligations. However, applicability depends on the specific role assumed within the supply chain and the commercialisation pathway of the software component.

The Cyber Resilience Act (CRA) outlines only few obligations and voluntary measures for open-source software stewards:

1. **Cybersecurity Policy**: Implement and document a cybersecurity policy to foster secure development and effective vulnerability handling by developers. This policy should promote voluntary reporting of vulnerabilities and include aspects related to documenting, addressing, and remediating vulnerabilities.
2. **Cooperation with Authorities**: Cooperate with market surveillance authorities to mitigate cybersecurity risks posed by open-source software. Provide documentation of the cybersecurity policy upon request.
3. **Reporting Obligations**: Notify actively exploited vulnerabilities and severe incidents impacting the security of products with digital elements to the CSIRT designated as coordinator and ENISA, if involved in the development of the products.
4. **Voluntary Reporting**: Facilitate voluntary reporting of vulnerabilities, cyber threats, incidents, and near misses to CSIRTs or ENISA.
5. **Security Attestation**: Participate in voluntary security attestation programs established by the Commission to assess conformity with essential cybersecurity requirements.

These obligations aim to ensure that open-source software communities contribute to the overall cybersecurity landscape by maintaining secure development practices and effectively handling vulnerabilities.

To further encourage collaborative software development an exception has been made so administrative fines do not apply to the open-source software stewards for a failure to meet the 24-hour deadline for the early warning notification of actively exploited vulnerabilities or severe cyber security incidents impacting the software projects they coordinate.

4 SME CRA self-qualification Questionnaire

The questionnaire has been developed to assist SMEs achieving the following objectives:

Objective1: Understand if the SME must comply with the Cyber Resilience Act regulation.

Objective2: If the SME falls under CRA regulation assess the important and/or criticality of their product or services:

a) Default products,
b) Important products class I ,
c) Important products class II,
d) Critical products.

Objective3: Provide guidance/QuickStart for:

e) Conformity assessment requirements (internal assessment and/or third-party assessment),
f) CRA Maturity assessment template.

4.1 Self-Qualification Questionnaire

Basic Company & Business Profiling

Q1: In which activity sector is your company operating?

Why it matters: Some sectors already have ***specific cybersecurity regulations*** *(e.g., medical devices, automotive, aviation, marine equipment, radio equipment). If you fall under a more specific regulatory regime, you might be* ***excluded*** *from the CRA or have overlapping requirements.*

Examples: Consumer electronics, healthcare, industrial IoT, finance/banking, retail, telecom, etc.

Q2: How many employees does your company/organization have?

Why it matters: Although the CRA applies regardless of size, smaller companies may have simpler processes or different compliance approaches and also might rely more heavily on self-assessment if possible.

Examples: 1–9 (micro), 10–49 (small), 50–249 (medium), 250+ (large).

Q3: Does your organization develop, manufacture, import, or distribute any product with “digital elements”?
[Yes / No / Maybe]

Examples of “digital elements” include:

- A **smart door lock** that connects to a home Wi-Fi network.
- A **software application** for desktops or mobile devices that relies on the internet for updates.

- A **hardware device** (e.g., a sensor) that sends data to a server or the cloud.

If the answer is “**No”**, you are **outside** the CRA scope.

For instance, if your company produces mechanical door locks with **no** digital interface then you do not need to comply with CRA regulation.

If the answer is “**Maybe”**, please clarify whether any connectivity is possible, **even indirectly** (e.g., it could connect via Bluetooth to a phone, or the device could upload logs to a cloud server).

If the answer is **“Yes”** you need to answer the following questions:

Q4: Do you place (or plan to place) your product(s) on the EU market?
[Yes / No / Maybe]

Examples include:

- Selling through an EU e-commerce site, having distributors in Europe, or a direct B2B partnership within the EU.

If the answer Is “**No”**, the CRA regulation does not apply □ “Stop”.

If the answer is “**Yes”**, please continue.

Q5: What is your activity type ?
[Manufacturer/Service Provider/ Importer/Distributor]

Choose **“Manufacture**r / **Service Provider”** if you produce or develop the product or service under your own brand. The product or service includes digital components.

Choose **“Importer”** if you bring to EU products from outside the EU area.

Choose **“Distributor”** if you sell or supply products already in free circulation within the EU.

Why it matters:

Manufacturers and Service providers bear the primary CRA obligations:

- Comply with the conformity assessment.
- Develop and maintain technical documentation for products or services.
- Ensure CE marking.
- Perform post-market surveillance.

Importers must verify that manufacturers’ products comply and bear correct markings. If the products have not been certified or have not been correctly labelled that the Importers must perform the conformity assessment and correctly mark the products.

Distributors must ensure products are properly marked and that the manufacturer/importer followed CRA requirements and provide for each product/server the corresponding conformity assessment.

Q6: Is your product or service entirely covered by another specific sectoral regulation (medical device, automotive, radio equipment)?
[Yes / No / Maybe]

Examples of sectoral regulations include:

- Certain medical devices that have specific cybersecurity requirements under EU medical device legislation.
- Certain radio equipment under the Radio Equipment Directive (RED), if the directive already addresses the relevant cybersecurity aspects.

If the answer is "**Yes**", you may be still *excluded* from the CRA scope. (E.g., a **pacemaker** covered fully by medical device regulations might be excluded as the health certification already encompasses the CRA requirements).

Q7: Is there any scenario in which your product handles or processes data (user data, logs, sensor readings, etc.) that could be compromised if hacked?
[Yes / No / Unsure]

If the answer is **"Yes"**, it strongly indicates your product has a cybersecurity relevance hence you must comply with the CRA regulation.

Even if the data processed seems minimal, if it contains personally identifiable information (home address, national id, date of birth, personal email or phone, etc.) or critical business info, the CRA regulation applies.

Q8: Is your product purely SaaS (Software-as-a-Service)
[Yes / No / Unsure]

Examples:

- A cloud-based CRM accessed only via browsers, no local install.

  (E.g. no physical or embedded software/hardware product placed on the market?)

If the answer is **"Yes"** (no hardware or installable software provided to the customers), your SME is not in the scope of CRA regulation. **"Stop"**

Q9: Is your software free, not-for-profit open source with no paid commercial services or revenue model?
Possible Answers = [Yes / No]

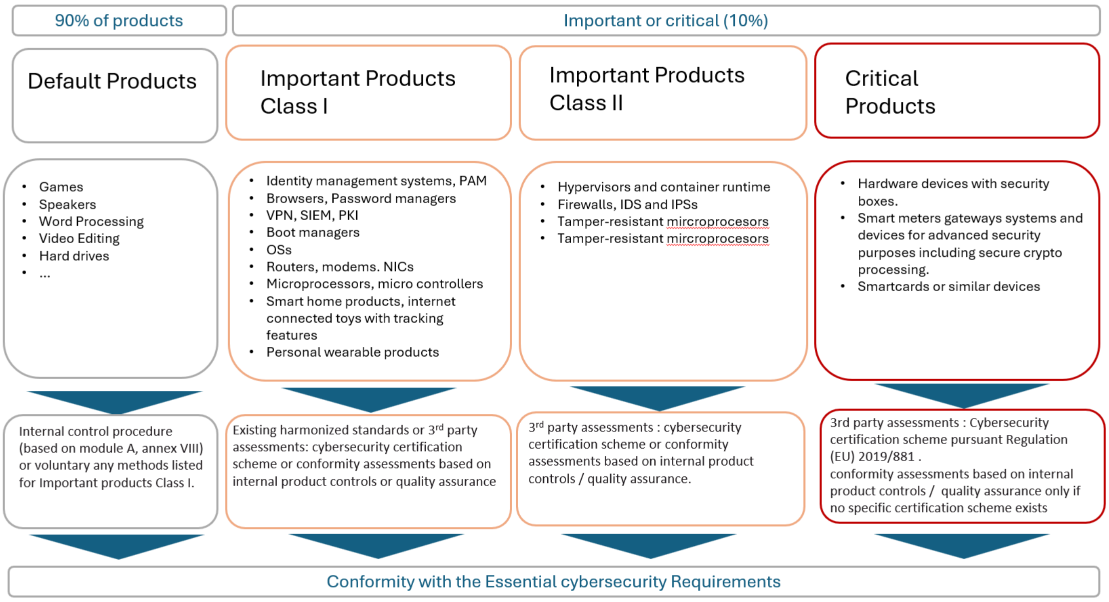
If the answer is "**Yes"**, not part of a commercial package and no commercial revenue model then your business is not in scope of CRA regulation **"Stop"**
If the answer is "No" continue to assess the criticality of your product or service.

Q10: Does your product appear in Annex III (list of "Important Products with Digital Elements") or Annex IV (critical products)?

Possible Answers = [Yes / No / Maybe]

If **Yes** or **Maybe**, see Sections **3.2** (Class I), **3.3** (Class II) or **3.4** (Critical) below.

If **No**, **your product is likely the "default product" (not important and not critical).**



90% of products	Important or critical (10%)		
Default Products	Important Products Class I	Important Products Class II	Critical Products
• Games • Speakers • Word Processing • Video Editing • Hard drives • ...	• Identity management systems, PAM • Browsers, Password managers • VPN, SIEM, PKI • Boot managers • OSs • Routers, modems. NICs • Microprocessors, micro controllers • Smart home products, internet connected toys with tracking features • Personal wearable products	• Hypervisors and container runtime • Firewalls, IDS and IPSs • Tamper-resistant mircroprocesors • Tamper-resistant mircroprocesors	• Hardware devices with security boxes. • Smart meters gateways systems and devices for advanced security purposes including secure crypto processing. • Smartcards or similar devices
Internal control procedure (based on module A, annex VIII) or voluntary any methods listed for Important products Class I.	Existing harmonized standards or 3rd party assessments: cybersecurity certification scheme or conformity assessments based on internal product controls or quality assurance	3rd party assessments : cybersecurity certification scheme or conformity assessments based on internal product controls / quality assurance.	3rd party assessments : Cybersecurity certification scheme pursuant Regulation (EU) 2019/881 . conformity assessments based on internal product controls / quality assurance only if no specific certification scheme exists

Conformity with the Essential cybersecurity Requirements

Q11: Even if not explicitly in Annex III or Annex IV, does your product's failure (due to a cyber security incident) pose a high risk for users or society, especially if used in critical infrastructures or essential services?

Possible Answers = [Yes / No / Maybe]

If the answer is "**Yes**", you may need to confirm with the relevant authority whether you are *de facto* considered "important" or "critical." Otherwise, you remain the default.

Outcome:

- **Default products** → see Section 2.4 for self-assessment.
- **Important Products** (Annex III or by determination) → (Class I) or (Class II).
- **Critical Products** (Annex IV or by determination) → required to obtain a European cybersecurity certificate at assurance level at least 'substantial' under a European cybersecurity certification scheme

4.1.1 Important Products Class I (Annex III, Class I)

Products listed under Class I in **Annex III** (e.g., identity management systems, standalone and embedded browsers, password managers, software that searches for, removes or quarantines malicious binaries, products with digital elements including the function of virtual private network, network management systems, certain routers, mobile device management software, non-Class II operating systems, etc.)

- If you **fully apply** recognized **harmonized standards** (EN standards from CEN/CENELEC/ETSI) or an **EU cybersecurity certification scheme** under the Cybersecurity Act, you can do a **self-assessment**.

Example: You develop a **consumer firewall device** and comply **100%** with an existing EN standard for consumer IoT security or you have fully adopted an **EU cybersecurity scheme**.

- If **no** such standard/certification scheme exists **or** you do **not** apply it in full, then you need a **third-party** conformity assessment.

Example: You make **specialized VPN software** but have not adopted any recognized EU cybersecurity standards → third-party security assessment is mandatory.

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 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 Regulation (EU) 2017/746 do not apply, or personal wearable products that are intended for the use by and for children

4.1.2 Important Products Class II (Annex III, Class II)

Review Annex III, Class II examples:

- **Hypervisor operating systems** (e.g., Windows Hyper-V, Linux KVM, VMware ESX, etc.)

- **General purpose microprocessors** (e.g., CPU chips typically integrated into a variety of devices)
- **Secure elements** (hardware-based security modules, e.g., TPMs)

For Class II, the rules are stricter:

1. Hypervisors and container runtime systems that support virtualized execution of operating systems and similar environments

2. Firewalls, intrusion detection and prevention systems

3. Tamper-resistant microprocessors

4. Tamper-resistant microcontrollers

Always requires **third-party** conformity assessment by a **Conformity Assessment Body (CAB)**.

4.1.3 Critical Products (Annex IV)

Examples:

- **Smart meters** used in energy distribution
- Smartcards
- **Industrial Automation & Control Systems (IACS)** intended for use by essential entities (like SCADA systems in a nuclear plant)

Always requires third-party certification or conformity assessment.

Fulfill applicable cybersecurity certifications as per Regulation (EU) 2019/881 or third-party compliant assessments based on internal product control (Annex VIII, module B) or full quality assurance (Annex VIII, module H)

5 CRA security requirements overview

The proposed CRA places the following obligations on **manufacturers, importers, and distributors**. The following section provides an overview for the different types of requirements introduced by the CRA regulation. A detailed list of requirements per each role is available in Annex IX .

There requirements related to the properties of the products, requirements related to the product release and requirements related to the post-market surveillance.

5.1 Security requirements relating to the properties of products with digital elements

Requirement	Sub-requirements
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	Perform a cyber security analysis should be conducted and monitored during the complete lifecycle of the product: ● Assess possible security risks. ● Define remediation strategy. Cybersecurity should be considered in every step of the product creation: ● Secure coding ● Security by design principles ● Adoption of Least Privilege Principle ("need-to-know" grants access only to the minimum set of actions required per role, "need-to-use" grants access to the minimum set of IT assets required per role).
Products with digital elements shall be delivered without any known exploitable vulnerabilities	Ensure vulnerability assessments were performed against the digital elements of the product prior release: ● During the design phase establish the list of digital components used.

	● Perform Static Code Analysis SCAP. ● Perform Dynamic Code Analysis Tests (DAST). blocking the release of the product if there are any “High” or “Critical” risks identified during tests. Ensure that detected vulnerabilities have been fixed prior to the release of the product.
(a) The product needs to be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	Foresee an initial/default credential which should use a complex and randomly chosen password, different for each product instance. Ensure that the default/factory configuration adopts a reasonable level of security for each item. Ensure that the default configuration is placed in a non-erasable memory. Implement the functionality to reset the product configuration to the default/factory configuration.
(b) Ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	An appropriate system to provide authentication and authorization should be implemented. Access to sensitive data and information should be granted only to authenticated and authorized users. In accordance with the nature of the product and to the relevant risks identified in the risk analysis, physical unauthorized access should be forbidden.
(c) 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;	Data stored in a product’s internal memory should be encrypted at rest using current non-deprecated technology. Transmission protocols used to send/receive data should support encrypted communications and enable them by default.
(d) Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not	Integrity of data, programs and configurations stored in the product’s internal memory should be ensured using current non-deprecated technology (e.g. hashing). Transmission protocols used to send/receive data should support ways to ensure it is possible to spot data alteration during the transmission (e.g. implement mechanism for integrity based on digital signatures and MACs).

authorized by the user, as well as report on corruptions;	The product should implement symmetric or asymmetric encryption schemes (including PKIs) to ensure that the integrity of exchanged data is protected. A product should perform self-test to verify integrity of relevant code/information (e.g. firmware checksum check).
(e) Process data that is adequate, relevant and limited to what is necessary in relation to the intended use of the product (minimization of data);	It should not be asked to the user the provision of data that is not strictly necessary to the execution of the task or service requested. Data no longer needed should be deleted without delay.
(f) Protect the availability of essential functions, including the resilience against and mitigation of denial-of-service attacks;	The product should be hardened against attacks, like for instance distributed denial of service attacks, by implementing, among other things, the following measures if appropriate: ● reverse proxies network segmentation ● load balancing ● rate limiting ● redundancy and high availability solutions ● backup sites ● disaster recovery plans minimize offered services
(g) Minimize the negative impact on the availability of services provided by other devices or networks;	The product should limit outgoing network connections to what is strictly needed. The product should implement measures such as timeouts and exception handling to avoid generating multiple requests to a busy/not responsive service.
(h) The product needs to be designed, developed and produced to limit attack surfaces, including external interfaces;	The product's hardware design should limit all the connections and interfaces that are not strictly required for performing the various tasks the product is expected to do. If required by a risk assessment, a physical product should include tamper-resistant features. The product/service should have all non-essential network ports closed as a default configuration.

	Software present in digital products should be designed to avoid having unnecessary entry points (e.g. API) open and available for external unauthorized callers.
(i) The product needs to be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	The product should be designed in a way that gaining unauthorized access to a function or data does not automatically lead to complete access to all product's functions and data (defense in depth principles). Sensitive data stored in a product's internal memory should be encrypted at rest. The product should not store data that is not relevant or necessary to perform its tasks (data minimization).
(j) Provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;	A product should contain a log of cybersecurity related events. Access or modification of data, services or functions should be logged. Such a log should be accessible to the privileged user. Logs should be protected from unauthorized modification or corruption.
(k) Ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users;	The company distributing a product or service should provide timely security updates for the software components of the product/service for a reasonable amount of time. A function to automatically check the presence of updates and install them, or notify the user of their presence, should be implemented, and where applicable this should be the default initial configuration. A product should provide a secure mechanism to install/implement updates. The company distributing a product should notify the user on the availability of updates

5.2 Release requirements for products with digital elements

- Pass a conformity assessment (detailed procedure available in Annex VIII).
- Attach the Conformity certificate (based conformity assessment made by national body or by ENISA)

- Ensure CE Marking on the product
- Provide Technical documentation

5.3 Post market surveillance

1.1

Requirement	Sub-requirements
Vulnerability management preparation	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: ● Monitor status of the overall supply chain for the acquisition of the necessary components incorporated in the product should be put in place. ● List all libraries and external components used in the software part of a product, including their version number in a Software Bill of Material (SBOM) available to the end users.
Vulnerability remediation process	Address and remediate vulnerabilities without delay, including by providing security updates: ● In case vulnerabilities are found they should be classified in accordance with standard severity metrics (e.g. CVSS) and disclosed to the end-users. ● Vulnerabilities that can be directly fixed by the company should be fixed without delay, in accordance with their severity and the risks posed. ● In case a vulnerability is found in a software component of a product (including libraries and third-party components), an update should be prepared and distributed as soon as possible. ● The company developing a product or service should be subscribed to updates coming from CERTs and cybersecurity organizations and analyze them to spot vulnerabilities in their products.

	● The company developing a product or service should remain updated on the release of new versions of the libraries or third-party software components included in their products/services and update the relative software whenever such new version includes a security update. Provide mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner: ● Security updates should be digitally signed using a Code Signing Certificate to ensure the identity of the issuer. ● Provide hashes (checksums) and instructions for the end-user to verify the integrity and authenticity of the updates. Register & monitor cyber threat intelligence (CTI) feeds for new threat indicators (TIs) related to any components contained in the SBOM. Inform users about the existence of new security updates via automatic distribution, pop ups, newsletters etc.
Regular tests and reviews	Perform periodic vulnerability assessments based on the products' criticality. The software maintenance process must include automatic tests before a new commit/build/version is prepared (part of the Continuous Integration/Continuous Deployment pipelines). Perform regular risk assessments re-evaluating if there are significant changes (new threats, new vulnerabilities) Set-up “bug bounty programmes” to incentivize security researchers.
Vulnerability disclosure process	When a new 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 affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities. Release publicly new CVE indicators as soon as a security update has been released. Develop and enforce a policy on coordinated vulnerability disclosure.

	The security policies should be published in a machine-readable format. The company distributing a product/service should have a contact point specifically advertised to collect information related to vulnerabilities found in their products/services.
Reporting cyber security incidents to authorities	The company distributing a product/service should inform any relevant authority (e.g. national CERT/CSIRT) about how they can be reached in a timely manner for reasons related to the handling of vulnerabilities

5.4 Example use cases

QuickStart

- **Manufacturers** → comprehensive obligations, including post-market surveillance, patching, etc.
- **Importers** → verify compliance, CE marking, etc.
- **Distributors** → ensure products are compliant before onward supply.

Are you a manufacturer?

You design and produce fitness **wearable** with embedded software under your brand, or you develop a **mobile operating system**.

You must ensure the product meets all CRA requirements: essential product security requirements, product release requirements and vulnerability handling requirements.

Are you an importer?

You buy “smart home sensors” from a company based outside the EU, then bring them into the EU and sell them under the original brand.

You must verify the product’s compliance, ensure the manufacturer provides conformity assessment, that if the CE marking is present, and that the vulnerability reporting and handling requirements are fulfilled.

Are you a distributor?

You operate a web store or a retail shop in the EU and sell consumer electronics that are already in free circulation (imported by someone else).

You must check the product has a CE marking and ensure that the manufacturer/importer complied with the CRA.

6 Conformity Assessment Path & Key Obligations

Once you determine the CRA scope (non-important, important Class I, important Class II or critical) and the business role (manufacturer/importer/distributor), you need to assess which conformity assessment procedure applies to your particular case. To achieve that we provide sample easy to answer questions and answers to highlight the decisional process involved.:

6.1 Question 1

Is your product classified as non-important?

Example: You produce a **digital photo frame** with optional Wi-Fi connectivity which is not listed under Annex III and it does not pose major security risks.

The answer is likely “**Yes”**, so it is sufficient that you perform a **conformity self assessment based on internal control**.

6.2 Question 2

Is your product classified as an important Class I product, and are you applying recognized EU harmonized standards or EU cybersecurity certification schemes in full?

Example: You produce a **home router** (listed under Class I products) and you fully adopt the relevant ETSI EN standards for consumer routers.

If the answer is **Yes**, you can perform a **self-assessment**.

If the answer is **No**, you need to initiate a **third-party** conformity assessment.

6.3 Question 3

Is your product classified as an important Class II product?

Example: A **general-purpose operating system** or a **smart meter** for utility companies.

The answer is “**Yes”**, hence a **third-party** conformity assessment is **mandatory**.

6.4 Question 4

Have you prepared the necessary technical documentation to show compliance with the essential cybersecurity requirements?

Examples of documents include:

- **Risk assessment reports** (showing identified threats and mitigations).
- **Secure development process**
- **System architecture** diagrams explaining how data flows are protected.
- **Testing reports** (vulnerability scans, penetration tests).

6.5 Question 5

Have you established procedures for?

- **Post-market surveillance obligations (**see section 5.3**)**:

Example: Ensure you have regular security assessment reviews, a dedicated vulnerability disclosure policy, a process which ensures that new patches are developed within a defined timeframe, the process to report security incidents or non-compliance to authorities.

6.6 Question 6

Can you provide a Simplified EU Declaration of Conformity (DoC) and affix a CE marking if you are the manufacturer?

Example: Ensure You have already the conformity assessment and the **CE marking**.

7 CRA Self-Qualification Examples

Below we offer practical examples evaluating the CRA regulation applicability for SMEs holding different roles (manufacturers, distributors, software developers, etc.) , indicating the decisional process and the outcomes.

7.1 Example 1: SME Producing Electrical Appliances

Such an SME integrates various IoT components allowing remote operations and / or collection of operational metrics used for forecasting/profiling the users. Although the SME is only fitting together components it has the obligation to ensure CRA compliance.

Scenario

- The SME manufactures **household electrical appliances** (e.g., washing machines, ovens) which now include **IoT components** enabling remote monitoring/operation.
- The appliance collects usage metrics for forecasting or user profiling.

Decision flow

Step 1: Identify Connectivity & Exclusions

- The appliances are connected (Wi-Fi/IoT).
- Not covered by other specific regulations (like medical or automotive), and not purely free OSS → **In scope**.

Step 2: Check Annex III

- Is a “smart oven” or “connected washing machine” explicitly in Annex III as a critical product? Typically, No, unless there’s a special note for high-risk embedded controllers.
- Most likely “Non-critical” (Common).
- However, if the control system is deemed critical (some industrial use), it could be Class I. Usually for consumer appliances, it remains non-critical.

Step 3: Determine Conformity Assessment

- As a **non-important** product, the SME can do **an internal assessment**: declare compliance with essential cybersecurity requirements.
- They must still ensure basic security, handle vulnerabilities, and maintain tech documentation.

Step 4: Verify Role

- The SME is the **manufacturer** → must affix CE marking, ensure full CRA obligations (updates, vulnerability disclosure channel, etc.).

Step 5: Confirm Ongoing Obligations

- Must provide **software/firmware updates** if vulnerabilities are found, keep a simple **SBOM** for IoT components, and maintain a **vulnerability disclosure channel**.

Result

- Conduct an **internal assessment** based on the essential requirements.

- Document the process, affix CE marking, continue to patch vulnerabilities.
- Because it's likely "non-critical," no **third-party** conformity assessment is needed (unless certain risk factors push it into Class I).

7.2 Example 2: SME Producing Web Components

Scenario

- The SME develops **web-based components** or libraries (e.g., a JavaScript framework or a web plugin) that customers integrate into their websites or apps.
- Some of these libraries collect user data or have built-in APIs for real-time communication.

Decision flow

Step 1: Identify Connectivity & Exclusions

- The software is definitely "with digital elements," and it's **distributed** to EU customers.
- It's not purely SaaS (the code is downloaded/embedded). Also not a non-profit OSS. → **In scope**.

Step 2: Check Annex III

- Typical "web components" are not listed as "critical" (like OS, routers, firewalls).
- So, likely non-critical again—unless it's more specialized (e.g., a security library for password management, which might appear in Class I).

Step 3: Determine Conformity Assessment

- As **non-critical**, the SME can **self-declare** compliance, ensuring the library meets CRA's essential requirements for cybersecurity.
- If the library includes advanced encryption or password vault features, it **could** be a "password manager" (Annex III, Class I) → then they'd need to see if recognized standards apply or do third-party certification.

Step 4: Verify Role

- They are effectively the **manufacturer** of the software → must keep documentation on design, vulnerabilities, patch process, and affix CE marking for distribution within the EU context.

Step 5: Confirm Ongoing Obligations

- Provide **updates/patches** for discovered vulnerabilities.
- Maintain a **vulnerability disclosure policy**.
- Have a notification process for the newly vulnerabilities identified
- Ensure you monitor CTI feeds regarding the possible discovery of new vulnerabilities in software components used.
- Perform regular vulnerability tests based on product criticality.
- Establish a cyber security incident reporting process to national authorities.

Result

- **Most** web components from an SME are likely "non-critical" requiring **self-assessment**.

- If the plugin is **“critical”** (like a password manager or privileged access control), check if it’s Class I → then either apply recognized standards or engage a third-party for completing the conformity assessment.

7.3 Example 3: SME Distributor of Hardware/Software Products

Scenario

- The SME **doesn’t** produce or modify products; it **imports** or **resells** various hardware and software solutions in the EU.
- The hardware/software is produced by external manufacturers (possibly non-EU).

Decision Flow

Step 1: Identify Connectivity & Exclusions

- The products being distributed may have digital elements. The distributor is placing them on the EU market, so the CRA might apply.
- However, **distributors** do **not** do the design/manufacturing. They must ensure the products they sell are CRA-compliant.

Step 2: Check Annex III

- The SME as a distributor doesn’t decide classification—**each product** could be non-critical or critical.
- The main question for them is: “Is the product accompanied by the correct **Declaration of Conformity** and CE marking?”

Step 3: Determine Conformity Assessment

- The **manufacturer** is responsible for the conformity assessment. As a distributor, the SME must **verify** the product is correctly assessed.
- If it’s a **critical Class II** product, they must ensure the manufacturer used a **third-party**.
- If it’s a **non-critical** or Class I (with recognized standards), it can be self-assessed.

Step 4: Verify Role

- They are a **distributor** (or **importer** if from outside the EU).
- They must check that each product has a **CE marking** and the manufacturer has met CRA obligations.

Step 5: Confirm Ongoing Obligations

- If the distributor finds a product with no compliance marks or sees potential non-compliance, they must not place it on the market.
- They may also coordinate with manufacturers for **recalls or updates** in case of security flaws.

Result

- As a **distributor**, the SME does **not** do the testing or compliance themselves but must **ensure** the manufacturers do.
- If products are found non-compliant, the distributor must stop distribution and inform authorities as needed.

7.4 Example 4: SME Producing Specialized VPN Software

Scenario

- The SME develops a **VPN client/server application** for secure remote access.
- The software is sold to businesses and individuals across the EU.

Decision flow

Step1: Identify Connectivity & Exclusions

- This is definitely "with digital elements" and is distributed in the EU.
- Not purely not-for-profit OSS → **In CRA scope**.

Step 2: Check Annex III

- **VPN software** is specifically mentioned under "Critical (Class I)" in many draft lists (Annex III) because it handles secure tunnels and encryption.
- This means it's at least **Class I**.

Step 3: Determine Conformity Assessment Needs

- As **Class I**: If the SME **fully applies** recognized harmonized standards or an **EU cybersecurity certification scheme**, they can do **self-assessment**.
- If no recognized standard is fully applied → must do **third-party** assessment.

Step 4: Verify Role

- The SME is the **manufacturer** of the VPN product → must produce the **technical docs**, handle **CE marking**, track vulnerabilities, etc.

Step 5: Confirm Ongoing Obligations

- Because it's a security product, the SME must be extra vigilant: publish updates quickly for vulnerabilities, maintain a robust **vulnerability disclosure** channel, keep a **risk analysis** on cryptographic methods used, etc.

Result

- If they comply with an official standard or scheme (e.g., an ETSI EN or an EU cybersecurity certification), it's **self-assessment**. Otherwise, a **CAB** is needed to verify compliance.
- Must keep extensive documentation to prove the VPN meets CRA's essential security requirements.

7.5 Example 5: SME per sector Quick start

Sector	Example
Wholesale trade, except of motor vehicles and motorcycles	A company specializing in wholesale trade of electronics imports networking equipment from a third-party supplier. The wholesaler is responsible for ensuring that the supplier's devices meet CRA security and documentation requirements. Even if the products are off-the-shelf, the wholesaler must ensure that vulnerability disclosure, patch management, and secure configuration comply with CRA regulations.
Transportation and storage	A logistics company uses a fleet of autonomous warehouse robots sourced from a third-party robotics manufacturer. The logistics provider must verify that the robotics system meets CRA security and documentation standards. Even though the robots are pre-built, the company must ensure that firmware updates, security patches, and access control measures align with CRA regulations.
Services covered by CIS regulation	A cloud hosting provider offers managed database services using third-party database software. The hosting provider must ensure that the software complies with CRA security and documentation requirements. Despite being a third-party product, the provider must oversee patch management, vulnerability disclosures, and secure configurations in alignment with CRA rules.
Manufacturing	An industrial automation firm integrates third-party IoT sensors into its smart factory solutions. The manufacturer is responsible for ensuring that these sensors meet CRA security and documentation requirements. Even if the sensors are commercial off-the-shelf components, the firm must guarantee secure configurations, firmware updates, and adherence to vulnerability disclosure policies.
Information and communication	A telecom company deploys network infrastructure relying on routers sourced from an external vendor. The telecom provider must ensure that these devices meet CRA security and documentation requirements. Although the routers are pre-configured by the vendor, the telecom company must oversee firmware updates, security patches, and secure deployment in accordance with CRA guidelines.

Industry (except construction)	A chemical processing plant incorporates third-party PLC (Programmable Logic Controller) units to manage industrial processes. The plant operator must ensure these PLCs comply with CRA security and documentation standards. Even though the units are vendor-supplied, the operator is responsible for managing patches, security updates, and secure configurations.
Financial and insurance activities	A bank integrates third-party fraud detection software into its transaction monitoring system. The bank must verify that the software meets CRA security and documentation standards. Even if the software is developed externally, the bank must ensure secure deployment, timely patching, and compliance with vulnerability disclosure policies.
Economic activities covered by CIS regulation	A cybersecurity firm uses third-party SIEM (Security Information and Event Management) software for its managed security services. The firm must ensure that the software meets CRA security and documentation requirements. Although it is an external product, the firm remains responsible for updates, vulnerability management, and secure configurations.
Architectural and engineering activities; technical testing and analysis; scientific research and development; advertising and market research	A research institution employs third-party AI-powered analytics software for market research and scientific studies. The institution must ensure that the software complies with CRA security and documentation requirements. Even if the AI model is sourced externally, the institution is responsible for securing data handling, managing software updates, and adhering to vulnerability disclosure policies.

8 Technical maturity and processes assessment

Under **CRA Annex I**, products with digital elements must meet **cybersecurity requirements** and establish a **vulnerability handling process**. This includes, for example, **basic protective measures** (like secure default configurations) up to **comprehensive risk analysis**. Many SMEs find advanced tasks (like detailed risk assessments) daunting, so we provide a simplified, sample checklist which starts with the most **feasible** questions, then progresses toward **more complex** demands. A detailed cyber security maturity questionnaire and the toolset for SMEs self-evaluation will be later provided by the OCCTET project.

How to Use

- **Answer "Yes," "No," or "Partially"** for each question.
- If you answer "No" or "Partially," investigate **ways to improve** before claiming CRA compliance.
- As you progress, your organization should achieve gradual **maturity** in line with CRA requirements.

8.1 Basic Maturity Checklist

8.1.1 Foundational Security Practices

8.1.1.1 Basic Patch & Update Management

Question: "Do you have a simple routine or process to install updates for your product's software/firmware?"

- *Annex I* requirement: Ensuring the product can be updated when vulnerabilities are discovered.
- *SME Tip:* Most SMEs can handle basic updates (e.g., Windows Update or simple firmware push).

8.1.1.2 Default Secure Configuration

Question: "Do you ship your product with secure defaults (e.g., no default 'admin/admin' credentials)?"

- *Annex I* requirement: Requires products to limit attack surfaces by default.
- *SME Tip*: Even a small tweak (like forcing password change at first login) greatly reduces risk.

8.1.1.3 Vulnerability Disclosure Channel

Question: "Do you provide a simple channel (e.g., an email address or web form) for security researchers or users to report product vulnerabilities?"

- *Annex I* requirement: Section 2 on vulnerability handling processes.

- *SME Tip*: Setting up a dedicated email (like security@yourdomain.com) is quick and inexpensive.

8.1.1.4 Minimal Technical Documentation

Question: “Do you maintain any form of documentation (e.g., a simple Word doc) describing your product’s key features, known dependencies, and update procedures?”

- *Annex I* requirement: Transparent documentation is part of post-market obligations.
- *SME Tip*: Even a basic one-page “technical summary” helps track changes and prove due diligence.

8.1.2 Intermediate Security Measures

8.1.2.1 Access Control & Authentication Basics

Question: “Do you enforce some authentication methods (e.g., unique credentials, no shared admin logins) and encourage strong passwords or MFA?”

- *Annex I* requirement: Secure configuration & user authentication.
- *SME Tip*: Tools like built-in Windows policies or open-source MFA plugins can achieve this with minimal cost.

8.1.2.2 Secure Development Practices – At Least Minimal

Question: “When coding or configuring your product, do you follow a short list of secure coding/design guidelines (e.g., OWASP Top 10)?”

- *Annex I* requirement: Mandates secure design and development to reduce vulnerabilities.
- *SME Tip*: Start with a **checklist** for your dev team—no advanced training required initially.

8.1.2.3 SBOM (Software Bill of Materials) Lite

Question: “Do you keep a basic list of open-source and third-party components used in your product (including versions)?”

- *Annex I* requirement: Product transparency, vulnerability tracking.
- *SME Tip*: Even a simple spreadsheet with library names and versions can suffice at first.

8.1.2.4 Basic Security Incident Handling Process

Question: “If a vulnerability or incident occurs, do you know who in your team handles it, and how you inform affected users (if needed)?”

- *Annex I* requirement: Annex I, Section 2 - vulnerability handling and notification.
- *SME Tip*: A single-page “incident response outline” clarifies roles and actions.

8.1.3 Advanced Security Measures

8.1.3.1 Regular Vulnerability Scanning

Question: “Do you periodically scan your product or network endpoints (e.g., using free tools like OpenVAS, Nessus trial) for known vulnerabilities?”

- *Annex I* requirement: Ongoing vigilance for new threats.
- *SME Tip*: You can schedule scans monthly/quarterly, build the results into your patch cycle.

8.1.3.2 Penetration Testing or Third-Party Security Assessment

Question: “Have you ever engaged an external party or used a professional testing tool to probe for security weaknesses?”

- *Annex I* requirement: Helps demonstrate that your product meets essential cybersecurity requirements.
- *SME Tip*: This might be done once a year or on major releases; smaller budgets can focus on key features only.

8.1.3.3 Extended Support & Lifecycle Planning

Question: “Do you plan to provide security patches and support for a defined period (e.g., 2–5 years) after product release?”

- *Annex I* requirement: Post-market obligations to keep products secure over time.
- *SME Tip*: Clarify in product documentation or EULA how long you commit to supporting it.

8.1.4 Risk Assessments & Advanced Governance

8.1.4.1 Basic Risk Identification

Question: “Do you have any process (even if informal) to identify major threats (like data breaches, unauthorized access) and note how they’d impact your business or users?”

- *Annex I* requirement: Risk analysis is the foundation for deciding security measures.
- *SME Tip*: A simple table of “Threat | Likelihood | Impact | Mitigation” is a good start.

8.1.4.2 Formal Risk Assessment & Continuous Monitoring

Question: “Have you adopted a recognized risk assessment methodology (e.g., ISO/IEC 27005, NIST SP 800-30) to quantify and prioritize vulnerabilities?”

- *Annex I* requirement: The CRA references thorough risk management processes for product-level security.
- *SME Tip*: If budgets are tight, start with a free or simplified method (some official frameworks have templates).

8.1.4.3 Secure Supply Chain Management

Question: “Do you vet suppliers/third-party libraries for potential vulnerabilities, track their updates, and have an alternative plan if they become compromised?”

- *Annex I* requirement: The Act requires a comprehensive approach to supply chain security.
- *SME Tip*: Even small companies can ask suppliers basic security questions or track open-source vulnerabilities.

8.1.4.4 Full Documentation of Security & Compliance

Question: "Do you maintain a structured set of documents (risk registers, patch logs, design specs) to prove compliance and support potential audits?"

- *Annex I* requirement: Must demonstrate how you meet essential requirements.
- *SME Tip*: A well-organized folder or simple wiki page is enough if updated regularly.

8.1.5 Scoring & Outcomes

8.1.5.1 Mostly "Yes" answers (>10/15)

You're covering **basic** obligations for an SME. You **likely** meet minimal CRA Annex I requirements—though see advanced steps if your product is "Critical" or "Highly Critical."

8.1.5.2 Some "No/Partial" Answers (3-5)

Address these promptly; lacking basics (patching, secure defaults, simple vulnerability disclosure) can easily **violate** CRA essential requirements.

8.1.5.3 Multiple "No/Partial" Answers (>5)

For high-risk or complex products (especially "Important Products Class I/II" or Critical products), you may need to gradually **adopt** advanced risk assessments, supply chain checks, etc. Even if your product is classified as non-important and not critical, you can still plan these improvements over time.

8.1.5.4 Putting It All Together

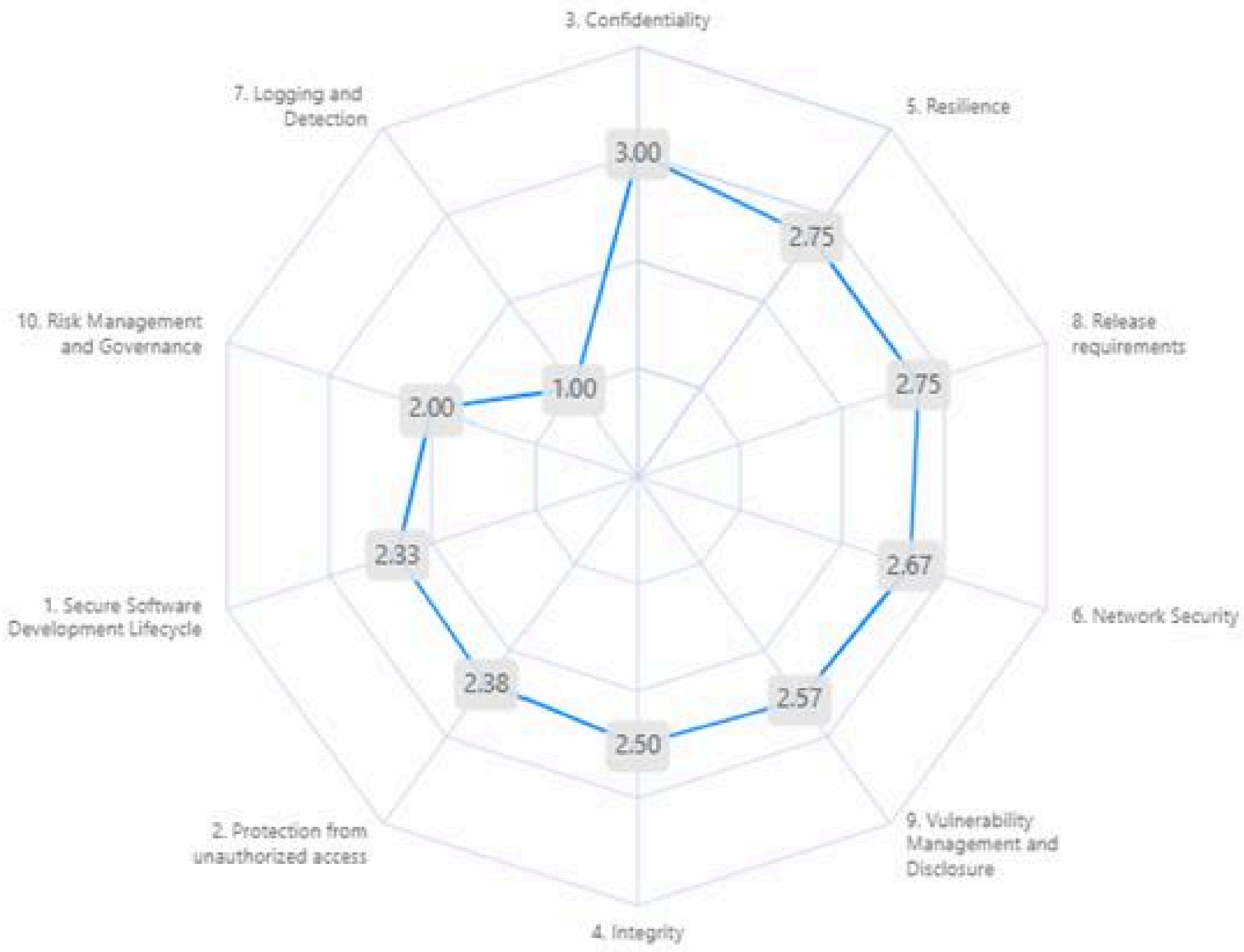
1. **Start with Easiest**: Confirm basic update processes, no insecure defaults, and that you have a way to fix/report vulnerabilities.
2. **Grow into Intermediate**: Enforce some authentication, keep a simple SBOM, handle incidents responsibly.
3. **Move to Advanced**: Conduct regular scanning/tests, define product lifecycle support, do basic risk identification.
4. **Finally**: For highly regulated or truly **important** products, implement **formal risk assessments**, secure supply chain, and robust documentation.

By **gradually** building up from **basic** patching and secure defaults to **comprehensive** risk assessments, SMEs can align with **CRA Annex I** without feeling overwhelmed. This tiered approach ensures **practical, incremental** cybersecurity improvements while fulfilling the **essential** and **vulnerability-handling** requirements the CRA mandates.

8.2 Sample detailed maturity assessment

OCCTET project aims at refining the “technical maturity assessment” providing a toolset. helping organizations identify their strengths and weaknesses.

Starting from the basic assessment highlighted above we gradually refine the questions producing a more detailed / refined assessment allowing us to pinpoint the areas of concern. Collecting assessments from multiple SMEs will allow us to produce advanced analytics, establish baselines, patterns, filtering and aggregating results based on activity sector, company size, main markets and more.



9 Third-party assessment

9.1 Technical Role of the Third-Party Assessment

A third-party assessment for Important products Class 2 or Class1 not following a harmonised standard involves a thorough evaluation of both the **product's architecture** and the **development processes** that underpin it. By verifying compliance with secure design principles, coding standards, and resilience measures, independent assessors help validate the product's defense against cyber-threats. Below are **key technical domains** that a third-party will scrutinize:

9.1.1 Secure Development Lifecycle (SDLC) Integration

- **Threat Modeling and Risk Assessment**
  Ensuring that the development team systematically identifies and mitigates potential threats during the design phase (e.g., using methodologies like STRIDE or PASTA).
- **Code Reviews and Static/Dynamic Analysis**
  Verifying that development processes incorporate automated scans (Static Application Security Testing, SAST) and manual reviews to detect common vulnerabilities (e.g., injection flaws, buffer overflows, and insecure API usage).

9.1.2 Secure Boot and Firmware Integrity

- **Cryptographic Integrity Checks**
  Confirming that each stage of the boot process validates the integrity and authenticity of the next stage (e.g., using signed bootloaders).
- **Firmware Update Mechanisms**
  Checking that over-the-air (OTA) or local firmware updates use secure channels (e.g., TLS) and require proper authentication to prevent unauthorized modifications.

9.1.3 Strong Authentication and Authorization

- **Robust Credential Management**
  Assessing password storage (hashed and salted), usage guidelines (complexity rules, rotation), and support for multi-factor authentication (MFA).
- **Role-Based Access Control (RBAC)**
  Verifying that access permissions adhere to the principle of least privilege, reducing the risk of unauthorized access.

9.1.4 Data Protection at Rest and in Transit

- **Encryption**
  Confirming the use of strong cryptographic algorithms (e.g., AES-256, RSA-2048) for data stored locally or transmitted over networks.
- **Key Management**
  Evaluating how cryptographic keys are generated, stored (e.g., in hardware security modules), and rotated to maintain confidentiality and integrity.

9.1.5 Network Security Measures

- **Firewall Configuration and Segmentation**
  Checking whether the product implements built-in firewalls or adheres to network segmentation best practices to isolate critical components.
- **Secure Protocols**
  Verifying that the product uses up-to-date secure protocols (e.g., TLS 1.3), rather than older, insecure versions like SSL or TLS 1.0.

9.1.6 Logging, Monitoring, and Incident Detection

- **Comprehensive Event Logging**
  Reviewing that critical system events (e.g., authentication attempts, configuration changes) are captured, timestamped, and stored in a secure, tamper-evident manner.
- **Automated Intrusion Detection/Prevention**
  Ensuring the product supports anomaly detection or integrates with an intrusion detection system (IDS) to flag suspicious activity in real-time.

9.1.7 Hardening and Configuration Management

- **Default Settings Review**
  Evaluating whether the product's default configurations are sufficiently hardened (e.g., disabling unnecessary services, ports, and protocols).
- **Secure Update Processes**
  Confirming that the product can be patched promptly and that it notifies administrators or users about critical security updates.

9.1.8 Vulnerability Management and Disclosure

- **Regular Scanning and Testing**
  Looking for evidence of scheduled vulnerability scans (e.g., using CVE-based tools) and periodic penetration testing.
- **Incident Response and Patch Deployment**
  Verifying there is a clear workflow for identifying, validating, and deploying patches—especially for critical vulnerabilities.

9.1.9 Supply Chain Security

- **Component Verification**
  Ensuring third-party libraries, modules, or frameworks meet recognized security standards and are tracked in a software bill of materials (SBOM).
- **Secure Procurement Processes**
  Reviewing how the organization vet suppliers and contractors, with evidence of contractual cybersecurity requirements and audits.

9.1.10 Product Maintenance and End-of-Life Planning

- **Lifecycle Documentation**
  Checking for a defined strategy on how long security updates will be provided and under what circumstances products are phased out.
- **Customer Guidance**
  Ensuring end-users or system administrators have access to secure deployment guides, best practices, and ongoing support.

Through **vulnerability and penetration testing**, the independent body assesses how well the product withstands active cyber-threat scenarios. Test results validate the **robustness of protective measures** and identify weaknesses that require remediation.

9.2 Strategic Role of the Third-Party Assessment

While technical checks form the backbone of the assessment, a holistic third-party review also examines broader governance and lifecycle processes.. The goal is to ensure that organizations not only implement robust security controls but also maintain them proactively.

9.2.1 Risk Management and Governance Evaluation

Beyond purely technical checks, the third-party assessment scrutinizes the organization's governance model for cybersecurity. This involves examining how **risk assessments** are conducted, documented, and updated; how **responsibilities** are assigned; and how **incident response and recovery plans** are maintained.

9.2.2 Supply Chain and Lifecycle Management Review

Assessors evaluate the organization's **supply chain security measures**, ensuring that components and software libraries are sourced from trusted vendors, properly vetted for vulnerabilities, and tracked through the development lifecycle. This extends to **updating and patching processes**, guaranteeing that known vulnerabilities are addressed swiftly and effectively.

9.2.3 Conformity with CRA Reporting and Transparency Obligations

As part of meeting the CRA requirements, organizations must establish **vulnerability disclosure policies** and **procedures** for notifying relevant authorities and customers about potential or confirmed security issues. Third-party assessors verify that these policies are in place and aligned with EU cybersecurity regulations, fostering a culture of transparency and accountability.

9.2.4 Continuous Improvement and Certification Maintenance

A third-party assessment is not just a **one-time exercise**. Strategic oversight includes verifying that the product owner has processes for **continuous monitoring**, **patching**, and **improvement**. This ongoing compliance helps maintain certification status over time, ensuring that products remain secure against evolving threats.

10 Conclusion

This deliverable consolidates a structured baseline of CRA-related requirements tailored to the specific operational realities of SMEs and the FOSS ecosystem. Through regulatory anchoring, stakeholder consultation, and expert validation, D2.1 translates legislative obligations into actionable compliance domains that can be operationalised within SME environments.

The findings confirm that while awareness of the Cyber Resilience Act is increasing, structured self-assessment, formalised vulnerability handling processes, documentation readiness, and lifecycle governance remain unevenly implemented across both SMEs and FOSS contributors. The recurring patterns identified through consultation underscore the need for practical, lightweight, and role-aware compliance tools that reduce interpretative ambiguity and lower the barrier to implementation.

Importantly, D2.1 represents the first phase of an iterative validation process. In alignment with the project lifecycle defined in the Description of Action, subsequent validation activities under WP4 will test the OCCTET toolkit with participating SMEs, enabling systematic data collection and refinement of requirement prioritisation and guidance materials. Dissemination and ecosystem engagement activities under WP5 will further support expanded SME participation and structured uptake This phased approach ensures that the compliance framework evolves based on cumulative evidence and real-world adoption dynamics.

By establishing a robust and regulation-aligned requirements foundation, D2.1 contributes directly to the overarching objective of OCCTET: to simplify CRA compliance for SMEs and FOSS communities while maintaining coherence with European cybersecurity policy objectives and market surveillance expectations.

11 ANNEXES

11.1 CRA Glossary and examples

The EU Cyber Resilience Act (CRA) is a landmark regulation aimed at strengthening cybersecurity and resilience of digital products and services across the European Union. With the increasing reliance on digital technologies, the CRA sets out essential requirements to ensure that products meet high standards of security and can withstand and recover from cyber threats.

This Glossary and Examples provides clear definitions of key terms and concepts within the CRA, along with real-world examples to illustrate how these terms apply in practice. This document is part of a broader effort to facilitate understanding and compliance with the CRA, supporting businesses, manufacturers, and regulators in meeting the Act's requirements.

Listed below are key concepts related to cybersecurity and compliance under the EU Cyber Resilience Act (CRA). They define essential principles for ensuring that digital products are secure and resilient against cyber threats. Here’s a brief explanation of each term:

- **Digital Product / Product with digital elements** – Any hardware or software product that is intended to be placed on the market in the EU and that incorporates or relies on digital elements (e.g., software, connectivity, data processing).
    - **Example**: A smart home device like a security camera that connects to the internet and processes video footage to alert users about potential intruders.
- **Remote Data Processing -** 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
    - **Example:** A web portal allowing customers to manage their home Wi-FI
- **Cybersecurity by Design** – The principle that cybersecurity measures must be incorporated into digital products and services from the very start of their design and development process.
    - **Example**: A company designing a new IoT device includes features such as secure authentication, encryption of data, and regular software updates from the outset, ensuring the product is resilient to cyber threats.
- **Cyber Incident** – Any event that compromises the confidentiality, integrity, or availability of a product or service’s data, systems, or networks.
    - **Example**: A hacker breaches the security of an e-commerce website, stealing customer payment details. This constitutes a cybersecurity incident that needs to be reported under the CRA.
- **“End-point”** - means any device that is connected to a network and serves as an entry point to that network,
- **“Software bill of materials”** - means a formal record containing details and chain relationships of components included in the software elements of a product with digital elements;

- **Resilience** – The ability of a digital product or service to maintain its functionality, even in the face of a cyber-attack or system failure, by responding to and recovering from such incidents effectively.
    - **Example**: A cloud service provider implements failover systems and data backups, ensuring that the service remains available even if one server is compromised.
- **Critical Infrastructure** – Systems and services that are vital to the functioning of the economy, society, or public safety, and that require high levels of cybersecurity protection.
    - **Example**: Energy grid management systems, water supply control systems, and healthcare databases that store sensitive patient information are considered critical infrastructure and require robust protection.
- **Vulnerability** – A flaw or weakness in a product's design, implementation, or maintenance that can be exploited by attackers to compromise the product or service.
    - **Example**: A software vulnerability that allows an attacker to bypass authentication protocols and gain unauthorized access to sensitive data.
- **Risk Management** – The process of identifying, assessing, and mitigating cybersecurity risks associated with a digital product or service.
    - **Example**: A company assesses the risk of a data breach in its mobile app by conducting regular security audits, identifying potential vulnerabilities, and patching them before they can be exploited.
- **Supply Chain Cybersecurity** – The practice of ensuring that all third-party vendors and suppliers involved in the production, development, or maintenance of a product or service meet the required cybersecurity standards.
    - **Example**: A tech company requires its software vendors to comply with industry cybersecurity standards before integrating their products into the company's system.
- **Incident Reporting** – The requirement for companies to report significant cybersecurity incidents that may affect the functioning of their digital products or services.
    - **Example**: A software company experiences a data breach where user information is compromised. According to the CRA, the company must report the breach to the relevant authorities and affected individuals within a specified timeframe.
- **Cyber Hygiene** – The regular practices and measures taken to ensure a high level of cybersecurity, such as keeping software up to date, applying patches, and using strong authentication methods.
    - **Example**: A company implements mandatory password changes every three months and ensures that all employees use multi-factor authentication to access the company's systems.
- **Market Surveillance Authority** – Regulatory bodies designated by EU member states to monitor and enforce compliance with the Cyber Resilience Act.

  - **Example**: In Germany, the Federal Office for Information Security (BSI) is responsible for ensuring that products placed on the market comply with the EU Cyber Resilience Act and other cybersecurity regulations.

- **Manufacturer's Obligation** – A manufacturer's responsibility under the CRA to ensure that their digital products meet specific cybersecurity standards before they are sold or distributed in the EU market.
  - **Example**: A company developing a new smartwatch must ensure that the device has secure communication protocols and can receive regular security updates throughout its lifecycle.

11.2 CRA ANNEX I: Essential cybersecurity requirements

11.2.1 Part I Cybersecurity requirements relating to the properties of products with digital elements

(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;

(a) 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;
(b) 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;
(c) 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;
(d) 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);
(e) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;
(f) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

(g) be designed, developed and produced to limit attack surfaces, including external interfaces;

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

(i) 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;

(j) 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.

11.2.2 Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

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.

11.3 CRA ANNEX II: Information and instructions to the user

ANNEX II ***INFORMATION AND INSTRUCTIONS TO THE USER***

At minimum, the product with digital elements shall be accompanied by:

1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted.

2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found.

3. name and type and any additional information enabling the unique identification of the product with digital elements.

4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties.

5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks.

6. where applicable, the internet address at which the EU declaration of conformity can be accessed;

7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;

8. detailed instructions or an internet address referring to such detailed instructions and information on:

(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;

(b) how changes to the product with digital elements can affect the security of data;

(c) how security-relevant updates can be installed;

(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;

(e) how the default setting enabling the automatic installation of security updates, as required, can be turned off;

(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in CRA Annex I and the documentation requirements set out in Annex VII.

9. If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed

11.4 CRA ANNEX III: Important Products with Digital Elements

OCCTET Note: At the time of writing, the Commission has prepared a draft to further define the categories of important and critical products with digital elements under Annexes III and IV of the Cyber Resilience Act. The aim is to provide more clarity on these categories, which *may be subject to stricter conformity assessments under Article 32. The draft can be consulted here:*

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements_en, and feedback is open until April 2025 via the provided template.

11.4.1 Important Products 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

11.4.2 Important Products 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

11.5 CRA ANNEX IV: Critical Products with Digital Elements

OCCTET Note: At the time of writing, the Commission has prepared a draft to further define the categories of important and critical products with digital elements under Annexes III and IV of the Cyber Resilience Act. The aim is to provide more clarity on these categories, which may be subject to stricter conformity assessments under Article 32. The draft can be consulted here:

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements_en , and feedback is open until April 2025 via the provided template.

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 and other devices for advanced security purposes, including for secure cryptoprocessing.

3. Smartcards or similar devices, including secure elements

11.6 CRA ANNEX V: EU Declaration of Conformity

The EU declaration of conformity, shall contain all of the following information:

1. Name and type and any additional information enabling the unique identification of the product with digital elements

2. Name and address of the manufacturer or its authorised representative

3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider

4. Object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate)

5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation

6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared

7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued

8. Additional information:

Signed for and on behalf of:

(place and date of issue):

(name, function) (signature):

11.7 CRA ANNEX VI: Simplified EU Declaration of conformity

The simplified EU declaration of conformity referred to in Article 13(20) shall be provided as follows:

Hereby, … *[name of manufacturer]* …. declares that the product with digital elements type … *[designation of type of product with digital element]* is in compliance with Regulation (EU) 2024/2847 (1).

The full text of the EU declaration of conformity is available at the following internet address: ….*[URI for the full declaration of conformity]*……..

11.8 CRA ANNEX VII: Content of the technical documentation

The technical documentation referred to in Article 31 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 CRA Annex I are applicable;

4. relevant information that was taken into account to determine the support period 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 Part I and Part 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.

11.9 CRA ANNEX VIII: Conformity Assessment Procedures

11.9.1 Part I Conformity assessment procedure based on internal control

1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2, 3 and 4 of this Part, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential cybersecurity requirements set out in Part I of Annex I and the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.

2. The manufacturer shall draw up the technical documentation described in Annex VII.

3. Design, development, production and vulnerability handling of products with digital elements

The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Parts I and II of Annex I.

4. Conformity marking and declaration of conformity

> 4.1 The manufacturer shall affix the CE marking to each individual product with digital elements that satisfies the applicable requirements set out in this Regulation.
>
> 4.2 The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 28 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

5. Authorised representatives

The manufacturer's obligations set out in point 4 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

11.9.2 Part II EU-type examination (based on module B)

1. 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.

2. 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, and the examination of specimens of one or more critical parts of the product (combination of production type and design type).

3. The manufacturer shall lodge an application for EU-type examination with a single notified body of its choice.

The application shall include:

3.1 the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;

3.2 a written declaration that the same application has not been lodged with any other notified body;

3.3 the technical documentation, which shall make it possible to assess the conformity of the product with digital elements with the applicable essential cybersecurity requirements as set out in Part I of Annex I and the manufacturer's vulnerability handling processes set out in Part II of Annex I and shall include an adequate analysis and assessment of the risks. The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product with digital elements. The technical documentation shall contain, wherever applicable, at least the elements set out in CRA Annex VII;

3.4 the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on its behalf and under its responsibility.

4. The notified body shall:

4.1 examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I;

4.2 verify that specimens have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;

4.3 carry out appropriate examinations and tests, or have them carried out, to check that, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards or technical specifications for the requirements set out in Annex I, they have been applied correctly;

4.4 carry out appropriate examinations and tests, or have them carried out, to check that, where the solutions in the relevant harmonised standards or technical specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential cybersecurity requirements;

4.5 agree with the manufacturer on a location where the examinations and tests will be carried out.

5. The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.

6. Where the type and the vulnerability handling processes meet the essential cybersecurity requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes. The certificate may have one or more annexes attached.

The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with digital elements with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control.

Where the type and the vulnerability handling processes do not satisfy the applicable essential cybersecurity requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.

7. The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential cybersecurity requirements set out in Annex I, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.

The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential cybersecurity requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.

8. The notified body shall carry out periodic audits to ensure that the vulnerability handling processes as set out in Part II of Annex I are implemented adequately.

9. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and any additions thereto refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and additions thereto which it has issued.

The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and any additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.

10. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for **10 years** after the product with digital elements has been placed on the market or for the support period, whichever is longer.

11. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 10, provided that the relevant obligations are specified in the mandate.

11.9.3 Part III Conformity of type based on internal production control (module C)

1. 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.

2. Production

The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products with digital elements with the approved type described in the EU-type examination certificate and with the essential cybersecurity requirements as set out in Part I of Annex I and ensures that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.

3. Conformity marking and declaration of conformity

3.1 The manufacturer shall affix the CE marking to each individual product with digital elements that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements set out in this Regulation.

3.2 The manufacturer shall draw up a written 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 elements has been placed on the market or for the support period, whichever is longer. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

4. Authorised representative

The manufacturer's obligations set out in point 3 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

11.9.4 Part IV: Conformity based on full quality assurance (module H)

1. 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.

2. Design, development, production and vulnerability handling of products with digital elements

The manufacturer shall operate an approved quality system as specified in point 3 for the design, development and final product inspection and testing of the products with digital elements concerned and for handling vulnerabilities, maintain its effectiveness throughout the support period, and shall be subject to surveillance as specified in point 4.

3. Quality system

3.1 The manufacturer shall lodge an application for assessment of its quality system with the notified body of its choice, for the products with digital elements concerned.

The application shall include:

(a) the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;

(b) the technical documentation for one model of each category of products with digital elements intended to be manufactured or developed. The technical documentation shall, wherever applicable, contain at least the elements as set out in CRA Annex VII;

(c) the documentation concerning the quality system; and

(d) a written declaration that the same application has not been lodged with any other notified body.

3.2 The quality system shall ensure compliance of the products with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Part II of Annex I.

All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.

It shall, in particular, contain an adequate description of:

(a) the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;

(b) the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part I of Annex I that apply to the products with digital elements will be met;

(c) the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part II of Annex I that apply to the manufacturer will be met;
(d) the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products with digital elements pertaining to the product category covered;

(e) the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;

(f) the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;

(g) the quality records, such as inspection reports and test data, calibration data and qualification reports on the personnel concerned;

(h) the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.

3.3 The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2.

It shall presume conformity with those requirements in respect of the elements of the quality system that comply with the corresponding specifications of the national standard that implements the relevant harmonised standard or technical specification.

In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and shall have knowledge of the applicable requirements set out in this Regulation. The audit shall include an assessment visit to the manufacturer’s premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1 (b), to verify the manufacturer’s ability to identify the applicable requirements set out in this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with digital elements with those requirements.

The manufacturer or its authorised representative shall be notified of the decision.

The notification shall contain the conclusions of the audit and the reasoned assessment decision.

3.4 The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.

3.5 The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system.

The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.

It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.

4. Surveillance under the responsibility of the notified body

4.1 The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.

4.2 The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:

(a) the quality system documentation;

(b) the quality records as provided for by the design part of the quality system, such as results of analyses, calculations and tests;

(c) the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data and qualification reports on the personnel concerned.

4.3 The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.

5. Conformity marking and declaration of conformity

5.1 The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product with digital elements that satisfies the requirements set out in Part I of Annex I.

5.2 The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The declaration of conformity shall identify the product model for which it has been drawn up.

A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

6. The manufacturer shall, for a period ending at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, keep at the disposal of the national authorities:

(a) the technical documentation referred to in point 3.1;

(b) the documentation concerning the quality system referred to in point 3.1;

(c) the change referred to in point 3.5, as approved;

(d) the decisions and reports of the notified body referred to in points 3.5 and 4.3.

7. Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.

8. Authorised representative

The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

A statement has been made with regard to this act and can be found in OJ C, 2024/6786, 20.11.2024, ELI: http://data. europa.eu/eli/C/2024/6786/oj.

11.10 ANNEX IX requirements detailed

11.10.1 Manufacturers of Non-Important Devices

In the context of the Cyber Resilience Act (CRA), manufacturers of non-important devices face regulatory expectations scaled appropriately to the comparatively lower cybersecurity risks associated with their products. Despite their classification as non-critical, ensuring compliance remains essential to maintain consumer trust, avoid market exclusion, and minimize cybersecurity threats. This section provides structured guidance tailored specifically for SMEs manufacturing such products, outlining clear, achievable compliance requirements and self-assessment procedures. It aims to facilitate compliance by detailing actionable guidelines, thus ensuring that even products deemed non-critical uphold fundamental cybersecurity standards, protecting consumers and maintaining market integrity.

Cybersecurity risk assessment

To ensure compliance with the Cyber Resilience Act (CRA), manufacturers of non-important devices must implement cybersecurity risk assessment measures tailored to their products. While these devices may not fall under the critical or important categories, they still require structured risk management to prevent vulnerabilities that could compromise user security or operational integrity. A proactive approach to cybersecurity helps manufacturers mitigate potential threats throughout the product lifecycle, from development to maintenance. The following section outlines the key cybersecurity risk assessment requirements applicable to non-important device manufacturers, providing guidance on documentation, implementation, and compliance with CRA standards.

The following table presents the cybersecurity risk assessment requirements for manufacturers of non-important devices:

ID	Requirement	Reference	Comment	Check
1	Manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.	article 13(2)	self-written - to be reviewed by notified body for critical and important products	- Verify that a comprehensive cybersecurity risk assessment has been conducted for each digital product. - Ensure that the outcomes of the risk assessment are integrated into all phases of the product life cycle, including planning, design, development, production, delivery, and maintenance. - Confirm that the risk assessment effectively identifies and mitigates risks to user health and safety arising from cybersecurity incidents.

2	The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements	Article 13(3)	self-written - to be reviewed by notified body for critical and important products	- Ensure that the cybersecurity risk assessment is thoroughly documented and stored in accordance with Annex I, Part I - Verify that the documented risk assessment is regularly updated during the support period as determined by paragraph 8 of the CRA. - Confirm that the risk assessment includes analyses based on the product's intended purpose, foreseeable use, operational environment, protected assets, and expected lifespan. - Ensure that the documentation indicates the applicability and implementation status of security requirements from Annex I and vulnerability handling requirements from Part II of Annex I.

	are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.			
3	When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment in the technical documentation. For products with digital elements which are also subject to other Union legal acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation.	Article 13(4)	self-written - to be reviewed by notified body for critical and important products	- Verify that the cybersecurity risk assessment is included in the technical documentation provided when placing the product on the market. - Ensure that if the product is subject to other Union legal acts, the cybersecurity risk assessment complies with those additional requirements. - Confirm that any non-applicable essential cybersecurity requirements are clearly justified within the technical documentation.

4	The manufacturers shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products	Article 13(7)	self-written - to be reviewed by notified body for critical and important products	- Ensure that all relevant cybersecurity aspects, including known vulnerabilities and third-party information, are systematically documented. - Verify that the cybersecurity risk assessment is updated in response to new vulnerabilities or changes in third-party information. - Confirm that the documentation process is proportionate to the nature and risks associated with the digital product.

General requirements

The Cyber Resilience Act (CRA) establishes fundamental cybersecurity requirements for products with digital elements to enhance their security throughout their lifecycle. These general requirements ensure that manufacturers incorporate cybersecurity best practices from the initial design phase through production and deployment. By adhering to these principles, manufacturers can proactively address vulnerabilities, mitigate risks, and ensure compliance with regulatory expectations. The following section outlines the essential general requirements that manufacturers must meet under the CRA to ensure an appropriate level of cybersecurity for their products.

ID	Requirement	Reference	Comment	Check

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.	Annex I, Part 1 §1	Self-assessment	- Verify that the product's design documentation includes detailed descriptions of cybersecurity measures implemented. - Assess whether comprehensive risk assessments have been performed during the design and development phases. - Confirm that identified risks have been mitigated through appropriate security controls and design choices. - Evaluate adherence to recognized cybersecurity frameworks and standards (e.g., ISO/IEC 27001) during the development process. - Implement static and dynamic application security testing (SAST/DAST) tools to detect potential security flaws early in the development cycle. - Confirm that a secure development lifecycle (SDLC) is integrated into the production process, encompassing phases such as design, development, testing, deployment, and maintenance.
2	On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:	Annex I, Part 1 §2	-	
3	(a) be made available on the market without known exploitable vulnerabilities;	Annex I, Part 1 §2a	Self-assessment	- Execute automated vulnerability scanning tools to identify known exploitable vulnerabilities within the product.

				- Ensure that scans cover all components, including third-party libraries and dependencies. - Validate that penetration tests are performed regularly and after significant code changes or updates. - Evaluate the security posture of all third-party components and libraries integrated into the product. - Ensure that third-party vulnerabilities are identified, assessed, and remediated in a timely manner.

4	(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;	Annex I, Part 1 §2b	Self-assessment	- Examine the product's default settings to ensure they prioritize security, minimizing potential attack vectors. - Confirm that unnecessary services and ports are disabled by default to reduce the product's attack surface. - Test the product's ability to reset to its original secure state, ensuring that all configurations revert to secure defaults upon reset. - Validate that the reset mechanism is reliable and user-friendly. - Assess the effectiveness of access controls surrounding configuration settings to prevent unauthorized modifications. - Ensure that changes to default configurations require appropriate authentication and authorization. - Review user guides and documentation to ensure that instructions for maintaining secure configurations are clear and comprehensive.
5	(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	Annex 1, Part 1 §2c	Self-assessment	- Evaluate the mechanisms in place for delivering security updates, ensuring they are effective and reliable. - Confirm the availability of automatic security updates that install within an appropriate timeframe by default. - Test the notification systems that inform users about available security updates.

	notification of available updates to users, and the option to temporarily postpone them;			- Ensure that notifications are clear, timely, and provide sufficient information for users to understand the update's importance. - Verify the presence of easy-to-use opt-out mechanisms allowing users to disable automatic updates if desired. - Assess the functionality that permits users to temporarily postpone security updates, ensuring it does not compromise overall security. - Review the policies governing the deployment of security patches to ensure vulnerabilities are addressed without undue delay. - Ensure that all security updates undergo rigorous testing before deployment to prevent the introduction of new vulnerabilities.
6	(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;	Annex I, Part 1 §2d	Self-assessment	- Ensure MFA is implemented and functioning correctly for all access points. - Verify that strong password policies (e.g., complexity, expiration) are enforced. - Confirm that user roles are appropriately defined and enforced. - Ensure users have the minimum level of access necessary for their roles.

7	(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;	Annex I, Part 1 §2e	Self-assessment	- Confirm that all sensitive data stored is encrypted using industry-standard algorithms (e.g., AES-256). - Ensure that data transmitted over networks is encrypted using protocols such as TLS 1.3. - Validate that only authorized personnel can access confidential data. - Verify the use of secure protocols for all data communications. - Ensure that sensitive data elements are masked or tokenized where applicable. - Perform periodic audits to identify and remediate vulnerabilities that could compromise data confidentiality.
8	(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;	Annex I, Part 1 §2f	Self-assessment	- Implement and test checksum or hash functions to detect unauthorized data modifications. - Ensure that digital signatures are used to verify the authenticity and integrity of data. - Confirm that only authorized users can modify critical data, commands, programs, and configurations. - Verify that logs cannot be altered or deleted without proper authorization.

				- Ensure that there are established procedures for reporting and responding to data corruption incidents. - Verify that procedures for handling integrity-related vulnerabilities are documented and effectively implemented.
9	(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);	Annex I, Part 1 §2g	Self-assessment	- Review data collection processes to ensure only necessary data for the product's intended purpose is collected. - Verify that the purpose for data collection is clearly defined and adhered to. - Ensure that data is not retained longer than necessary for its intended purpose. - Implement and test automated mechanisms for deleting data that is no longer needed. - Monitor who accesses data and for what purposes to ensure compliance with data minimization principles. - Ensure that personally identifiable information (PII) is anonymized where possible. - Test pseudonymization methods to protect data while retaining usability for analysis. - Ensure data minimization practices comply with GDPR and other relevant data protection regulations.

				- Verify that users provide informed consent for data collection and processing.
10	(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	Annex I, Part 1 §2h	Self-assessment	- Test failover systems to ensure continuity of essential functions during incidents. - Conduct simulated DoS attacks to assess the system's resilience and mitigation capabilities. - Ensure that critical components have redundancy to prevent single points of failure. - Ensure timely application of security patches to address vulnerabilities that could impact availability.
11	(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	Annex I, Part 1 §2i	Self-assessment	- Verify that the product does not excessively consume network or device resources, ensuring it does not degrade the performance or availability of connected services. - Ensure the product operates independently without causing cascading failures in connected systems.
12	(j) be designed, developed and produced to limit attack surfaces, including external interfaces;	Annex I, Part 1 §2j	Self-assessment	- Identify and evaluate potential vulnerabilities in all external interfaces (e.g., APIs, ports, network connections). - Ensure that only necessary external interfaces are enabled and properly secured.
13	(k) be designed, developed and produced to reduce the impact of	Annex I, Part 1 §2k	Self-assessment	- Validate the effectiveness of incident detection and response mechanisms in mitigating the impact of security breaches.

	an incident using appropriate exploitation mitigation mechanisms and techniques;			- Ensure the product can maintain essential functions and recover quickly from incidents.
14	(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;	Annex I, Part 1 §2l	Self-assessm ent	- Ensure that the product accurately records and monitors relevant internal activities, including data access and modifications. - Validate that users can effectively opt out of security-related information recording and monitoring without compromising overall security.
15	(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.	Annex I, Part 1 §2m	Self-assessm ent	- Confirm that users can permanently delete all personal and configuration data from the product. - Ensure that data transfer between products or systems is conducted securely, maintaining confidentiality and integrity.
16	Manufacturers of products with digital elements shall:	Annex I - Part II	-	
17	(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	Annex I, Part 2 §2	Self-assessm ent	- Ensure the creation and maintenance of a comprehensive SBOM in a standardized, machine-readable format (e.g., SPDX, CycloneDX) that encompasses at least the top-level dependencies of the product. - Confirm that all identified vulnerabilities and components are systematically documented, including detailed descriptions,

	at the very least the top-level dependencies of the products;			affected components, and remediation statuses.
18	(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;	Annex I, Part 2 §1	Self-assessment	- Verify that identified vulnerabilities are addressed and remediated promptly in accordance with their associated risk levels, ensuring the provision of security updates without undue delays. - Ensure that, when technically feasible, security updates are delivered independently from functionality updates to minimize the risk of introducing new vulnerabilities.
19	(3) apply effective and regular tests and reviews of the security of the product with digital elements;	Annex I, Part 2 §3	Self-assessment	- Ensure that regular and effective security tests are conducted to proactively identify and mitigate potential vulnerabilities within the product. - Validate that security reviews are thoroughly documented, capturing findings, remedial actions, and verification of remediation efforts.
20	(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	Annex I, Part 2 §4	Self-assessment	- Confirm that once a security update is available, comprehensive information about fixed vulnerabilities is shared and publicly disclosed, including descriptions, affected products, impacts, severity, and remediation steps. - Ensure that in scenarios where immediate public disclosure could pose security risks, the manufacturer appropriately delays information release until users have the opportunity to apply necessary patches.

	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;			
21	(5) put in place and enforce a policy on coordinated vulnerability disclosure;	Annex I, Part 2 §5	Self-assessment	- Verify the existence of a formally documented vulnerability disclosure policy. - Ensure the policy outlines roles and responsibilities, reporting channels, and timelines for response. - Check that the policy is publicly accessible to all stakeholders, including users and third-party researchers.
22	(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	Annex I, Part 2 §6	Self-assessment	- Verify the provision of a dedicated contact address (e.g., email, web form) for vulnerability reporting on official platforms. - Assess the channels used for sharing vulnerability information with third parties and stakeholders. - Confirm the use of secure communication protocols to protect

	the reporting of the vulnerabilities discovered in the product with digital elements;			sensitive information during sharing. - Identify and document all third-party components within the product.
23	(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;	Annex I, Part 2 §7	Self-assessment	- Evaluate the security of the distribution channels used for delivering updates (e.g., HTTPS protocols, digital signatures). - Ensure that updates are hosted on trusted and secure servers to prevent tampering. - Measure the interval between vulnerability identification and the deployment of corresponding updates. - Confirm that updates include integrity checks (e.g., checksums, cryptographic signatures) to verify authenticity.
24	(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	Annex I, Part 2 §8	Self-assessment	- Confirm that security updates are made available immediately upon their release. - Verify that security updates are provided free of charge unless an alternative agreement exists for tailor-made products. - Review the content of advisory messages to ensure they include comprehensive information about the vulnerability, affected products, severity, and remediation steps. - Ensure that advisory messages provide clear instructions on actions users should take to apply updates or mitigate

	action to be taken.			vulnerabilities.

Information and instruction to the users

Ensuring transparency and accessibility of cybersecurity-related information is a key requirement under the Cyber Resilience Act (CRA). Manufacturers of products with digital elements must provide users with essential details, including company identification, contact information, and reporting channels for vulnerabilities. Clear and accurate documentation helps users verify product authenticity, contact the manufacturer for support, and report security concerns efficiently. The following section outlines the necessary information that must accompany a product with digital elements, ensuring compliance with CRA standards while enhancing user trust and security.

ID	Requirement	Reference	Comment	Check
1	At minimum, the product with digital elements shall be accompanied by:	Annex II	-	
2	1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;	Annex II, §1	self-written	- Confirm that the product packaging and accompanying documentation clearly display the manufacturer's name, registered trade name or trademark, and a valid postal address. This includes cross-referencing the provided information with official trademark and business registries to ensure accuracy and authenticity. - Test the provided email address and digital contact methods to ensure they are operational and responsive. Additionally, verify that the manufacturer's website (if available) is accessible, regularly maintained, and provides up-to-date contact information, facilitating effective communication channels for users.

3	2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer’s policy on coordinated vulnerability disclosure can be found;	Annex II, §2	self-written	- Ensure that the designated single point of contact for reporting vulnerabilities is prominently listed in the product documentation and is easily accessible to users. This includes verifying that the contact method (e.g., dedicated email address or web portal) is functional and that submissions are acknowledged within an appropriate timeframe. - Review the manufacturer's policy on coordinated vulnerability disclosure to confirm its presence, clarity, and comprehensiveness. The policy should be readily accessible, detailing procedures for reporting vulnerabilities, the manufacturer's responsibilities, expected timelines for responses, and guidelines for responsible disclosure practices.
4	3. name and type and any additional information enabling the unique identification of the product with digital elements;	Annex II, §3	self-written	- Check that the product is clearly labeled with its specific name and type, and include unique identifiers such as model numbers, serial numbers, or other distinguishing features. This facilitates unambiguous identification and differentiation from other products in the market. - Verify that the unique identification information is consistently presented across all platforms, including physical packaging, digital documentation, online listings, and regulatory filings. Consistency ensures that users can reliably reference and access product-specific information when needed.
5	4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product’s essential functionalities and information	Annex II, §4	self-written	- Assess whether the product documentation clearly outlines the intended purpose and primary functionalities of the product. This includes evaluating whether the descriptions accurately reflect the product's capabilities and are free from ambiguities that could lead to misuse. - Examine the detailed information provided about the product’s security properties and the security environment established by the manufacturer.

	about the security properties;			This involves verifying that security measures, such as encryption standards, authentication mechanisms, and data protection protocols, are described and align with industry best practices.
6	5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	Annex II, §5	self-written	- Review the product information to identify any listed or potential cybersecurity risks associated with both intended use and reasonably foreseeable misuse. This includes evaluating whether the risks are comprehensively documented and accompanied by clear descriptions of their implications. - Ensure that the product documentation includes detailed instructions or references for mitigating identified cybersecurity risks.
7	6. where applicable, the internet address at which the EU declaration of conformity can be accessed;	Annex II, §6	self-written	- verifying that product packaging and accompanying documentation include a clear and functional internet address where users can access the EU Declaration of Conformity. - To confirm that the provided internet address is not only present but also active, directs users correctly to the EU Declaration of Conformity, and remains accessible over time, thereby maintaining continuous compliance.
8	7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;	Annex VI, §7	self-written	- Ensure that the end-date of the technical security support period is clearly stated in the product documentation, allowing users to plan for ongoing security needs and understand the timeline for receiving updates and support. - Verify that product documentation comprehensively outlines the types of technical security support provided by the manufacturer, including the

				available support channels, thereby enabling users to effectively address cybersecurity concerns.
9	8. detailed instructions or an internet address referring to such detailed instructions and information on:	Annex II, §8	self-written	
10	(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;	Annex II, §8 (a)	self-written	- Ensure that the detailed instructions for initial commissioning encompass essential security configurations to establish a secure foundation for the product from the outset, - Validate that the provided instructions offer exhaustive guidelines for maintaining security throughout the product's operational lifetime
11	(b) how changes to the product with digital elements can affect the security of data;	Annex II, §8 (b)	self-written	- Evaluate the instructions' guidance on how modifications to the product may influence data security, ensuring that changes do not introduce new vulnerabilities - Ensure that the instructions incorporate measures to uphold data security continuity when product changes occur,
12	(c) how security-relevant updates can be installed;	Annex II, §8 (c)	self-written	- Confirm that the instructions provide clear and effective procedures for installing security-relevant updates - Assess the effectiveness of automated update mechanisms as described in the instructions, ensuring timely and secure application of updates

13	(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;	Annex II, §8 (d)	self-written	- Ensure that the instructions delineate clear and secure methods for permanently removing user data during decommissioning - Verify that the instructions outline comprehensive steps for the secure decommissioning of the product, mitigating the risk of data breaches during the process
14	(e) how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of Annex I, can be turned off;	Annex II, §8 (e)	self-written	- Verify that the instructions provide a secure, user-friendly method for disabling the default setting that enables automatic security updates - Ensure that the instructions include appropriate warnings and guidance for users who choose to disable automatic security updates, maintaining overall security integrity.
15	(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII.	Annex II, §8 (f)	self-written	- Ensure that comprehensive information necessary for integrators to comply with the essential cybersecurity requirements-
16	9. If the manufacturer decides to make available the software bill of materials to the user, information on where the	Annex II, §9	Not mandatory	- Ensure that when manufacturers choose to make the Software Bill of Materials (SBOM) available to users, comprehensive information on how to access the SBOM is clearly provided.

	software bill of materials can be accessed.			-
17	The user information and instructions as set out in Annex II (detailed above), shall be included in the Technical Documentation.	Annex VII, §1 (d)	-	

EU declaration of conformity

The EU Declaration of Conformity is a mandatory document that certifies a product's compliance with relevant European Union (EU) regulations. This declaration ensures that products with digital elements meet essential safety, security, and performance standards before being placed on the EU market. It must contain specific information, such as product identification details, and compliance references, to facilitate regulatory checks and consumer trust. The following section outlines the key requirements for the EU Declaration of Conformity, ensuring transparency and adherence to the CRA's provisions.

ID	Requirement	Reference	Comment	Check
1	The EU declaration of conformity referred to in Article 28, shall contain all of the following information:	Annex V	The EU Declaration of conformity is self-written	
2	(1) Name and type and any additional information enabling the unique identification of the product with digital elements	Annex V, §1	-	- Ensure that the product's name, type, and any additional identifying information (e.g., model number, serial number) are accurately listed in the EU Declaration of Conformity. - Confirm that unique identifiers (such as serial numbers or batch codes)

				included in the declaration facilitate the unambiguous identification of the product.
3	(2) Name and address of the manufacturer or its authorised representative	Annex V, §2	-	- Verify that the manufacturer’s name, official trade name or trademark, and complete postal address are correctly stated in the declaration. - Ensure that if an authorized representative is listed, their information is accurate and up-to-date.
4	(3) A statement that the EU declaration of conformity is issued under the sole responsibility of the provider	Annex V, §3	-	- Confirm that the declaration includes a clear statement asserting that it is issued under the sole responsibility of the provider. - Ensure that the responsibility statement aligns with legal requirements and certification standards.
5	(4) Object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate)	Annex V, §4	-	- Ensure that the declaration includes sufficient information (e.g., product ID, version) to allow for the traceability of the product. - Confirm that a photograph of the product is included when appropriate, aiding in visual identification and verification.
6	(5) A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation	Annex V, §5	-	- Verify that the declaration explicitly states that the product conforms with all relevant Union harmonisation legislation. - Ensure that the conformity statement is supported by appropriate evidence, such as test reports or certifications.
7	(6) References to any relevant harmonised standards used or any other common	Annex V, §6	if applicable	- Confirm that all referenced harmonised standards, common specifications, or cybersecurity certifications are correctly cited in the declaration.

	specification or cybersecurity certification in relation to which conformity is declared			- Ensure that the referenced standards and certifications are relevant to the product's intended use and functionalities.
8	(7) Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued	Annex V, §7	if applicable	- Ensure that the declaration includes the correct name and identification number of the notified body involved in the conformity assessment. - Verify that the declaration describes the conformity assessment procedures performed by the notified body.
9	(8) Additional information: Signed for and on behalf of: (place and date of issue): (name, function) (signature):	Annex V, §8	-	- Ensure that the declaration is signed by an authorized representative of the manufacturer, including their name and function. - Confirm that the declaration includes the accurate place and date of issue, ensuring temporal and geographical validity.
10	SIMPLIFIED EU DECLARATION OF CONFORMITY	Annex VI	Only for SMEs and micro-enterprises	
11	The simplified EU declaration of conformity referred to shall be provided as follows: Hereby, ... [name of manufacturer] declares that the product with digital elements type ... [designation of type of product with digital element] is in	Annex VI	self-written	

	compliance with Regulation (EU) 2024/...+ . The full text of the EU declaration of conformity is available at the following internet address: ...			
12	The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 28 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.	Annex VIII, Part I, §4.2	-	- Ensure that manufacturers maintain the EU Declaration of Conformity appropriately alongside technical documentation for the mandated retention period - Verify that manufacturers can promptly provide a copy of the EU Declaration of Conformity to national authorities upon request, as required by Article 28.9.

Technical documentation

The technical documentation must provide comprehensive details of the product's intended purpose, relevant software versions in the context of cybersecurity compliance, hardware architecture descriptions, and clear processes for vulnerability handling. It must also include a Software Bill of Materials (SBOM) covering at least the product's top-level dependencies. Additionally, manufacturers must systematically document their approach to managing cybersecurity vulnerabilities throughout the product lifecycle, including maintaining test reports and outlining production, monitoring, and lifecycle validation activities suitable for the product’s risk profile.

ID	Requirement	Reference	Comment	Check
1	The technical documentation shall contain at least the following information, as applicable to the relevant product with digital elements:	Annex VII	-	
2	1. a general description of the product with digital elements, including:	Annex VII, §1	self-written	
3	(a) its intended purpose;	Annex VII, §1 (a)	self-written	- Verify that the documentation clearly states the primary function and intended use cases of the product. - Ensure the description aligns with the product’s marketing materials and user manuals.
4	(b) versions of software affecting compliance with essential cybersecurity requirements;	Annex VII, §1 (b)	self-written	- Ensure that all relevant software versions are explicitly mentioned. - Verify that version numbering follows a consistent and clear schema.

5	(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;	Annex VII, §1 (c)	self-written	- Check for high-resolution photographs or detailed illustrations showcasing all external components and interfaces. - Ensure that labels, ports, and indicators are clearly marked and described.
6	(d) user information and instructions as set out in Annex II;	Annex VII, §1 (d)	self-written	- Verify that the user manual includes all sections outlined in Annex II, such as installation, configuration, operation, and troubleshooting.
7	2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:	Annex VII, §2	self-written	
8	(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;	Annex VII, §2 (a)	self-written	- Ensure that the technical documentation encompasses exhaustive drawings and schematics that accurately delineate the system architecture of the digital product. - Verify that the documentation explicitly explains the integration points and dependencies among various software components within the digital product.
9	(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	Annex VII, §2 (b)	self-written	- Confirm that the Software Bill of Materials (SBOM) is provided in a standardized, machine-readable format and encompasses at least the top-level dependencies of the digital product. - Ensure the establishment of a robust coordinated vulnerability disclosure policy, including a designated contact address for

	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;			reporting vulnerabilities.
10	(c) necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;	Annex VII, §2 (c)	self-written	- Verify that the technical documentation furnishes comprehensive information on the production processes, encompassing quality assurance and security measures. - Ensure that the technical documentation includes specifications for monitoring processes designed to validate the product's functionality and security throughout its lifecycle.
11	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;	Annex VII, §3	self-written	- Ensure that the technical documentation encompasses a thorough assessment of cybersecurity risks associated with the product throughout its lifecycle
12	4. relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements;	Annex VII, §4	self-written	- Ensure that the technical documentation incorporates relevant information and criteria utilized to determine the support period for the product

13	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;	Annex VII, §5	self-written	- Ensure that the technical documentation includes a comprehensive list of harmonised standards applied to the product, complete with their official references as published in the Official Journal of the European Union.
14	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	Annex VII, §6	if applicable	- Ensure that the technical documentation includes detailed reports of tests conducted to verify the product's conformity with essential cybersecurity requirements

	essential cybersecurity requirements as set out in Parts I and II of Annex I;			- Verify that the documentation contains detailed reports on the vulnerability handling processes
15	7. a copy of the EU declaration of conformity;	Annex VII, §7	self-written	- Ensure that a complete and accurate copy of the EU Declaration of Conformity is included in the technical documentation
16	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.	Annex VII, §8	if applicable	- Ensure that the technical documentation specifies where users can access the Software Bill of Materials (SBOM) when it is made available - Verify that the manufacturer can provide the SBOM upon a reasoned request from a market surveillance authority

Reporting Requirements

Manufacturers of products with digital elements under the CRA have a legal obligation to report cybersecurity vulnerabilities, especially those that are actively exploited. Timely and transparent reporting is critical for mitigating potential risks, preventing further exploitation, and ensuring coordinated incident response across the EU. Manufacturers must notify the Computer Security Incident Response Team (CSIRT) and ENISA, using the designated reporting platform, within strict timeframes. The following section outlines the specific reporting requirements, including mandatory notification timelines and procedural obligations, to ensure compliance with the CRA and maintain the security of digital products.

ID	Requirement	Reference	Comment	Check
1	A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to	Article 14(1) and 14(7)	Mandatory Reporting	

	the CSIRT designated as coordinator and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.			
2	For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:	Article 14 (2)	Mandatory Reporting	
3	(a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;	Article 14 (2) (a)	Mandatory Reporting	
4	(b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature	Article 14 (2) (b)	Mandatory Reporting	

	of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;			
5	(c) unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available, including at least the following:	Article 14 (2) (c)	Mandatory Reporting	
6	(i) a description of the vulnerability, including its severity and impact;	Article 14 (2) (c) (i)	Mandatory Reporting	
7	(ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;	Article 14 (2) (c) (ii)	Mandatory Reporting	
8	(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.	Article 14 (2) (c) (iII)	Mandatory Reporting	
9	A manufacturer shall notify any severe incident having an impact on the security of the product with digital	Article 14 (3)	Single platform is not yet	

	elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform		established (Dec 2024)	
10	For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit:	Article 14 (4)	Mandatory Reporting	
11	(a) an early warning notification of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;	Article 14 (4) (a)	Mandatory Reporting	

12	(b) unless the relevant information has already been provided, an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;	Article 14 (4) (b)	Mandatory Reporting	
13	(c) unless the relevant information has already been provided, a final report, within one month after the submission of the incident notification under point (b), including at least the following:	Article 14 (4) (c)	Mandatory Reporting	
14	(i) a detailed description of the incident, including its severity and impact;	Article 14 (4) (c) (i)	Mandatory Reporting	
15	(ii) the type of threat or root cause that is likely to have triggered the incident;	Article 14 (4) (c) (ii)	Mandatory Reporting	
16	(iii) applied and ongoing mitigation measures.	Article 14 (4) (c) (iii)	Mandatory Reporting	

17	After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.	Article 14 (8)	Mandatory Reporting	
18	Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats	Article 15 (1)	Voluntary Reporting	

	that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA.			
19	Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA.	Article 15 (2)	Voluntary Reporting	

11.10.2 Manufacturer of Important and Critical Hardware Devices:

Manufacturers responsible for important and critical hardware devices under the Cyber Resilience Act (CRA) face stringent compliance obligations due to the elevated cybersecurity implications of their products. Such hardware, explicitly categorized within Annexes III and IV of the CRA, includes vital components like smart meter gateways, secure cryptoprocessors, and hardware security modules. Given their pivotal role in safeguarding critical infrastructure and digital ecosystems, manufacturers must implement comprehensive cybersecurity practices and rigorous assessment protocols. This section outlines detailed requirements, emphasizing proactive risk management, robust vulnerability handling, and meticulous technical documentation, ensuring manufacturers can demonstrate compliance effectively and maintain the resilience of Europe’s critical infrastructure.

Cybersecurity risk assessment

Manufacturers of important and critical hardware devices are required to conduct detailed cybersecurity risk assessments in accordance with Article 13 of the CRA. These assessments must thoroughly evaluate cybersecurity risks related to the product's intended use, foreseeable misuse, operational environment, and critical assets to be protected. Results from these assessments should directly inform the implementation of security measures throughout the product lifecycle. Manufacturers must document this process meticulously and regularly update their assessments to reflect evolving cybersecurity threats and technological developments.

Id	Requirement	Reference	Comment	Check
1	Manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.	article 13(2)	self-written - to be reviewed by notified body for critical and important products	- Verify that a comprehensive cybersecurity risk assessment has been conducted for each digital product. - Ensure that the outcomes of the risk assessment are integrated into all phases of the product lifecycle, including planning, design, development, production, delivery, and maintenance. - Confirm that the risk assessment effectively identifies and mitigates risks to user health and safety arising from cybersecurity incidents.
2	The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the	Article 13(3)	self-written - to be reviewed by notified body for critical and important products	- Ensure that the cybersecurity risk assessment is thoroughly documented and stored in accordance with Annex I, Part I - Verify that the documented risk assessment is regularly updated during the support period as determined by paragraph 8 of the CRA. - Confirm that the risk assessment includes analyses based on the product's intended purpose, foreseeable use,

	operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.			operational environment, protected assets, and expected lifespan. - Ensure that the documentation indicates the applicability and implementation status of security requirements from Annex I and vulnerability handling requirements from Part II of Annex I.
3	When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment in the technical documentation. For products with digital elements which are also subject to other Union legal acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation.	Article 13(4)	self-written - to be reviewed by notified body for critical and important products	- Verify that the cybersecurity risk assessment is included in the technical documentation provided when placing the product on the market. - Ensure that if the product is subject to other Union legal acts, the cybersecurity risk assessment complies with those additional requirements. - Confirm that any non-applicable essential cybersecurity requirements are clearly justified within the technical documentation.

4	The manufacturers shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products	Article 13(7)	self-written - to be reviewed by notified body for critical and important products	- Ensure that all relevant cybersecurity aspects, including known vulnerabilities and third-party information, are systematically documented. - Verify that the cybersecurity risk assessment is updated in response to new vulnerabilities or changes in third-party information. - Confirm that the documentation process is proportionate to the nature and risks associated with the digital product.

General requirements

SMEs manufacturing critical and important hardware products must adhere to CRA cybersecurity requirements, which are essential yet proportionate to their scale and resources. The following table highlights these key requirements, with practical guidelines suitable for SMEs.

ID	Requirement	Reference	Comment	Check
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.	Annex I, Part 1 §1	Assessed by notified body	- Verify that the product's design documentation includes detailed descriptions of cybersecurity measures implemented. - Assess whether comprehensive risk assessments have been performed during the design and development phases. - Confirm that identified risks have been mitigated through appropriate security controls and design choices.

				- Evaluate adherence to recognized cybersecurity frameworks and standards (e.g., ISO/IEC 27001) during the development process. - Implement static and dynamic application security testing (SAST/DAST) tools to detect potential security flaws early in the development cycle. - Confirm that a secure development lifecycle (SDLC) is integrated into the production process, encompassing phases such as design, development, testing, deployment, and maintenance.
2	On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:	Annex I, Part 1 §2	-	
3	(a) be made available on the market without known exploitable vulnerabilities;	Annex I, Part 1 §2a	Assessed by notified body	- Execute automated vulnerability scanning tools to identify known exploitable vulnerabilities within the product. - Ensure that scans cover all components, including third-party libraries and dependencies. - Validate that penetration tests are performed regularly and after significant code changes or updates. - Evaluate the security posture of all third-party

				components and libraries integrated into the product. - Ensure that third-party vulnerabilities are identified, assessed, and remediated in a timely manner.
4	(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;	Annex I, Part 1 §2b	Assessed by notified body	- Examine the product's default settings to ensure they prioritize security, minimizing potential attack vectors. - Confirm that unnecessary services and ports are disabled by default to reduce the product's attack surface. - Test the product's ability to reset to its original secure state, ensuring that all configurations revert to secure defaults upon reset. - Validate that the reset mechanism is reliable and user-friendly. - Assess the effectiveness of access controls surrounding configuration settings to prevent unauthorized modifications. - Ensure that changes to default configurations require appropriate authentication and authorization. - Review user guides and documentation to ensure that instructions for maintaining secure configurations are clear and comprehensive.

5	(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;	Annex 1, Part 1 §2c	Assessed by notified body	- Evaluate the mechanisms in place for delivering security updates, ensuring they are effective and reliable. - Confirm the availability of automatic security updates that install within an appropriate timeframe by default. - Test the notification systems that inform users about available security updates. - Ensure that notifications are clear, timely, and provide sufficient information for users to understand the update's importance. - Verify the presence of easy-to-use opt-out mechanisms allowing users to disable automatic updates if desired. - Assess the functionality that permits users to temporarily postpone security updates, ensuring it does not compromise overall security. - Review the policies governing the deployment of security patches to ensure vulnerabilities are addressed without undue delay. - Ensure that all security updates undergo rigorous testing before deployment to prevent the introduction of new vulnerabilities.

6	(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;	Annex I, Part 1 §2d	Assessed by notified body	- Ensure MFA is implemented and functioning correctly for all access points. - Verify that strong password policies (e.g., complexity, expiration) are enforced. - Confirm that user roles are appropriately defined and enforced. - Ensure users have the minimum level of access necessary for their roles.
7	(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;	Annex I, Part 1 §2e	Assessed by notified body	- Confirm that all sensitive data stored is encrypted using industry-standard algorithms (e.g., AES-256). - Ensure that data transmitted over networks is encrypted using protocols such as TLS 1.3. - Validate that only authorized personnel can access confidential data. - Verify the use of secure protocols for all data communications. - Ensure that sensitive data elements are masked or tokenized where applicable. - Perform periodic audits to identify and remediate vulnerabilities that could compromise data confidentiality.

8	(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;	Annex I, Part 1 §2f	Assessed by notified body	- Implement and test checksum or hash functions to detect unauthorized data modifications. - Ensure that digital signatures are used to verify the authenticity and integrity of data. - Confirm that only authorized users can modify critical data, commands, programs, and configurations. - Verify that logs cannot be altered or deleted without proper authorization. - Ensure that there are established procedures for reporting and responding to data corruption incidents. - Verify that procedures for handling integrity-related vulnerabilities are documented and effectively implemented.

9	(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);	Annex I, Part 1 §2g	Assessed by notified body	- Review data collection processes to ensure only necessary data for the product's intended purpose is collected. - Verify that the purpose for data collection is clearly defined and adhered to. - Ensure that data is not retained longer than necessary for its intended purpose. - Implement and test automated mechanisms for deleting data that is no longer needed. - Monitor who accesses data and for what purposes to ensure compliance with data minimization principles. - Ensure that personally identifiable information (PII) is anonymized where possible. - Test pseudonymization methods to protect data while retaining usability for analysis. - Ensure data minimization practices comply with GDPR and other relevant data protection regulations. - Verify that users provide informed consent for data collection and processing.

10	(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	Annex I, Part 1 §2h	Assessed by notified body	- Test failover systems to ensure continuity of essential functions during incidents. - Conduct simulated DoS attacks to assess the system's resilience and mitigation capabilities. - Ensure that critical components have redundancy to prevent single points of failure. - Ensure timely application of security patches to address vulnerabilities that could impact availability.
11	(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	Annex I, Part 1 §2i	Assessed by notified body	- Verify that the product does not excessively consume network or device resources, ensuring it does not degrade the performance or availability of connected services. - Ensure the product operates independently without causing cascading failures in connected systems.
12	(j) be designed, developed and produced to limit attack surfaces, including external interfaces;	Annex I, Part 1 §2j	Assessed by notified body	- Identify and evaluate potential vulnerabilities in all external interfaces (e.g., APIs, ports, network connections). - Ensure that only necessary external interfaces are enabled and properly secured.
13	(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	Annex I, Part 1 §2k	Assessed by notified body	- Validate the effectiveness of incident detection and response mechanisms in mitigating the impact of security breaches. - Ensure the product can maintain essential functions and

				recover quickly from incidents.
14	(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;	Annex I, Part 1 §2l	Assessed by notified body	- Ensure that the product accurately records and monitors relevant internal activities, including data access and modifications. - Validate that users can effectively opt out of security-related information recording and monitoring without compromising overall security.
15	(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.	Annex I, Part 1 §2m	Assessed by notified body	- Confirm that users can permanently delete all personal and configuration data from the product. - Ensure that data transfer between products or systems is conducted securely, maintaining confidentiality and integrity.
16	Manufacturers of products with digital elements shall:	Annex I - Part II	-	
17	(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;	Annex I, Part 2 §2	Assessed by notified body	- Ensure the creation and maintenance of a comprehensive SBOM in a standardized, machine-readable format (e.g., SPDX, CycloneDX) that encompasses at least the top-level dependencies of the product. - Confirm that all identified vulnerabilities and components are systematically documented, including detailed descriptions, affected components, and remediation statuses.

18	(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;	Annex I, Part 2 §1	Assessed by notified body	- Verify that identified vulnerabilities are addressed and remediated promptly in accordance with their associated risk levels, ensuring the provision of security updates without undue delays. - Ensure that, when technically feasible, security updates are delivered independently from functionality updates to minimize the risk of introducing new vulnerabilities.
19	(3) apply effective and regular tests and reviews of the security of the product with digital elements;	Annex I, Part 2 §3	Assessed by notified body	- Ensure that regular and effective security tests are conducted to proactively identify and mitigate potential vulnerabilities within the product. - Validate that security reviews are thoroughly documented, capturing findings, remedial actions, and verification of remediation efforts.
20	(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	Annex I, Part 2 §4	Assessed by notified body	- Confirm that once a security update is available, comprehensive information about fixed vulnerabilities is shared and publicly disclosed, including descriptions, affected products, impacts, severity, and remediation steps. - Ensure that in scenarios where immediate public disclosure could pose security risks, the manufacturer appropriately delays information release until users have the opportunity to apply necessary patches.

	delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;			
21	(5) put in place and enforce a policy on coordinated vulnerability disclosure;	Annex I, Part 2 §5	Assessed by notified body	- Verify the existence of a formally documented vulnerability disclosure policy. - Ensure the policy outlines roles and responsibilities, reporting channels, and timelines for response. - Check that the policy is publicly accessible to all stakeholders, including users and third-party researchers.
22	(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;	Annex I, Part 2 §6	Assessed by notified body	- Verify the provision of a dedicated contact address (e.g., email, web form) for vulnerability reporting on official platforms. - Assess the channels used for sharing vulnerability information with third parties and stakeholders. - Confirm the use of secure communication protocols to protect sensitive information during sharing. - Identify and document all third-party components within the product.

23	(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;	Annex I, Part 2 §7	Assessed by notified body	- Evaluate the security of the distribution channels used for delivering updates (e.g., HTTPS protocols, digital signatures). - Ensure that updates are hosted on trusted and secure servers to prevent tampering. - Measure the interval between vulnerability identification and the deployment of corresponding updates. - Confirm that updates include integrity checks (e.g., checksums, cryptographic signatures) to verify authenticity.
24	(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.	Annex I, Part 2 §8	Assessed by notified body	- Confirm that security updates are made available immediately upon their release. - Verify that security updates are provided free of charge unless an alternative agreement exists for tailor-made products. - Review the content of advisory messages to ensure they include comprehensive information about the vulnerability, affected products, severity, and remediation steps. - Ensure that advisory messages provide clear instructions on actions users should take to apply updates or mitigate vulnerabilities.

Information and instruction to the users

Manufacturers are required to deliver clear and comprehensive user information and instructions, including the manufacturer's name, registered trade name or trademark, full contact details, and a dedicated vulnerability reporting contact point. User documentation must detail the intended use of the product, instructions on maintaining cybersecurity throughout its operational life, the impact of any product changes on data security, guidance for securely applying security updates, and instructions for secure product decommissioning.

ID	Requirement	Reference	Comment	Check
1	At minimum, the product with digital elements shall be accompanied by:	Annex II	-	
2	1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;	Annex II, §1	Assessed by notified body, as part of the Technical Documentation	- Confirm that the product packaging and accompanying documentation clearly display the manufacturer's name, registered trade name or trademark, and a valid postal address. This includes cross-referencing the provided information with official trademark and business registries to ensure accuracy and authenticity. - Test the provided email address and digital contact methods to ensure they are operational and responsive. Additionally, verify that the manufacturer's website (if available) is accessible, regularly maintained, and provides up-to-date contact information, facilitating effective communication channels for users.

3	2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;	Annex II, §2	Assessed by notified body, as part of the Technical Documentation	- Ensure that the designated single point of contact for reporting vulnerabilities is prominently listed in the product documentation and is easily accessible to users. This includes verifying that the contact method (e.g., dedicated email address or web portal) is functional and that submissions are acknowledged within an appropriate timeframe. - Review the manufacturer's policy on coordinated vulnerability disclosure to confirm its presence, clarity, and comprehensiveness. The policy should be readily accessible, detailing procedures for reporting vulnerabilities, the manufacturer's responsibilities, expected timelines for responses, and guidelines for responsible disclosure practices.
4	3. name and type and any additional information enabling the unique identification of the product with digital elements;	Annex II, §3	Assessed by notified body, as part of the Technical Documentation	- Check that the product is clearly labeled with its specific name and type, and include unique identifiers such as model numbers, serial numbers, or other distinguishing features. This facilitates unambiguous identification and differentiation from other products in the market. - Verify that the unique identification information is consistently presented across all platforms, including physical packaging, digital documentation, online listings, and regulatory filings. Consistency ensures that users can reliably reference and access product-specific information when needed.

5	4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product’s essential functionalities and information about the security properties;	Annex II, §4	Assessed by notified body, as part of the Technical Documentation	- Assess whether the product documentation clearly outlines the intended purpose and primary functionalities of the product. This includes evaluating whether the descriptions accurately reflect the product's capabilities and are free from ambiguities that could lead to misuse. - Examine the detailed information provided about the product’s security properties and the security environment established by the manufacturer. This involves verifying that security measures, such as encryption standards, authentication mechanisms, and data protection protocols, are described and align with industry best practices.
6	5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	Annex II, §5	Assessed by notified body, as part of the Technical Documentation	- Review the product information to identify any listed or potential cybersecurity risks associated with both intended use and reasonably foreseeable misuse. This includes evaluating whether the risks are comprehensively documented and accompanied by clear descriptions of their implications. - Ensure that the product documentation includes detailed instructions or references for mitigating identified cybersecurity risks.
7	6. where applicable, the internet address at which the EU declaration of conformity can be accessed;	Annex II, §6	Assessed by notified body, as part of the Technical	- verifying that product packaging and accompanying documentation include a clear and functional internet address where users can access the EU Declaration of Conformity.

			Documentation	- To confirm that the provided internet address is not only present but also active, directs users correctly to the EU Declaration of Conformity, and remains accessible over time, thereby maintaining continuous compliance.
8	7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;	Annex VI, §7	Assessed by notified body, as part of the Technical Documentation	- Ensure that the end-date of the technical security support period is clearly stated in the product documentation, allowing users to plan for ongoing security needs and understand the timeline for receiving updates and support. - Verify that product documentation comprehensively outlines the types of technical security support provided by the manufacturer, including the available support channels, thereby enabling users to effectively address cybersecurity concerns.
9	8. detailed instructions or an internet address referring to such detailed instructions and information on:	Annex II, §8	Assessed by notified body, as part of the Technical Documentation	
10	(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;	Annex II, §8 (a)	Assessed by notified body, as part of the Technical Documentation	- Ensure that the detailed instructions for initial commissioning encompass essential security configurations to establish a secure foundation for the product from the outset, - Validate that the provided instructions offer exhaustive guidelines for maintaining security throughout the

				product's operational lifetime
11	(b) how changes to the product with digital elements can affect the security of data;	Annex II, §8 (b)	Assessed by notified body, as part of the Technical Documentation	- Evaluate the instructions' guidance on how modifications to the product may influence data security, ensuring that changes do not introduce new vulnerabilities - Ensure that the instructions incorporate measures to uphold data security continuity when product changes occur,
12	(c) how security-relevant updates can be installed;	Annex II, §8 (c)	Assessed by notified body, as part of the Technical Documentation	- Confirm that the instructions provide clear and effective procedures for installing security-relevant updates - Assess the effectiveness of automated update mechanisms as described in the instructions, ensuring timely and secure application of updates
13	(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;	Annex II, §8 (d)	Assessed by notified body, as part of the Technical Documentation	- Ensure that the instructions delineate clear and secure methods for permanently removing user data during decommissioning - Verify that the instructions outline comprehensive steps for the secure decommissioning of the product, mitigating the risk of data breaches during the process
14	(e) how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of Annex I, can be turned off;	Annex II, §8 (e)	Assessed by notified body, as part of the Technical Documentation	- Verify that the instructions provide a secure, user-friendly method for disabling the default setting that enables automatic security updates - Ensure that the instructions include appropriate warnings and guidance for users who choose to disable automatic

				security updates, maintaining overall security integrity.
15	(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII.	Annex II, §8 (f)	Assessed by notified body, as part of the Technical Documentation	- Ensure that comprehensive information necessary for integrators to comply with the essential cybersecurity requirements-
16	9. If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.	Annex II, §9	Not mandatory	- Ensure that when manufacturers choose to make the Software Bill of Materials (SBOM) available to users, comprehensive information on how to access the SBOM is clearly provided. -

EU Declaration of Conformity:

Manufacturers must produce an EU Declaration of Conformity confirming compliance with the relevant provisions of the CRA. This declaration must clearly state the product's name, type, and unique identifiers, the manufacturer's complete contact information, and explicitly declare adherence to the Cyber Resilience Act. It must also reference applicable harmonized standards, common specifications, or cybersecurity certifications and include a detailed statement outlining the conformity assessment procedures applied.

ID	Requirement	Reference	Comment	Check
1	The EU declaration of conformity referred to in Article 28, shall contain all of the following information:	Annex V	The EU Declaration of conformity is	

			self-written	
2	(1) Name and type and any additional information enabling the unique identification of the product with digital elements	Annex V, §1	-	- Ensure that the product’s name, type, and any additional identifying information (e.g., model number, serial number) are accurately listed in the EU Declaration of Conformity. - Confirm that unique identifiers (such as serial numbers or batch codes) included in the declaration facilitate the unambiguous identification of the product.
3	(2) Name and address of the manufacturer or its authorised representative	Annex V, §2	-	- Verify that the manufacturer’s name, official trade name or trademark, and complete postal address are correctly stated in the declaration. - Ensure that if an authorized representative is listed, their information is accurate and up-to-date.
4	(3) A statement that the EU declaration of conformity is issued under the sole responsibility of the provider	Annex V, §3	-	- Confirm that the declaration includes a clear statement asserting that it is issued under the sole responsibility of the provider. - Ensure that the responsibility statement aligns with legal requirements and certification standards.
5	(4) Object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate)	Annex V, §4	-	- Ensure that the declaration includes sufficient information (e.g., product ID, version) to allow for the traceability of the product. - Confirm that a photograph of the product is included when appropriate, aiding in visual identification and

				verification.
6	(5) A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation	Annex V, §5	-	- Verify that the declaration explicitly states that the product conforms with all relevant Union harmonisation legislation. - Ensure that the conformity statement is supported by appropriate evidence, such as test reports or certifications.
7	(6) References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared	Annex V, §6	if applicable	- Confirm that all referenced harmonised standards, common specifications, or cybersecurity certifications are correctly cited in the declaration. - Ensure that the referenced standards and certifications are relevant to the product's intended use and functionalities.
8	(7) Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued	Annex V, §7	mandatory	- Ensure that the declaration includes the correct name and identification number of the notified body involved in the conformity assessment. - Verify that the declaration describes the conformity assessment procedures performed by the notified body.
9	(8) Additional information: Signed for and on behalf of: (place and date of issue): (name, function) (signature):	Annex V, §8	-	- Ensure that the declaration is signed by an authorized representative of the manufacturer, including their name and function. - Confirm that the declaration includes the accurate place and date of issue, ensuring temporal and geographical

				validity.
10	SIMPLIFIED EU DECLARATION OF CONFORMITY	Annex VI	Only for SMEs and micro-enterprises	
11	The simplified EU declaration of conformity referred to shall be provided as follows: Hereby, ... [name of manufacturer] declares that the product with digital elements type ... [designation of type of product with digital element] is in compliance with Regulation (EU) 2024/…+ . The full text of the EU declaration of conformity is available at the following internet address: …	Annex VI	self-written	
12	The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.	Annex VIII, Part II, §10 and Part III, §3.2	-	- Ensure that manufacturers maintain the EU Declaration of Conformity appropriately alongside technical documentation for the mandated retention period - Verify that manufacturers can promptly provide a copy of the EU Declaration of Conformity to national authorities upon request, as required by Article 28.9.

Technical documentation

The technical documentation must comprehensively detail the intended purpose of the device, specifying software versions pertinent to cybersecurity compliance, providing detailed hardware architecture descriptions, and outlining robust processes for identifying, handling, and remediating vulnerabilities promptly. This documentation must mandatorily include a detailed Software Bill of Materials (SBOM) listing all relevant software components and dependencies, ensuring transparency and traceability. Manufacturers must systematically demonstrate their structured vulnerability handling processes, including detailed test reports and evidence of rigorous production, monitoring, and lifecycle validation practices. Given the critical nature of these products, third-party conformity assessments or relevant European cybersecurity certification at a substantial assurance level are required to validate compliance comprehensively.

ID	Requirement	Reference	Comment	Check
1	The technical documentation shall contain at least the following information, as applicable to the relevant product with digital elements:	Annex VII	-	
2	1. a general description of the product with digital elements, including:	Annex VII, §1	Assessed by notified body	
3	(a) its intended purpose;	Annex VII, §1 (a)	Assessed by notified body	- Verify that the documentation clearly states the primary function and intended use cases of the product. - Ensure the description aligns with the product's marketing materials and user manuals.
4	(b) versions of software affecting compliance with essential cybersecurity requirements;	Annex VII, §1 (b)	Assessed by notified body	- Ensure that all relevant software versions are explicitly mentioned. - Verify that version numbering follows a consistent and clear schema.

5	(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;	Annex VII, §1 (c)	Assessed by notified body	- Check for high-resolution photographs or detailed illustrations showcasing all external components and interfaces. - Ensure that labels, ports, and indicators are clearly marked and described.
6	(d) user information and instructions as set out in Annex II;	Annex VII, §1 (d)	Assessed by notified body	- Verify that the user manual includes all sections outlined in Annex II, such as installation, configuration, operation, and troubleshooting.
7	2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:	Annex VII, §2	Assessed by notified body	
8	(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;	Annex VII, §2 (a)	Assessed by notified body	- Ensure that the technical documentation encompasses exhaustive drawings and schematics that accurately delineate the system architecture of the digital product. - Verify that the documentation explicitly explains the integration points and dependencies among various software components within the digital product.
9	(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	Annex VII, §2 (b)	Assessed by notified body	- Confirm that the Software Bill of Materials (SBOM) is provided in a standardized, machine-readable format and encompasses at least the top-level dependencies of the digital product. - Ensure the establishment of a robust coordinated

	address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;			vulnerability disclosure policy, including a designated contact address for reporting vulnerabilities.
10	(c) necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;	Annex VII, §2 (c)	self-Assessed by notified body	- Verify that the technical documentation furnishes comprehensive information on the production processes, encompassing quality assurance and security measures. - Ensure that the technical documentation includes specifications for monitoring processes designed to validate the product's functionality and security throughout its lifecycle.
11	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;	Annex VII, §3	Assessed by notified body	- Ensure that the technical documentation encompasses a thorough assessment of cybersecurity risks associated with the product throughout its lifecycle
12	4. relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements;	Annex VII, §4	Assessed by notified body	- Ensure that the technical documentation incorporates relevant information and criteria utilized to determine the support period for the product

13	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;	Annex VII, §5	Assessed by notified body	- Ensure that the technical documentation includes a comprehensive list of harmonised standards applied to the product, complete with their official references as published in the Official Journal of the European Union.
14	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;	Annex VII, §6	Assessed by notified body	- Ensure that the technical documentation includes detailed reports of tests conducted to verify the product's conformity with essential cybersecurity requirements - Verify that the documentation contains detailed reports on the vulnerability handling processes

15	7. a copy of the EU declaration of conformity;	Annex VII, §7	Assessed by notified body	- Ensure that a complete and accurate copy of the EU Declaration of Conformity is included in the technical documentation
16	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.	Annex VII, §8	Assessed by notified body	- Ensure that the technical documentation specifies where users can access the Software Bill of Materials (SBOM) when it is made available - Verify that the manufacturer can provide the SBOM upon a reasoned request from a market surveillance authority

Reporting requirements:

Manufacturers have mandatory obligations to promptly report any actively exploited cybersecurity vulnerabilities and severe cybersecurity incidents affecting their products. Notifications must be made simultaneously to the designated CSIRT coordinator and ENISA, including early warning notifications within 24 hours, detailed vulnerability notifications within 72 hours, and comprehensive final incident reports within one month of the initial notification. Reports must clearly detail the vulnerabilities or incidents, their impacts, the remedial actions taken, and provide recommendations for affected users.

ID	Requirement	Reference	Comment	Check
1	A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established	Article 14(1) and 14(7)	Mandatory Reporting	

	pursuant to Article 16.			
2	For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:	Article 14 (2)	Mandatory Reporting	
3	(a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;	Article 14 (2) (a)	Mandatory Reporting	
4	(b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive	Article 14 (2) (b)	Mandatory Reporting	

	the manufacturer considers the notified information to be;			
5	(c) unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available, including at least the following:	Article 14 (2) (c)	Mandatory Reporting	
6	(i) a description of the vulnerability, including its severity and impact;	Article 14 (2) (c) (i)	Mandatory Reporting	
7	(ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;	Article 14 (2) (c) (ii)	Mandatory Reporting	
8	(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.	Article 14 (2) (c) (iII)	Mandatory Reporting	
9	A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform	Article 14 (3)	Single platform is not yet established (Dec 2024)	
10	For the purposes of the notification referred to in paragraph 3, the	Article 14 (4)	Mandatory Reporting	

	manufacturer shall submit:			
11	(a) an early warning notification of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;	Article 14 (4) (a)	Mandatory Reporting	
12	(b) unless the relevant information has already been provided, an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer	Article 14 (4) (b)	Mandatory Reporting	

	considers the notified information to be;			
13	(c) unless the relevant information has already been provided, a final report, within one month after the submission of the incident notification under point (b), including at least the following:	Article 14 (4) (c)	Mandatory Reporting	
14	(i) a detailed description of the incident, including its severity and impact;	Article 14 (4) (c) (i)	Mandatory Reporting	
15	(ii) the type of threat or root cause that is likely to have triggered the incident;	Article 14 (4) (c) (ii)	Mandatory Reporting	
16	(iii) applied and ongoing mitigation measures.	Article 14 (4) (c) (iii)	Mandatory Reporting	
17	After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable.	Article 14 (8)	Mandatory Reporting	

	Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.			
18	Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA.	Article 15 (1)	Voluntary Reporting	
19	Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA.	Article 15 (2)	Voluntary Reporting	

Lodging an application for certification:

Manufacturers of important or critical devices must submit comprehensive applications for third-party conformity assessments or applicable European cybersecurity certifications to demonstrate compliance with the Cyber Resilience Act. The application must include detailed technical documentation, clearly outlining cybersecurity design choices, vulnerability management practices, security test reports, and evidence of secure-by-design and secure-by-default configurations. Additionally, manufacturers are required to provide thorough information on vulnerability disclosure policies, Software Bill of Materials (SBOM), and ongoing product monitoring and lifecycle validation processes. Certification or conformity assessments should reflect the high assurance levels appropriate to the critical nature of the devices.

ID	Requirement	Reference	Comment	Check
1	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.	Annex VIII, Part II, §1	-	
2	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, and the examination	Annex VIII, Part II, §2	-	

	of specimens of one or more critical parts of the product (combination of production type and design type).			
3	The manufacturer shall lodge an application for assessment of its quality system with the notified body of its choice, for the products with digital elements concerned. The application shall include:	Annex VIII, Part II, §3	-	
4	the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;	Annex VIII, Part II, §3.1	-	
5	a written declaration that the same application has not been lodged with any other notified body;	Annex VIII, Part II, §3.2	-	
6	the technical documentation, which shall make it possible to assess the conformity of the product with digital elements with the applicable essential cybersecurity requirements as set out in Part I of Annex I and the manufacturer’s vulnerability handling processes set out in Part II of Annex I and shall include an adequate analysis and assessment of the risks. The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design,	Annex VIII, Part II, §3.3	-	

	manufacture and operation of the product with digital elements. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex VII;			
7	the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on its behalf and under its responsibility.	Annex VIII, Part II, §3.4	-	
8	The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential cybersecurity requirements set out in Annex I, or the	Annex VIII, Part II, §7	-	

	conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.			
9	The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.	Annex VIII, Part II, §10	-	

11.10.3 Manufacturer of Important and Critical Softwares:

Important and critical software plays a crucial role in Europe’s digital infrastructure, necessitating rigorous compliance with the Cyber Resilience Act (CRA). Manufacturers of such software must manage complex cybersecurity risks due to their products’ substantial impact on digital ecosystems, user data protection, and critical operations. The CRA mandates comprehensive security measures, frequent risk assessment updates, and stringent vulnerability disclosure policies to minimize potential cyber threats effectively. This section provides structured guidance, highlighting critical requirements to ensure thorough documentation, ongoing vulnerability management, and secure software development practices. The goal is to empower software manufacturers with clear, practical strategies for CRA compliance, fostering secure innovation and building user trust.

Cybersecurity risk assessment

Manufacturers of important or critical software are required to conduct thorough cybersecurity risk assessments in compliance with Article 13 of the Cyber Resilience Act (CRA). This assessment must comprehensively evaluate cybersecurity risks associated with the software’s intended purpose, clearly accounting for foreseeable conditions of use and potential misuse scenarios. The assessment must explicitly address the software's operational environment and critical assets, reflecting the expected lifespan and usage conditions of the software product.

The risk assessment must document how the essential cybersecurity requirements outlined in Annex I (Parts I and II) are applicable and specifically implemented in the software. Manufacturers must detail systematic processes for identifying, mitigating, and remediating vulnerabilities, ensuring these processes are fully integrated into the design, development, delivery, and ongoing maintenance stages of the software lifecycle. Furthermore, the risk assessment must explicitly address how vulnerabilities are managed through timely security updates and corrective actions.

Additionally, manufacturers must provide comprehensive documentation demonstrating regular reviews and updates to their cybersecurity risk assessments, reflecting new vulnerabilities, evolving threats, and changes in operational conditions. This documentation must clearly justify any non-applicable cybersecurity requirements, outlining specific reasons in the technical documentation. All assessment activities must be proportionate to the identified cybersecurity risks, thoroughly documented, and maintained consistently throughout the defined support period of the software product.

ID	Requirement	Reference	Comment	Check
1	Software developers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety	article 13(2)	self-written - to be reviewed by notified body for critical and important products	- Verify that a comprehensive cybersecurity risk assessment has been conducted for each digital product. - Ensure that the outcomes of the risk assessment are integrated into all phases of the product lifecycle, including planning, design, development, production, delivery, and maintenance. - Confirm that the risk assessment effectively identifies and mitigates risks to user health and safety arising from cybersecurity incidents.

	of users.			
2	The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the software developer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.	Article 13(3)	self-written - to be reviewed by notified body for critical and important products	- Ensure that the cybersecurity risk assessment is thoroughly documented and stored in accordance with Annex I, Part I - Verify that the documented risk assessment is regularly updated during the support period as determined by paragraph 8 of the CRA. - Confirm that the risk assessment includes analyses based on the product's intended purpose, foreseeable use, operational environment, protected assets, and expected lifespan. - Ensure that the documentation indicates the applicability and implementation status of security requirements from Annex I and vulnerability handling requirements from Part II of Annex I.

3	When placing a product with digital elements on the market, the software developer shall include the cybersecurity risk assessment in the technical documentation. For products with digital elements which are also subject to other Union legal acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the software developer shall include a clear justification to that effect in that technical documentation.	Article 13(4)	self-written - to be reviewed by notified body for critical and important products	- Verify that the cybersecurity risk assessment is included in the technical documentation provided when placing the product on the market. - Ensure that if the product is subject to other Union legal acts, the cybersecurity risk assessment complies with those additional requirements. - Confirm that any non-applicable essential cybersecurity requirements are clearly justified within the technical documentation.
4	The software developer shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products	Article 13(7)	self-written - to be reviewed by notified body for critical and important products	- Ensure that all relevant cybersecurity aspects, including known vulnerabilities and third-party information, are systematically documented. - Verify that the cybersecurity risk assessment is updated in response to new vulnerabilities or changes in third-party information. - Confirm that the documentation process is proportionate to the nature and risks associated with the digital product.

General requirements

Manufacturers of important or critical software must ensure adherence to the fundamental cybersecurity requirements outlined by the Cyber Resilience Act throughout the entire lifecycle of their software products. This includes implementing cybersecurity measures based on thorough risk assessments relevant to the software's intended use and operational environment. Software must be free from known exploitable vulnerabilities at the point of market entry, incorporate secure-by-default configurations, and facilitate timely, often automatic, security updates. Manufacturers must also maintain robust mechanisms for unauthorized access control, comprehensive data confidentiality and integrity protections, and effective data minimization practices. Detailed documentation is required, including explicit instructions on vulnerability management, secure commissioning, secure updates, and secure decommissioning.

ID	Requirement	Reference	Comment	Check
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.	Annex I, Part 1 §1	Assessed by notified body	- Verify that the product's design documentation includes detailed descriptions of cybersecurity measures implemented. - Assess whether comprehensive risk assessments have been performed during the design and development phases. - Confirm that identified risks have been mitigated through appropriate security controls and design choices. - Evaluate adherence to recognized cybersecurity frameworks and standards (e.g., ISO/IEC 27001) during the development process. - Implement static and dynamic application security testing (SAST/DAST) tools to detect potential security flaws early in the development cycle.

				- Confirm that a secure development lifecycle (SDLC) is integrated into the production process, encompassing phases such as design, development, testing, deployment, and maintenance.
2	On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:	Annex I, Part 1 §2	-	
3	(a) be made available on the market without known exploitable vulnerabilities;	Annex I, Part 1 §2a	Assessed by notified body	- Execute automated vulnerability scanning tools to identify known exploitable vulnerabilities within the product. - Ensure that scans cover all components, including third-party libraries and dependencies. - Validate that penetration tests are performed regularly and after significant code changes or updates. - Evaluate the security posture of all third-party components and libraries integrated into the product. - Ensure that third-party vulnerabilities are identified, assessed, and remediated in a timely manner.
4	(b) be made available on the market with a secure by default configuration, unless otherwise agreed between the software developer and business user in relation to a tailor-made product with digital elements,	Annex I, Part 1 §2b	Assessed by notified body	- Examine the product's default settings to ensure they prioritize security, minimizing potential attack vectors. - Confirm that unnecessary services and ports are disabled by default to reduce the product's attack surface.

	including the possibility to reset the product to its original state;			- Test the product's ability to reset to its original secure state, ensuring that all configurations revert to secure defaults upon reset. - Validate that the reset mechanism is reliable and user-friendly. - Assess the effectiveness of access controls surrounding configuration settings to prevent unauthorized modifications. - Ensure that changes to default configurations require appropriate authentication and authorization. - Review user guides and documentation to ensure that instructions for maintaining secure configurations are clear and comprehensive.
5	(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;	Annex 1, Part 1 §2c	Assessed by notified body	- Evaluate the mechanisms in place for delivering security updates, ensuring they are effective and reliable. - Confirm the availability of automatic security updates that install within an appropriate timeframe by default. - Test the notification systems that inform users about available security updates. - Ensure that notifications are clear, timely, and provide

				sufficient information for users to understand the update's importance. - Verify the presence of easy-to-use opt-out mechanisms allowing users to disable automatic updates if desired. - Assess the functionality that permits users to temporarily postpone security updates, ensuring it does not compromise overall security. - Review the policies governing the deployment of security patches to ensure vulnerabilities are addressed without undue delay. - Ensure that all security updates undergo rigorous testing before deployment to prevent the introduction of new vulnerabilities.
6	(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;	Annex I, Part 1 §2d	Assessed by notified body	- Ensure MFA is implemented and functioning correctly for all access points. - Verify that strong password policies (e.g., complexity, expiration) are enforced. - Confirm that user roles are appropriately defined and enforced. - Ensure users have the minimum level of access necessary for their roles.

7	(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;	Annex I, Part 1 §2e	Assessed by notified body	- Confirm that all sensitive data stored is encrypted using industry-standard algorithms (e.g., AES-256). - Ensure that data transmitted over networks is encrypted using protocols such as TLS 1.3. - Validate that only authorized personnel can access confidential data. - Verify the use of secure protocols for all data communications. - Ensure that sensitive data elements are masked or tokenized where applicable. - Perform periodic audits to identify and remediate vulnerabilities that could compromise data confidentiality.
8	(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;	Annex I, Part 1 §2f	Assessed by notified body	- Implement and test checksum or hash functions to detect unauthorized data modifications. - Ensure that digital signatures are used to verify the authenticity and integrity of data. - Confirm that only authorized users can modify critical data, commands, programs, and configurations. - Verify that logs cannot be altered or deleted without proper authorization.

				- Ensure that there are established procedures for reporting and responding to data corruption incidents. - Verify that procedures for handling integrity-related vulnerabilities are documented and effectively implemented.
9	(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);	Annex I, Part 1 §2g	Assessed by notified body	- Review data collection processes to ensure only necessary data for the product's intended purpose is collected. - Verify that the purpose for data collection is clearly defined and adhered to. - Ensure that data is not retained longer than necessary for its intended purpose. - Implement and test automated mechanisms for deleting data that is no longer needed. - Monitor who accesses data and for what purposes to ensure compliance with data minimization principles. - Ensure that personally identifiable information (PII) is anonymized where possible. - Test pseudonymization methods to protect data while retaining usability for analysis. - Ensure data minimization practices comply with GDPR and

				other relevant data protection regulations. - Verify that users provide informed consent for data collection and processing.
10	(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	Annex I, Part 1 §2h	Assessed by notified body	- Test failover systems to ensure continuity of essential functions during incidents. - Conduct simulated DoS attacks to assess the system's resilience and mitigation capabilities. - Ensure that critical components have redundancy to prevent single points of failure. - Ensure timely application of security patches to address vulnerabilities that could impact availability.
11	(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	Annex I, Part 1 §2i	Assessed by notified body	- Verify that the product does not excessively consume network or device resources, ensuring it does not degrade the performance or availability of connected services. - Ensure the product operates independently without causing cascading failures in connected systems.
12	(j) be designed, developed and produced to limit attack surfaces, including external interfaces;	Annex I, Part 1 §2j	Assessed by notified body	- Identify and evaluate potential vulnerabilities in all external interfaces (e.g., APIs, ports, network connections). - Ensure that only necessary external interfaces are enabled and properly secured.

13	(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	Annex I, Part 1 §2k	Assessed by notified body	- Validate the effectiveness of incident detection and response mechanisms in mitigating the impact of security breaches. - Ensure the product can maintain essential functions and recover quickly from incidents.
14	(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;	Annex I, Part 1 §2l	Assessed by notified body	- Ensure that the product accurately records and monitors relevant internal activities, including data access and modifications. - Validate that users can effectively opt out of security-related information recording and monitoring without compromising overall security.
15	(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.	Annex I, Part 1 §2m	Assessed by notified body	- Confirm that users can permanently delete all personal and configuration data from the product. - Ensure that data transfer between products or systems is conducted securely, maintaining confidentiality and integrity.
16	Software developers of products with digital elements shall:	Annex I - Part II	-	
17	(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	Annex I, Part 2 §2	Assessed by notified body	- Ensure the creation and maintenance of a comprehensive SBOM in a standardized, machine-readable format (e.g., SPDX, CycloneDX) that encompasses at least the top-level dependencies of the product. - Confirm that all identified vulnerabilities and components

	top-level dependencies of the products;			are systematically documented, including detailed descriptions, affected components, and remediation statuses.
18	(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;	Annex I, Part 2 §1	Assessed by notified body	- Verify that identified vulnerabilities are addressed and remediated promptly in accordance with their associated risk levels, ensuring the provision of security updates without undue delays. - Ensure that, when technically feasible, security updates are delivered independently from functionality updates to minimize the risk of introducing new vulnerabilities.
19	(3) apply effective and regular tests and reviews of the security of the product with digital elements;	Annex I, Part 2 §3	Assessed by notified body	- Ensure that regular and effective security tests are conducted to proactively identify and mitigate potential vulnerabilities within the product. - Validate that security reviews are thoroughly documented, capturing findings, remedial actions, and verification of remediation efforts.
20	(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	Annex I, Part 2 §4	Assessed by notified body	- Confirm that once a security update is available, comprehensive information about fixed vulnerabilities is shared and publicly disclosed, including descriptions, affected products, impacts, severity, and remediation steps. - Ensure that in scenarios where immediate public disclosure could pose security risks, the manufacturer appropriately delays information release until users have the opportunity to apply necessary patches.

	vulnerabilities; in duly justified cases, where software developers 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;			
21	(5) put in place and enforce a policy on coordinated vulnerability disclosure;	Annex I, Part 2 §5	Assessed by notified body	- Verify the existence of a formally documented vulnerability disclosure policy. - Ensure the policy outlines roles and responsibilities, reporting channels, and timelines for response. - Check that the policy is publicly accessible to all stakeholders, including users and third-party researchers.
22	(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;	Annex I, Part 2 §6	Assessed by notified body	- Verify the provision of a dedicated contact address (e.g., email, web form) for vulnerability reporting on official platforms. - Assess the channels used for sharing vulnerability information with third parties and stakeholders. - Confirm the use of secure communication protocols to protect sensitive information during sharing. - Identify and document all third-party components within the product.

23	(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;	Annex I, Part 2 §7	Assessed by notified body	- Evaluate the security of the distribution channels used for delivering updates (e.g., HTTPS protocols, digital signatures). - Ensure that updates are hosted on trusted and secure servers to prevent tampering. - Measure the interval between vulnerability identification and the deployment of corresponding updates. - Confirm that updates include integrity checks (e.g., checksums, cryptographic signatures) to verify authenticity.
24	(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a software developer 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.	Annex I, Part 2 §8	Assessed by notified body	- Confirm that security updates are made available immediately upon their release. - Verify that security updates are provided free of charge unless an alternative agreement exists for tailor-made products. - Review the content of advisory messages to ensure they include comprehensive information about the vulnerability, affected products, severity, and remediation steps. - Ensure that advisory messages provide clear instructions on actions users should take to apply updates or mitigate vulnerabilities.

General documentation

Manufacturers of important or critical software must provide thorough documentation that accompanies each product, clearly detailing essential cybersecurity-related information. This documentation must include the manufacturer's official identification, such as name, registered trade name or trademark, full postal address, digital contact methods, and an accessible website where available. Additionally, it must clearly state a single dedicated contact point for vulnerability reporting, alongside a transparent policy for coordinated vulnerability disclosure.

The documentation should precisely describe the intended purpose of the software, highlighting essential functionalities, security properties, and clearly outlining the intended operational environment, including any known or foreseeable circumstances under which significant cybersecurity risks could arise. Manufacturers must explicitly document secure usage guidelines, necessary actions for secure initial commissioning, lifecycle management, and potential security implications arising from modifications to the software.

Detailed instructions on the secure installation of security updates, secure product decommissioning, and secure removal of user data must also be included. Furthermore, if applicable, the documentation should clearly specify the internet address where users can access the Software Bill of Materials (SBOM), facilitating transparency and traceability.

Additionally, manufacturers must identify a clearly defined single point of contact for vulnerability reporting and provide comprehensive details about their coordinated vulnerability disclosure policy, ensuring effective and efficient vulnerability management.

ID	Requirement	Reference	Comment	Check
1	At minimum, the product with digital elements shall be accompanied by:	Annex II	Assessed by notified body, as part of the Technical Documentation	
2	1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital	Annex II, §1	Assessed by notified body, as part of the Technical	

	contact as well as, where available, the website at which the manufacturer can be contacted;		Documentation	
3	2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;	Annex II, §2	Assessed by notified body, as part of the Technical Documentation	
4	3. name and type and any additional information enabling the unique identification of the product with digital elements;	Annex II, §3	Assessed by notified body, as part of the Technical Documentation	
5	4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;	Annex II, §4	Assessed by notified body, as part of the Technical Documentation	
6	5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	Annex II, §5	Assessed by notified body, as part of the Technical Documentation	
7	6. where applicable, the internet address at which the EU declaration of conformity can be accessed;	Annex II, §6	Assessed by notified body, as part of the Technical Documentation	

8	7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;	Annex VI, §7	Assessed by notified body, as part of the Technical Documentation	
9	8. detailed instructions or an internet address referring to such detailed instructions and information on:	Annex II, §8	Assessed by notified body, as part of the Technical Documentation	
10	(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;	Annex II, §8 (a)	Assessed by notified body, as part of the Technical Documentation	
11	(b) how changes to the product with digital elements can affect the security of data;	Annex II, §8 (b)	Assessed by notified body, as part of the Technical Documentation	
12	(c) how security-relevant updates can be installed;	Annex II, §8 (c)	Assessed by notified body, as part of the Technical Documentation	
13	(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;	Annex II, §8 (d)	Assessed by notified body, as part of the Technical Documentation	

14	(e) how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of Annex I, can be turned off;	Annex II, §8 (e)	Assessed by notified body, as part of the Technical Documentation	
15	(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII.	Annex II, §8 (f)	Assessed by notified body, as part of the Technical Documentation	
16	9. If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.	Annex II, §9	Not mandatory	
17	The user information and instructions as set out in Annex II (detailed above), shall be included in the Technical Documentation.	Annex VII, §1 (d)	-	

EU declaration of conformity:

Manufacturers of important or critical software must issue an EU Declaration of Conformity, explicitly declaring their software products' compliance with the relevant Cyber Resilience Act (CRA) cybersecurity requirements. This declaration must include essential product identification information, such as software name, type, and version, facilitating clear traceability. Manufacturers must clearly state their identity and provide contact details, including a postal address and digital communication channels, to ensure effective accountability and communication.

The declaration must explicitly confirm compliance with applicable Union harmonisation legislation, referencing relevant harmonised standards, common specifications, or European cybersecurity certification schemes utilized during compliance evaluation. If applicable, it must detail third-party assessments, including notified body identification, conformity assessment procedures performed, and references to issued certifications.

Manufacturers must sign and date the declaration, including their representative’s name and position, confirming their sole responsibility for product compliance. They must maintain this EU Declaration of Conformity alongside technical documentation, readily accessible to regulatory authorities upon request, for a minimum of 10 years after the product has been placed on the market or throughout its declared support period, whichever is longer.

ID	Requirement	Reference	Comment	Check
1	The EU declaration of conformity referred to in Article 28, shall contain all of the following information:	Annex V	The EU Declaration of conformity is self-written	
2	(1) Name and type and any additional information enabling the unique identification of the product with digital elements	Annex V, §1	-	
3	(2) Name and address of the manufacturer or its authorised representative	Annex V, §2	-	
4	(3) A statement that the EU declaration of conformity is issued under the sole responsibility of the provider	Annex V, §3	-	
5	(4) Object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate)	Annex V, §4	-	

6	(5) A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation	Annex V, §5	-	
7	(6) References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared	Annex V, §6	if applicable	
8	(7) Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued	Annex V, §7	if applicable	
9	(8) Additional information: Signed for and on behalf of: (place and date of issue): (name, function) (signature):	Annex V, §8	-	
10	SIMPLIFIED EU DECLARATION OF CONFORMITY	Annex VI	Only for SMEs and micro-enterprises	
11	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;	Annex VII, §3	Assessed by notified body	
12	4. relevant information that was taken into account to determine the support period	Annex VII, §4	Assessed by notified body	

	pursuant to Article 13(8) of the product with digital elements;			
13	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;	Annex VII, §5	Assessed by notified body	
14	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	Annex VII, §6	Assessed by notified body	

	I;			
15	7. a copy of the EU declaration of conformity;	Annex VII, §7	Assessed by notified body	
16	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.	Annex VII, §8	Assessed by notified body	

Technical documentation

The technical documentation for important or critical software must comprehensively outline the intended cybersecurity purpose of the software, including explicit documentation of software versions relevant to cybersecurity compliance, descriptions of architecture, and a robust vulnerability handling framework. This documentation must include a complete and detailed Software Bill of Materials (SBOM), explicitly listing and documenting the software components, dependencies, and any known vulnerabilities. Additionally, manufacturers must maintain thorough evidence showing proactive and systematic handling and remediation of cybersecurity vulnerabilities, supported by extensive testing and clearly documented test reports. The documentation must also detail rigorous practices concerning production, ongoing monitoring, and lifecycle validation procedures, suitable to the critical impact of the software on user security and operational continuity. Compliance verification via third-party assessments or applicable European cybersecurity certification schemes is mandatory.

ID	Requirement	Reference	Comment	Check
1	The technical documentation shall contain at least the following information, as applicable to the relevant product with digital elements:	Annex VII	-	

2	1. a general description of the product with digital elements, including:	Annex VII, §1	Assessed by notified body	
3	(a) its intended purpose;	Annex VII, §1 (a)	Assessed by notified body	- Verify that the documentation clearly states the primary function and intended use cases of the product. - Ensure the description aligns with the product's marketing materials and user manuals.
4	(b) versions of software affecting compliance with essential cybersecurity requirements;	Annex VII, §1 (b)	Assessed by notified body	- Ensure that all relevant software versions are explicitly mentioned. - Verify that version numbering follows a consistent and clear schema.
5	(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;	Annex VII, §1 (c)	Assessed by notified body	- Check for high-resolution photographs or detailed illustrations showcasing all external components and interfaces. - Ensure that labels, ports, and indicators are clearly marked and described.
6	(d) user information and instructions as set out in Annex II;	Annex VII, §1 (d)	Assessed by notified body	- Verify that the user manual includes all sections outlined in Annex II, such as installation, configuration, operation, and troubleshooting.
7	2. a description of the design, development and production of the product with digital elements	Annex VII, §2	Assessed by notified body	

	and vulnerability handling processes, including:			
8	(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;	Annex VII, §2 (a)	Assessed by notified body	- Ensure that the technical documentation encompasses exhaustive drawings and schematics that accurately delineate the system architecture of the digital product. - Verify that the documentation explicitly explains the integration points and dependencies among various software components within the digital product.
9	(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;	Annex VII, §2 (b)	Assessed by notified body	- Confirm that the Software Bill of Materials (SBOM) is provided in a standardized, machine-readable format and encompasses at least the top-level dependencies of the digital product. - Ensure the establishment of a robust coordinated vulnerability disclosure policy, including a designated contact address for reporting vulnerabilities.
10	(c) necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;	Annex VII, §2 (c)	self-Assessed by notified body	- Verify that the technical documentation furnishes comprehensive information on the production processes, encompassing quality assurance and security measures. - Ensure that the technical documentation includes specifications for monitoring

				processes designed to validate the product's functionality and security throughout its lifecycle.
11	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;	Annex VII, §3	Assessed by notified body	- Ensure that the technical documentation encompasses a thorough assessment of cybersecurity risks associated with the product throughout its lifecycle
12	4. relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements;	Annex VII, §4	Assessed by notified body	- Ensure that the technical documentation incorporates relevant information and criteria utilized to determine the support period for the product
13	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	Annex VII, §5	Assessed by notified body	- Ensure that the technical documentation includes a comprehensive list of harmonised standards applied to the product, complete with their official references as published in the Official Journal of the European Union.

	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;			
14	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;	Annex VII, §6	Assessed by notified body	- Ensure that the technical documentation includes detailed reports of tests conducted to verify the product's conformity with essential cybersecurity requirements - Verify that the documentation contains detailed reports on the vulnerability handling processes
15	7. a copy of the EU declaration of conformity;	Annex VII, §7	Assessed by notified body	- Ensure that a complete and accurate copy of the EU Declaration of Conformity is included in the technical documentation
16	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.	Annex VII, §8	Assessed by notified body	- Ensure that the technical documentation specifies where users can access the Software Bill of Materials (SBOM) when it is made available - Verify that the manufacturer can provide the SBOM upon a reasoned request from a market surveillance authority

Communication with the authorities

Manufacturers of important or critical software must proactively communicate and collaborate with relevant authorities as required by the Cyber Resilience Act. They must promptly notify the designated Computer Security Incident Response Team (CSIRT) and the European Union Agency for Cybersecurity (ENISA) via the official reporting platform about any actively exploited vulnerabilities within 24 hours after discovery, followed by detailed notifications within 72 hours. Final comprehensive reports must be submitted within 14 days of providing corrective or mitigating measures. This communication must include detailed descriptions of vulnerabilities, their severity and impacts, potential exploitation, corrective measures, and guidelines for users to mitigate risks effectively.

Manufacturers must also ensure transparency by maintaining and publishing clear, comprehensive vulnerability disclosure policies and providing accessible contact channels for reporting vulnerabilities and security incidents.

ID	Requirement	Reference	Comment	Check
1	A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.	Article 14(1) and 14(7)	Mandatory Reporting	
2	For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:	Article 14 (2)	Mandatory Reporting	
3	(a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;	Article 14 (2) (a)	Mandatory Reporting	

4	(b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;	Article 14 (2) (b)	Mandatory Reporting	
5	(c) unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available, including at least the following:	Article 14 (2) (c)	Mandatory Reporting	
6	(i) a description of the vulnerability, including its severity and impact;	Article 14 (2) (c) (i)	Mandatory Reporting	
7	(ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;	Article 14 (2) (c) (ii)	Mandatory Reporting	
8	(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.	Article 14 (2) (c) (iII)	Mandatory Reporting	

9	A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform	Article 14 (3)	Single platform is not yet established (Dec 2024)	
10	For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit:	Article 14 (4)	Mandatory Reporting	
11	(a) an early warning notification of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;	Article 14 (4) (a)	Mandatory Reporting	
12	(b) unless the relevant information has already been provided, an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and	Article 14 (4) (b)	Mandatory Reporting	

	corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;			
13	(c) unless the relevant information has already been provided, a final report, within one month after the submission of the incident notification under point (b), including at least the following:	Article 14 (4) (c)	Mandatory Reporting	
14	(i) a detailed description of the incident, including its severity and impact;	Article 14 (4) (c) (i)	Mandatory Reporting	
15	(ii) the type of threat or root cause that is likely to have triggered the incident;	Article 14 (4) (c) (ii)	Mandatory Reporting	
16	(iii) applied and ongoing mitigation measures.	Article 14 (4) (c) (iii)	Mandatory Reporting	
17	After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of	Article 14 (8)	Mandatory Reporting	

	the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.			
18	Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA.	Article 15 (1)	Voluntary Reporting	
19	Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA.	Article 15 (2)	Voluntary Reporting	

Lodging an application for certification

Manufacturers of important or critical software are required to apply for third-party conformity assessments or obtain relevant European cybersecurity certifications, providing extensive documentation to validate compliance with the Cyber Resilience Act. Applications must encompass a clear description of cybersecurity mechanisms integrated within the software, detailed vulnerability handling and remediation procedures, comprehensive test reports validating security effectiveness, and evidence demonstrating rigorous lifecycle management practices. Manufacturers must also present thorough documentation, including a Software Bill of Materials (SBOM), vulnerability assessment reports, and coordinated vulnerability disclosure policies. The documentation must be complete and transparent, facilitating third-party evaluation of the cybersecurity standards throughout the software's entire lifecycle.

ID	Requirement	Reference	Comment	Check
1	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.	Annex VIII, Part II, §1	-	
2	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, and the examination of specimens of one or more critical parts of the product (combination of production type and design type).	Annex VIII, Part II, §2	-	
3	The manufacturer shall lodge an application for assessment of its quality system with the notified body of its choice, for the products with digital elements concerned. The application shall include:	Annex VIII, Part II, §3	-	

4	the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;	Annex VIII, Part II, §3.1	-	
5	a written declaration that the same application has not been lodged with any other notified body;	Annex VIII, Part II, §3.2	-	
6	the technical documentation, which shall make it possible to assess the conformity of the product with digital elements with the applicable essential cybersecurity requirements as set out in Part I of Annex I and the manufacturer's vulnerability handling processes set out in Part II of Annex I and shall include an adequate analysis and assessment of the risks. The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product with digital elements. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex VII;	Annex VIII, Part II, §3.3	-	
7	the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards or technical specifications have not been applied in full. The supporting	Annex VIII, Part II, §3.4	-	

	evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on its behalf and under its responsibility.			
8	The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential cybersecurity requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.	Annex VIII, Part II, §7	-	
9	The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.	Annex VIII, Part II, §10	-	

11.10.4 Developers of open source software

The Cyber Resilience Act (CRA) defines free and open-source software (FOSS) as software whose source code is publicly accessible and distributed under a license that permits users to freely access, modify, use, and redistribute it. This open model fosters transparency, collaboration, and innovation, enabling a broad community of developers to contribute to software security, functionality, and sustainability.

The FOSS community consists of individuals, organizations, and contributors who actively develop, maintain, and govern open-source software projects containing digital elements. Unlike commercial manufacturers, the FOSS community operates on principles of collaborative development and shared responsibility, without direct involvement in marketing, branding, or commercial distribution of products. Their primary focus is on ensuring the long-term sustainability of open-source projects, facilitating contributions, and maintaining software integrity. However, members of the FOSS community may be subject to CRA obligations if their involvement extends into commercial activities, such as integrating open-source software into a monetized product, bundling it with proprietary services, or offering it as a commercial solution.

Furthermore, the CRA applies to the FOSS community only when its activities directly support products “intended for commercial use.” These activities include integrating open-source software into enterprise solutions, offering it as a core component of a monetized service, or providing enhanced versions under paid licensing models. However, the primary role of the FOSS community remains focused on open collaboration, knowledge sharing, and technical contributions, ensuring that free and open-source software remains publicly available and actively maintained. Unlike manufacturers, contributors to the FOSS community do not claim ownership over the software, nor do they derive significant financial gain apart from what is necessary to sustain their projects and infrastructure.

By recognizing the distinct nature of the FOSS community, the CRA seeks to balance cybersecurity regulations with the need to preserve open innovation. While commercially integrated open-source software must meet security requirements, non-commercial open-source projects should retain the flexibility and openness that drive their success.

General requirements

For Free and Open-Source Software (FOSS) developers, compliance with the Cyber Resilience Act requires structured yet adaptable cybersecurity practices. FOSS projects must systematically conduct and document cybersecurity risk assessments reflecting the intended use and foreseeable operational contexts of the software. Projects must proactively handle vulnerabilities, applying clear vulnerability disclosure policies and timely security updates. FOSS software should be designed securely by default, ensuring protection against unauthorized access, data breaches, and integrity violations. Documentation should clearly outline cybersecurity measures, available technical support, and transparent instructions for secure usage, updating, and decommissioning of software, tailored proportionately to the resource limitations and operational characteristics of the open-source development environment.

ID	Requirement	Reference	Comment	Check
1	Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. That policy shall also foster the voluntary reporting of vulnerabilities as laid down in Article 15 by the developers of that product and take into account the specific nature of the open- source software steward and the legal and organisational arrangements to which it is subject. That policy shall, in particular, include aspects related to documenting, addressing and remediating vulnerabilities and promote the sharing of information concerning discovered vulnerabilities within the open-source community	Article 24 §1	-	- Ensure the presence of a clearly documented cybersecurity policy tailored to the unique operational model of the open-source software steward, explicitly covering procedures for vulnerability documentation, assessment, and remediation, aligned with the community-driven nature of the software. - Confirm that a transparent mechanism exists for developers and external contributors to voluntarily report vulnerabilities, ensuring clarity on reporting channels and procedures.

2	Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software. Further to a reasoned request from a market surveillance authority, open-source software stewards shall provide that authority, in a language which can be easily understood by that authority, with the documentation referred to in paragraph 1, in paper or electronic form.	Article 24 §2	-	- Ensure that documentation outlining cybersecurity practices, vulnerability handling processes, and community reporting guidelines is available and maintained in an easily understandable and structured format. - Confirm that, upon request by a market surveillance authority, the documentation can be promptly provided in the requested language, in digital or physical formats, enabling quick assessment and review.

Security attestation of free and open-source software

The FOSS community, under the Cyber Resilience Act (CRA), must provide clear security attestations that transparently document their software's cybersecurity compliance. This attestation should explicitly outline cybersecurity measures incorporated throughout the software's lifecycle, including development, deployment, and maintenance phases. It must provide detailed evidence demonstrating adherence to secure-by-design and secure-by-default principles, systematically addressing known cybersecurity risks and vulnerabilities relevant to the software's intended use and operational environment.

FOSS maintainers must explicitly document their processes for identifying, mitigating, and managing vulnerabilities, alongside maintaining a transparent and publicly accessible coordinated vulnerability disclosure policy. Attestation documents should include a Software Bill of Materials (SBOM) provided in a standardized, machine-readable format, facilitating clear identification and traceability of software components, dependencies, and known vulnerabilities.

Further, FOSS projects must systematically document regular security testing practices, detailing vulnerability assessments, penetration testing outcomes, and corrective measures taken. The attestation must clearly indicate available technical security support, the defined period for security updates, and user guidance on securely configuring, operating, updating, and decommissioning the software.

ID	Requirement	Reference	Comment	Check
1	In order to facilitate the due diligence obligation set out in Article 13(5), in particular as regards manufacturers that integrate free and open-source software components in their products with digital elements, the Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by establishing voluntary security attestation programmes allowing the developers or users of products with digital elements qualifying as free and open-source software as well as other third parties to assess the conformity of such products with all or certain essential cybersecurity requirements or other obligations laid down in this Regulation.	Article 25	As of 12.2024 - no delegated act has been published	
2	For the purpose of complying with paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties so that those components do not compromise the cybersecurity of the product with digital elements, including when integrating components of free and open-source software	Article 13 §5	Requirement for manufacturers	- Ensure a documented and repeatable process is in place to systematically review open-source software components for known vulnerabilities prior to integration, utilizing publicly accessible vulnerability databases or other trusted sources. - Confirm that measures are implemented to track

	that have not been made available on the market in the course of a commercial activity.			and promptly apply security updates or patches for integrated open-source components, clearly documenting such actions to ensure ongoing cybersecurity compliance throughout the product's lifecycle.

Communication with the Authorities

The FOSS community must establish transparent communication channels with cybersecurity authorities in alignment with the Cyber Resilience Act. Contributors and maintainers of open-source projects must promptly report actively exploited vulnerabilities and significant cybersecurity incidents to the relevant CSIRT and ENISA via the standardized reporting platform, adhering to mandatory reporting timelines (initial notification within 24 hours and detailed follow-up within 72 hours, culminating with a full report within 14 days of providing remediation measures).

Furthermore, FOSS projects must clearly define and publicly share coordinated vulnerability disclosure policies, including contact details for responsible disclosure. Community members must ensure continuous communication regarding security vulnerabilities, corrective actions taken, and recommended mitigation steps to maintain trust, transparency, and security effectiveness throughout the software's lifecycle.

ID	Requirement	Reference	Comment	Check
1	The obligations laid down in Article 14(1) shall apply to open-source software stewards to the extent that they are involved in the development of the products with digital elements.	Article 24 §3	-	- Maintain accurate and accessible documentation of cybersecurity practices, vulnerability management, and risk assessments applicable to the contributions.

2	A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA.	Article 14 §1	only applicable if the steward is involved in commercial product development	- Ensure a clear and documented procedure exists enabling immediate identification and classification of actively exploited vulnerabilities, including defined criteria for evaluating exploit activity. - Confirm timely, simultaneous reporting processes are established and operational, enabling immediate notification to both the designated CSIRT coordinator and ENISA upon discovery of actively exploited vulnerabilities, with relevant communication records securely maintained.
3	For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:	Article 14 §2	only applicable if the steward is involved in commercial product development	
4	(a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;	Article 14 §2 (a)	only applicable if the steward is involved in commercial product development	- Confirm the existence of a documented and tested process ensuring notification of actively exploited vulnerabilities occurs within 24 hours, clearly specifying the exact reporting channels to the designated CSIRT coordinator and ENISA.

5	(b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;	Article 14 §2 (b)	only applicable if the steward is involved in commercial product development	- Ensure to maintain a standardized template or procedure for promptly gathering and documenting details about actively exploited vulnerabilities, including product specifics, vulnerability descriptions, exploitation details, and recommended mitigations. - Confirm the capability to submit a complete vulnerability report within the mandated timeframe (24 hours for early warning, and comprehensive details within the subsequent notification), ensuring consistency, clarity, and completeness of reported information to relevant cybersecurity authorities.
6	(c) unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available, including at least the following: (i) a description of the vulnerability, including its severity and impact; (ii) where available, information concerning any	Article 14 §2 (c)	only applicable if the steward is involved in commercial product development	- Ensure manufacturers implement processes to systematically track and document detailed information regarding security updates or corrective measures provided to address actively exploited vulnerabilities, clearly outlining remedial actions and steps for users to follow. - Verify that documentation on active exploitation incidents includes comprehensive information about identified malicious actors (when available), and clearly presents corrective actions,

	malicious actor that has exploited or that is exploiting the vulnerability; (iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.			ensuring the notification is submitted within the regulated timeframe.
7	The obligations laid down in Article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products.	Article 24 §3	-	
8	A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA.	Article 14 §3	only applicable if the steward is involved in commercial product development	- Establish and document clear criteria defining what constitutes a “severe” cybersecurity incident, incorporating parameters such as scale of impact, data compromised, or loss of functionality. - Implement a procedure ensuring immediate notification of severe cybersecurity incidents to the designated CSIRT coordinator and ENISA simultaneously, with records demonstrating timely notifications and responses clearly timestamped and securely maintained.

9	For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit:	Article 14 §4	only applicable if the steward is involved in commercial product development	
10	(a) an early warning notification of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;	Article 14 §4 (a)	only applicable if the steward is involved in commercial product development	- Maintain clear, predefined procedures to rapidly identify and categorize severe incidents impacting product security, facilitating immediate (within 24 hours) reporting that clearly identifies suspicion of malicious involvement.
11	(b) unless the relevant information has already been provided, an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming	Article 14 §4 (b)	only applicable if the steward is involved in commercial	- Ensure a structured process to gather incident details, including initial assessments, clearly documented mitigation steps taken, recommendations for users, and sensitivity evaluations of the information provided.

	aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;		product development	- Utilize a standardized notification format or procedure to promptly and clearly communicate the nature of the incident, mitigation measures implemented, and user actions, verifying compliance with the 72-hour notification window.
12	(c) unless the relevant information has already been provided, a final report, within one month after the submission of the incident notification under point (b), including at least the following: (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures.	Article 14 §4 (c)	only applicable if the steward is involved in commercial product development	- Ensure processes are established and documented to identify and report the root cause or type of threat behind incidents, including comprehensive descriptions of applied and ongoing mitigation measures.

13	For the purposes of paragraph 3, an incident having an impact on the security of the product with digital elements shall be considered to be severe where:	Article 14 §5	only applicable if the steward is involved in commercial product development	
14	(a) it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or	Article 14 §5 (a)	only applicable if the steward is involved in commercial product development	
15	(b) it has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements	Article 14 §5 (b)	only applicable if the steward is involved in commercial product development	

16	After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.	Article 14 §8	only applicable if the steward is involved in commercial product development	

11.10.5 Importers

Importers serve as a vital gateway between non-EU manufacturers and the internal market. Under the Cyber Resilience Act, they play a central role in verifying that products with digital elements, especially those manufactured outside the EU conform to the applicable cybersecurity requirements. By examining technical documentation, confirming proper labeling (including the CE marking where required), and ensuring that manufacturers uphold their obligations, importers help safeguard end users and the broader digital ecosystem from potential security threats.

As part of T2.1's mission to streamline CRA adoption, this section outlines the specific responsibilities and checks importers must conduct to support SMEs and FOSS communities in maintaining a secure and compliant product supply chain.

General requirements

ID	Requirement	Reference	Check
1	Importers shall place on the market only products with digital elements that comply with the essential cybersecurity requirements set out in Part I of Annex I and where the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.	article 19(1)	
2	Before placing a product with digital elements on the market, importers shall ensure that:	article 19(2)	
3	the appropriate conformity assessment procedures (modules A, B, C or H) have been carried out by the manufacturer;	article 19(2) (a)	
4	the manufacturer has drawn up the technical documentation;	article 19(2) (b)	
5	the product with digital elements bears the CE marking and is accompanied by the EU declaration of conformity and the information and instructions to the user in a language which can be easily understood by users and market	article 19(2) (c)	

	surveillance authorities;		
6	the manufacturer has complied with the requirements set out in Article 13(15 - product can be identified with a batch number or similar), (16 - manufacturers' contact information) and (19 - end of support period).	article 19(2) (d)	
7	Importers shall, for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.	article 19(6)	

Product Requirements

ID	Requirement	Reference	Check
1	Importers shall indicate their name, registered trade name or registered trademark, the postal address, email address or other digital contact as well as, where applicable, the website at which they can be contacted on the product with digital elements or on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.	article 19 (4)	

Reporting Requirements

ID	Requirement	Reference	Check
1	Where the importer of a product with digital elements becomes aware that the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer	article 19(8)	

	shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.		
2	Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I as well as of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.	article 19(7)	
4	Importers who know or have reason to believe that a product with digital elements which they have placed on the market is not in conformity with this Regulation shall immediately take the corrective measures necessary to ensure that the product with digital elements is brought into conformity with this Regulation, or to withdraw or recall the product, if appropriate. Upon becoming aware of a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of non-compliance and of any corrective measures taken.	article 19(5)	

3	Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with this Regulation, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with this Regulation. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect. Where an importer has reason to believe that a product with digital elements may present a significant cybersecurity risk in light of non-technical risk factors, the importer shall inform the market surveillance authorities to that effect. Upon receipt of such information, the market surveillance authorities shall follow the procedures referred to in Article 54(2).	article 19(3)	

11.10.6 Resellers / Distributors

Resellers operate as commercial intermediaries, offering CRA-regulated products with digital elements to end users, often without altering or directly importing the products themselves. Under the Cyber Resilience Act, resellers are treated as distributors, meaning they share similar obligations: ensuring that products display the CE marking, include the required user information and documentation, and show no obvious signs of non-compliance.

Case when an economic operator becomes a manufacturer

ID	Requirement	Reference	Check
1	A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of a product with digital elements and makes that product available on the market, shall be considered to be a manufacturer for the purposes of this Regulation.	article 22(1)	
2	The person referred to in paragraph 1 of this Article shall be subject to the obligations set out in Articles 13 (obligations of the manufacturer) and 14 (reporting obligations) for the part of the product with digital elements that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.	article 22(2)	

Reporting Requirements

ID	Requirement	Reference	Check
1	Economic operators shall, on request, provide the market surveillance authorities with the following information:	article 23(1)	
2	the name and address of any economic operator who has supplied them	article 23(1)	

	with a product with digital elements;	(a)	
3	where available, the name and address of any economic operator to whom they have supplied a product with digital elements.	article 23(1) (b)	
4	Economic operators shall be able to present the information referred to in paragraph 1 for 10 years after they have been supplied with the product with digital elements and for 10 years after they have supplied the product with digital elements.	article 23(2)	

12 ACRONYMS AND ABBREVIATION

ABCD — ABOUTCODE EUROPE ASBL
API — Application Programming Interface
CCRA — Common Criteria Recognition Arrangement
CRA — Cyber Resilience Act
CSIRT — Computer Security Incident Response Team
CVD — Coordinated Vulnerability Disclosure
DoA — Description of Action
DSME — European DIGITAL SME Alliance
ECCC — European Cybersecurity Industrial, Technology and Research Competence Centre
ECL — Eclipse Foundation Europe
ENISA — European Union Agency for Cybersecurity
EU — European Union
EUCC — European Cybersecurity Certification Scheme based on Common Criteria
EXP — Expertware SRL
FAQ — Frequently Asked Questions
FOSS — Free and Open Source Software
GA — Grant Agreement
IDE — Integrated Development Environment
IoT — Internet of Things
OSS — Open Source Software
PU — Public (Dissemination Level)
RAL — Red Alert Labs
RP — Reporting Period
SBOM — Software Bill of Materials
SME — Small and Medium-sized Enterprise
STRIDE — Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (Threat Modeling Framework)
PASTA — Process for Attack Simulation and Threat Analysis
WP — Work Package

13 BIBLIOGRAPHY

1. European Commission (2022). *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).* COM(2022) 454 final.
2. European Commission. *Cyber Resilience Act – Implementation Frequently Asked Questions (FAQs).* Available at:https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions
3. European Commission. *Register of Commission Expert Groups – Cyber Resilience Act Expert Group.* Available at: https://ec.europa.eu/transparency/expert-groups-register/
4. European Union Agency for Cybersecurity (ENISA) (2023). *Cyber Resilience Act Implementation via EUCC and its Applicable Technical Elements.* Available at: https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en
5. OCCTET Consortium (2024). *Description of Action (DoA), Grant Agreement No. 101190474.*