CONFIRMATE

CONFormIty assessment, metRics and compliance autoMATion for the cyber resiliencE act

Cyber Resilience Act Compliance Guide for SMEs

Output date: 2025-10-30
Status: Final
Version: 1.0

The project funded under Grant Agreement **No. 101190193** is supported by the European Cybersecurity Competence Centre. 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 Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

List of changes

Version	Date	Description	Author(s)
0.1	07.04.2025	Initial draft	CYEN
0.2	27.06.2025	Additional text added	CYEN
0.3	06.08.2025	First version finalised, additional text / guidance added	CYEN
0.4	03.09.2025	Version reviewed by project partners, to distribute to external peer review	CYEN
0.5	24.10.2025	Revised version considering the peer review	CYEN
1.0	30.10.2025	Final published version	CYEN

Contributors

Role	Contributor's Name	Entity Name - Beneficiary
Deliverable Lead	Iva Tasheva, Steve Purser, Krasimir Simonski, Azeez Kamal	CYEN
Contributor	Christine Demeter, Gabriel Niculescu	DNSC
Contributor	Andreas Binder	AISEC Fraunhofer
Peer Review	Harald Fischer	Balena
Peer Review	Argyro Chatzopoulou et al.	CURIUM Project
Peer Review	Romain Muguet et al.	Red Alert Labs

Disclaimer: Confirmate tools, including the CRA compliance guide, are intended solely for general informational and educational purposes. They provide a high-level introduction to the CRA compliance process and are not tailored to the circumstances of any specific organisation, product, or situation. The content reflects the individual experience and opinions of contributing experts, authors, and peer reviewers, and may not be comprehensive, updated continuously, or applicable to every case.

Nothing in these tools constitutes legal, regulatory, or professional advice. Confirmate does not accept any responsibility or liability for actions taken based on the information provided. Users remain solely responsible for ensuring compliance with applicable laws, regulations, and standards.

Because regulatory requirements evolve, we strongly recommend consulting a qualified legal professional or regulatory expert for advice specific to your circumstances.

Contents

1. Glossary: Acronyms, Terms and Abbreviations

The following terms appear in the text of these guidelines:

Authorised Representative:	A natural or legal person established within the Union who has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks.
CE marking:	A marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential cybersecurity requirements set out in Annex I of the CRA and other applicable Union harmonisation legislation providing for its affixing.
Declaration of Conformity (DoC):	A legal document, drawn by the manufacturer, asserting that a product meets the applicable essential requirements of the CRA. It must be made available to relevant authorities as well as to the users as part of the technical documentation.
Conformity assessment:	The process of verifying whether the essential cybersecurity requirements set out in Annex I of the CRA have been fulfilled.
Harmonised standard:	A technical specification developed by a European standardisation organisation (ESO) at the request of the European Commission to help implement European legislation. These are officially recognised European standards that give presumption of conformity with specific legal requirements in EU legislation.
Incident:	An event that 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 data or functions.
Distributor	A natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties
Importer	A natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a manufacturer established outside the Union

Manufacturer:	A natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge.
New Legislative Framework (NLF):	Regulations that set structured and harmonized requirements for how product conformity is assessed before goods are placed on the EU market.
Product with digital elements (PDE):	A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.
SMEs:	The category of small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million. Respectively, within the SME category, small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million, while for a microenterprise, these thresholds are fewer than 10 employees and less than EUR 2 million.
Software bill of materials:	A formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements.
Support period:	The period during which a manufacturer is required to ensure that vulnerabilities of a product with digital elements are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I of the CRA.
Vulnerability:	Weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat. - An exploitable vulnerability is a vulnerability that has the potential to be effectively used by an adversary under practical operational conditions; - An actively exploited vulnerability is a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner

2. Introduction

About the Confirmate project

CONFIRMATE is an innovative project co-funded by the European Union (EU) and the European Cybersecurity Competence Centre and Network (ECCC), designed to help manufacturing SMEs stay ahead of evolving cybersecurity regulations. By streamlining compliance with the EU Cyber Resilience Act (CRA), CONFIRMATE delivers open-source tools, practical training, and standardized methods that make CRA compliance more accessible, efficient, and cost-effective.

The project's name stands for Conformity Assessment, Metrics, and Automation for the Cyber Resilience Act. Built on the open-source Clouditor framework, CONFIRMATE provides automated service decomposition and compliance views, clear assessment results, a robust penetration testing methodology, multilingual cybersecurity training modules[1], and a comprehensive CRA compliance guide (this document). See published materials in Appendix E.

Bringing together leading partners, including CYEN, Fraunhofer AISEC, ITKAM, and Romania's National Cybersecurity Directorate (DNSC), CONFIRMATE equips SMEs with the knowledge and resources needed to confidently meet essential cybersecurity requirements and ensure the resilience of their digital products. Other EU projects currently running and SME's compliance with the CRA are listed in Appendix F.

2.1 Purpose and target audience of this guide

The compliance guide is a dedicated free resource aimed at supporting EU manufacturing SMEs in understanding the essential cybersecurity requirements of the EU Cyber Resilience Act (CRA)[2]. The guide is specifically designed to provide an overview of the compliance requirements and support SMEs in breaking down its expectations into actionable, easy-to-understand steps. It is tailored to the unique needs and challenges faced by SMEs in the manufacturing sector. Originally drafted in English, it will be translated into four European languages: German, French, Italian, Romanian, reaching over 60% of the EU population.

[1] See the intro video on YouTube: https://youtu.be/QeIjDeVvbL0

[2] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

The guide provides a comprehensive overview of the EU Cyber Resilience Act (CRA), covering key aspects such as roles and responsibilities, essential cybersecurity requirements, conformity assessment procedures, and incident reporting with post-market obligations. It also offers practical steps for SMEs to implement the CRA, along with suggestions for supporting tools, templates, and resources to enhance their security posture and support continuous improvement.

Purpose: The primary purpose of the guide is to empower SMEs by providing them with the knowledge and tools necessary to achieve and maintain compliance with the CRA. It aims to reduce the complexity of navigating regulatory requirements, enabling businesses to confidently meet their obligations while focusing on their core operations. Additionally, the guide serves to highlight the importance to SMEs of managing cybersecurity risks, protecting their reputation, and ensuring the security and trustworthiness of their digital products. Ultimately, it will equip SMEs with the knowledge and practical steps to improve the cyber resilience of their products.

Target Audience: The guide is specifically tailored for European SMEs that develop, produce, or market products with digital elements. These businesses often lack the extensive resources and expertise of larger organisations, making compliance with complex regulations like the CRA a significant challenge. By focusing on SMEs, the guide seeks to address their specific challenges, such as limited budgets, smaller teams, and the need for practical, scalable solutions.

Despite demonstrating an understanding of the above challenges facing SMEs, CRA obligations are the same for SMEs as for large enterprises, with a few exceptions, i.e. simplified documentation templates (Technical documentation and Declaration of Conformity) and priority guidance, which this guide also addresses.

In this sense, unless explicitly mentioned, all guidance in this document applies to SMEs.

In summary, this compliance guide is a valuable resource for EU manufacturing SMEs, offering them clarity, confidence, and practical tools to navigate the requirements of the EU Cyber Resilience Act. It not only supports compliance but also fosters a culture of cybersecurity maturity, helping SMEs protect their products, customers, and reputation in an increasingly digitised market.

2.2 Key Questions and Answers on the Cyber Resilience Act (CRA)

Q1. What is the Cyber Resilience Act (CRA)?

The CRA is an EU regulation aiming to ensure cybersecurity of products with digital elements (PDEs), such as connected devices and software. It introduces mandatory security requirements throughout the product lifecycle, from design to post-sale support.

Although widely recognized, CRA's definition of "products with digital elements, PDE" is worth elaborating in more detail, as it is related to whether SMEs products must meet its requirements.

By definition, PDE includes software or hardware products and its remote data processing solutions. As for software, there is no room for interpretations here, as it is easily recognizable as programming code. But in terms of hardware, there is a clarification that it must be capable of processing, storing or transmitting digital data as well as being placed on the market separately, even if it is a part of a supply chain as a component of another product.

Q2. Does the CRA apply to our products?

If your company manufactures or places products with digital elements on the EU market (e.g., IoT devices, embedded software, industrial machinery with network interfaces), then yes, the CRA likely applies. Exemptions exist for products already regulated, such as medical devices, light-weight vehicles, aviation, products designed exclusively for military, national security, classified information use.

Q3. Am I impacted by the CRA?

If you are a manufacturer, importer, distributor, and open-source steward of a PDE placed on the EU market, then you have specific obligations under the CRA.

Q4. What are the main obligations for manufacturers?

- Conducting and documenting **cybersecurity risk assessments** including supply-chain risks
- Ensuring **secure-by-design** and **secure-by-default** practices
- Implementing **vulnerability handling** processes, including reporting and zero tolerance for actively exploited vulnerabilities that are known by the public.
- Providing **security updates** for the product lifecycle
- **Undertaking conformity assessment procedures** adapted to the product class.
- Creating and maintaining **technical documentation, user information files, EU Declaration of Conformity** (in the languages of the market country)

Q5. When does the CRA take effect?

The CRA will be enforced in a staged approach. Key dates for manufacturers are:

- ➔ **11 September 2026** when the Reporting obligations for vulnerabilities and security incidents become applicable
- ➔ **11 December 2027** when the Full application of the CRA takes place.

Q6. What are the penalties for non-compliance?
Non-compliance can lead to fines up to **€15 million or 2.5% of global annual turnover**, whichever is higher. Market withdrawal and reputational damage are also risks.

Q7. What should manufacturers do now?

- **Map your product portfolio** for CRA applicability
- Start **cybersecurity risk assessments and gap analysis**
- Update **design, technical documentation, and support policies**
- **Consider alignment with cybersecurity standards** (e.g., EUCC, ISO/IEC 2700x, ETSI EN 303 645)

2.3 Background and objective of the Cyber Resilience Act (CRA)

The Cyber Resilience Act comes as a continuation of first horizontal product safety legislation, the Radio Equipment Directive (RED)[3], which introduced the first cybersecurity requirements for a broad range of products sold in the EU, particularly for internet-connected devices and those handling personal data, which become mandatory as from August 1, 2025. These requirements, outlined in Article 3(3) of the RED, aim to enhance the safety and security of users and networks by addressing network protection, data privacy, and fraud prevention. The CRA is also related to the Product Liability Directive (PLD)[4], which addresses liability for defective products, including those with digital elements.

The objectives of the EU Cyber Resilience Act (CRA) are to *'enhance cybersecurity standards of products that contain a digital component, requiring manufacturers and retailers to ensure cybersecurity throughout the lifecycle of their products (...) The Cyber Resilience Act addresses the inadequate level of cybersecurity in many products, and the lack of timely security updates for products and software'*[5]. It aims to establish a consistent and high level of cybersecurity by setting clear requirements for manufacturers, developers, importers and distributors, while also fostering transparency regarding cybersecurity risks.

[3] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053

[4] Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024: https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng

[5] European Commission (2025) Cyber Resilience Act, accessed on April 14, 2025 here: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

'The Cyber Resilience Act will ensure that:

- *Wired and wireless products that are connected to the internet, and software placed on the EU market are more secure;*
- *Manufacturers remain responsible for the cybersecurity of a product throughout its lifecycle;*
- *Consumers are properly informed about the cybersecurity of the products they buy and use.'*[6]

It 'introduces mandatory cybersecurity requirements for manufacturers and retailers, governing the planning, design, development, and maintenance of such products'[7]. These obligations must be met at every stage of the value chain. It emphasizes security-by-design principles, conformity assessments, and the reporting of cyber incidents and actively exploited vulnerabilities, to create a safer digital ecosystem.

The CRA impact is not limited to a specific sector, allowing for a wider impact and setting up a minimum level of acceptable security for products sold across the EU. As such, contributing to a better cyber resilience. For SMEs, in particular, the CRA provides a framework to integrate cybersecurity into their processes, helping them compete in a secure and trustworthy market.

The link and relation between the CRA and other relevant EU safety and security regulations is described in Appendix G Relation to Other EU Legislation.

2.4 Scope and enforcement of the Cyber Resilience Act (CRA)

Scope: The CRA applies to all products with digital elements placed on the EU market (i.e. sold separately, not as a part of a service)*, 'connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules, which is the case for medical devices, aviation and cars. Products will bear the CE marking to indicate that they comply with the CRA requirements.'*[8] The obligations span across the complete lifecycle of the product, from inception, design, production, and maintenance, up until disposal.

It is worth clarifying that if a PDE is not connected directly to a network or another electronic information system, it may still indirectly propagate a threat to a certain target

[6] European Commission (2025) Cyber Resilience Act - Questions and Answers, accessed on April 14, 2025 here: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375

[7] European Commission (2025) Cyber Resilience Act, accessed on April 14, 2025 here: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[8] ibid

by infected files, flash drives, etc. (Recital 9). It could be a standalone device like smart lock, toy, and others (Recital 10).

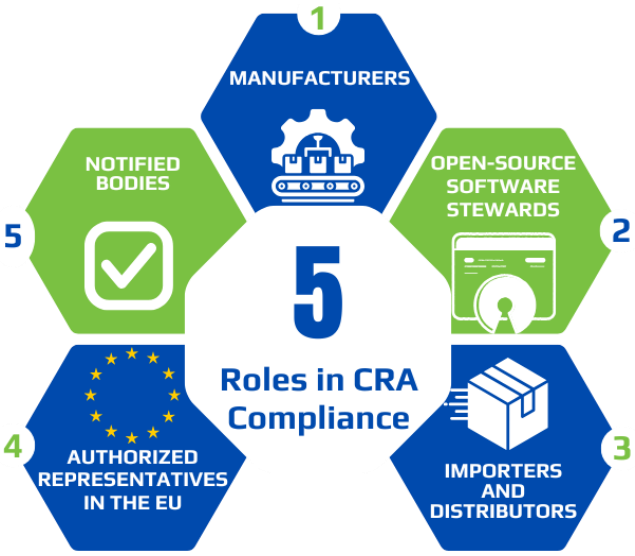
'Based on the New Legislative Framework for product legislation in the EU, manufacturers would undergo a process of conformity assessment to demonstrate whether the specified requirements relating to a product have been fulfilled. This could be done via self-assessment or a third-party conformity assessment, depending on the level of risk associated with the product in question.'[9]

The CRA classifies the products with digital elements into four categories (Default, Important Class I, Important Class II, Critical). All product categories shall implement the same essential cybersecurity requirements (laid down by the Act, which are discussed in section 3 of this document), but assume adequate level of protection according to the risk and need to follow different enforcement (conformity assessment) procedures:

- **Default product with digital elements** are approx. 90% of all products with digital elements. They shall meet essential cybersecurity requirements, asserting that by self-assessment and Declaration of Conformity.
- **Important products with digital elements** are listed in Annex III and divided into two categories - Class I and Class II**.** These products are considered to perform functions critical to the cybersecurity of other products, networks or services and, in this sense, pose a significant risk. In addition to meeting essential cybersecurity requirements, there are stricter cybersecurity verification requirements for them before they are placed on the market.
- **Critical products with digital elements** are listed in Annex IV. Very limited list of products, which are considered the most risky, and they will be required to obtain a European cybersecurity certificate at assurance level at least 'substantial' under a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881.

[9] European Commission (2025) Cyber Resilience Act, accessed on April 14, 2025 here: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

3. Roles and Responsibilities



The CRA obligations target a variety of actors in the supply chain of a product, with no distinction between size or origin, but focused on the role of the legal or physical person with relation to the PDE in scope. Yet, guidance (as laid out in this document) and simplified templates will be published to enable SMEs in particular to fulfil as effectively and efficiently their roles and responsibilities.

CRA defines specific roles and respective responsibilities as follows:

3.1 Manufacturers

The manufacturer plays a major role for the cybersecurity of the products with digital elements at the design, development, production, and support stage. As such, the manufacturer is the leading enterprise profile in the CRA, bearing the full set of responsibilities (i.e. implementing the essential cybersecurity requirements and conformity assessment procedures).

The CRA defines a manufacturer as *'a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge'*.

This definition implies that all stages of a product's life are performed by a single manufacturer who bears all responsibility for the cybersecurity of the product. In practice, as we know, the production line is always much more complex, involving supply chains,

third-parties and other players, which, however, does not lead to shared responsibility. For each stage of the product lifecycle there are specific cybersecurity requirements for each individual activity, stage and operation. The responsibilities of the manufacturer do not even end with placing the PDE on the market.

The obligations of manufacturers (see Table 1) are summarised in CRA Articles 13 and 14 of the official text and are interpreted in the present document.

Obligation	Activity
Implement the CRA essential cybersecurity requirements	When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.
Regular risk assessment	Conduct and regularly update cybersecurity risk assessments for products and the supply chain. Consider the assessment outcomes for the PDE planning, design, development, production, delivery and maintenance with a view to minimise cybersecurity risks, prevent incidents and minimise their impact, including in relation to the health and safety of users. The cybersecurity risk assessment shall indicate how the essential cybersecurity requirements (incl. vulnerability handling) are implemented.
Secure-by-design & default	Ensure products are designed securely and come with secure default configurations.
Vulnerability management	Implement clear processes with zero tolerance for publicly known, actively exploited vulnerabilities.
Security updates	Provide timely, free security updates throughout the product lifecycle, separate from feature updates.
Conformity & CE marking	Carry out conformity assessment (self-assessment or third-party) and apply the CE marking.
Documentation & DoC	Create and maintain technical documentation and the EU Declaration of Conformity (in the languages of the target market).
Reporting	Report actively exploited vulnerabilities and significant incidents with impact on security, simultaneously to CSIRT and ENISA, via the single (EU) reporting platform, as below:
	- Early warning: within 24h
	- Initial report: within 72h
	- Final report: within 14 days (vulnerability) / 1 month (incident)

	Inform the impacted users of the product with digital elements

Table 1: The obligations of manufacturers

Section 3 of this document details the essential cybersecurity requirements laid down by the Act Annex I, summarized here as follows:

- Conducting and documenting **cybersecurity risk assessment** including supply-chain risks**;**
- Ensuring **secure-by-design** and **secure-by-default** practices
- Implementing **vulnerability handling** processes, including reporting and zero tolerance for actively exploited vulnerabilities that are known by the public.
- Providing **security updates** for the product lifecycle
- Undertaking **conformity assessment** procedures adapted to the product class.
- Creating and maintaining **technical documentation, user information files, EU Declaration of Conformity** (in the languages of the county where the product is placed, including the required information. A simplified template of the Declaration of Conformity is available to SMEs can be found in Annex VI of the CRA and Annex I of the current document).

The SMEs recognized as manufacturers should be advised that CRA introduces mandatory reporting of actively exploited vulnerabilities and severe incidents when the manufacturer becomes aware of them. An incident is considered severe when it is caused by or may introduce malicious code or affects the availability, authenticity, integrity or confidentiality of sensitive or important data or functions of the PDE.

Although micro- and small- enterprises are not subject to administrative fines if not meeting the early warning deadline of 24 hours, they are recommended to do that as soon as possible. The reporting obligations are discussed in detail in Chapter 6.

3.2 Open-source software stewards

The role of open-source software steward is very typical for SMEs, as the concept of free and open-source code originates from the SMEs and freelance society and is of a community-driven nature rather than a commercial purpose. Therefore, introduction of obligations to open-source software providers is complicated to be defined when they are part of the supply chain for manufacturing products with digital elements.

The definition of open-source software steward qualifies their PDE as free and open-source software expecting that it is systematically supported on a sustained basis as well as stressing that it is intended for commercial activities.
Providers of open source software are not classified as manufacturers by the CRA unless they engage in commercial activities with open-source software, such as charging for the

software itself, providing technical support for a fee, or monetizing through related services. This is clearly stated in the CRA recital 18: 'only free and open-source software made available on the market, and therefore supplied for distribution or use in the course of a commercial activity, should fall within the scope of this Regulation'.

Although the CRA does not set administrative fines to open-source software stewards, they are subject to a light-weight regulatory regime, with obligations listed in CRA Article 24 and summarised in Table 2 below.

Obligation	Activity
Cybersecurity & vulnerability handling policy	Put in place and document a cybersecurity policy to foster the development of a secure PDE as well as an effective handling of vulnerabilities by the developers of that product, fostering the voluntary reporting of vulnerabilities and sharing of information concerning discovered vulnerabilities within the open-source community.
Cooperation	Cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by free and open-source software products.
Notification	Notify the competent authorities and impacted users (or all users) of actively exploited vulnerabilities (if involved in the development of the product) and severe incidents having an impact on the security of products with digital elements to the extent they affect network and information systems provided by the open-source software stewards for the development of such products.
	Communicate, where necessary, any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident.

Table 2: The obligations of open-source software stewards

Articles 21 and 22 of the CRA treat cases in which the obligations of manufacturers apply to other parties. These guidelines are therefore also relevant in these cases.

3.3 Importers & Distributors

SMEs could be importers or distributors of products with digital elements too. For those roles, CRA sets specific obligations in Articles 19 and 20 respectively, such as to comply with the essential cybersecurity requirements discussed in Chapter 3 below and assume some of the manufacturer obligations.

An importer is defined as *'a natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union'*

A distributor on the other hand is *'a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties'*

Whilst these guidelines have been produced with manufacturers in mind, they can sensibly be used by both importers and distributors as long as the differences in obligations applying to these groups are understood.

Key obligations for both importers (article 19) and distributors (article 20) are summarised in Table 3 below:

Obligation	Activity	Actor	
		Importer	Distributor
Place only CRA-compliant products on the EU market	Refrain from placing on the EU market products that don't comply with the CRA;	✅	✅
Handle non-compliant products	Ensure correction or withdraw / recall if suspecting product non-compliance with the CRA or with its Annex I - Essential Cybersecurity Requirement;	✅	✅
Report	Inform the manufacturer and the market surveillance authorities, without undue delay, in case of a significant cybersecurity risk posed by the PDE;	✅	✅
	Inform the manufacturer about any vulnerability in the product;	✅	✅
	Inform the market surveillance authorities, and to the extent possible, the users, in case the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations under the CRA.	✅	✅
Self-identify	*Place your contact details on the PDE or on the product accompanying documentation, in a language easily understood by users and market surveillance authorities.*	✅	
Keep compliance documents	*Keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities for at least 10 years*	✅	
Ensure	Before placing a product on the market:		
	(a) the appropriate conformity assessment procedures have been carried out[10]*;*	✅	
	(b) the manufacturer has drawn up the technical documentation;	✅	
	(c) the PDE bears the CE marking and is accompanied by the EU declaration of conformity, and the information and instructions to the user as set out in Annex II in a language which can be easily understood by users and market surveillance authorities[11]*;*	✅	
	(d) the PDE or its documentation bears identification of the product, the manufacturer and the support period[12]*.*	✅	

[10] *As set in Article 32*

[11] *As set in Article 30 and Article Article 13(20) accordingly*

[12] *As set in Article 13(15), (16) and (19)*

	The manufacturer and the importer have complied with the obligations, and have provided all necessary documents to the distributor.		✅

Table 3: The obligations of importers and distributors

Moreover, Article 21 identifies circumstances under which obligations applying to manufacturers also apply to importers and distributors. This occurs when the importer or distributor places a PDE on the market under its name or trademark or carries out a substantial modification of a PDE already placed on the market.

3.4 Other natural or legal persons (Article 22)

Article 22 addresses the case where a natural or legal person (other than the manufacturer, the importer or the distributor) carries out a substantial modification of a PDE and makes that product available on the market. In this case, the entity concerned shall be considered to be a manufacturer.

3.5 Authorized Representatives in the EU

Another role in which SME can be recognized is that of an authorized representative of the manufacturer. It is a derivative of manufacturer's role and is defined in a special mandate with which the manufacturer appoints the authorised representative. The mandate may include any of the manufacturer's duties, with the exception of those specified explicitly by CRA in Article 18, which are mostly related to cybersecurity during the design, development and production stages. However, with regard to the CRA requirements for the cybersecurity compliance of the product when on the market, the representative shall cooperate with the authorities exerting control on the PDE they represent.

Manufacturers can choose to appoint an authorised representative to carry out tasks on their behalf - this is done by issuing the representative with a mandate. The authorised representative is obliged to provide a copy of this mandate to the market surveillance authorities if requested to do so.

When the manufacturer chooses to do this, the mandate must allow the authorised representative to do at least the following:

- Keep the EU declaration of conformity and the technical documentation (see section 4 of these guidelines) at the disposal of the market surveillance authorities for at least 10 years after the PDE has been placed on the market or for the support period, whichever is longer;

- If requested, provide market surveillance authorities with all the information and documentation necessary to demonstrate the conformity of the PDE;
- Cooperate with the market surveillance authorities.

3.6 Conformity Assessment Bodies

SMEs could also assume the role of Conformity Assessment Bodies (CABs) which are also referred to as Notified Bodies in CRA. They are independent organizations designated by EU Member States and notified to the European Commission to carry out third-party conformity assessments. They assess whether certain digital products comply with cybersecurity requirements before CE marking can be requested.

CABs are primarily responsible for carrying out conformity assessments in line with the CRA requirements (modules B, C and H) and verifying the corresponding technical documentation. In the case of a successful assessment, the notifying body issues a statement of conformity, which is required to qualify for a CE marking.

Accordingly, Conformity Assessment Bodies must be:

- Accredited and designated under EU rules[13]
- Technically competent in cybersecurity and product evaluation

They are subject to national oversight and EU-level coordination.

[13] NANDO (New Approach Notified and Designated Organisations) Information System https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies

4. Essential Cybersecurity Requirements

4.1 Relating to the properties of products

4.1.1 Secure-by-Design and Secure-by-Default Principles

The CRA requirements to adopt the principle of secure-by-design and secure-by-default, referencing it at several points in the text:

- Recital 32 of the CRA recognises that '*Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679*'[14].
- Recital 34 states that *'When integrating components sourced from third parties in products with digital elements during the design and development phase, manufacturers should, in order to ensure that the products are designed, developed and produced in accordance with the essential cybersecurity requirements set out in this Regulation'*,
- Article 13(1), which details the obligations of manufacturers, requires that *'When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.*'
- Annex I, detailing the essential cybersecurity requirements, requires that *'(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.'*

As an evidence for compliance with the principle of secure-by-design, SMEs may use the risk management plan for product development including risk identification, analysis and mitigation strategies for each development stage.

More explicitly, Annex I point (2)b provides an explicit requirement for a secure default configuration: *'Products with digital elements shall: (b) be made available on the market*

14 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

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.'

These concepts are not defined in the text, and their meaning is assumed to be self-evident. For example, the German Regulator - the Federal Office of Information Security in Germany (BSI)[15] extends by explaining that the CRA security by design principle means that *'connected products must be designed with cybersecurity in mind, e.g. by ensuring that the data stored or transmitted with the product is encrypted and that the attack surface is as small as possible'* and for the security-by-default principle, *'the default settings of networked products must contribute to increase their security, for example, by banning weak default passwords, by installing automatically security updates, etc'*.

What refers to acceptable evidence for compliance with the Secure-by-Default Principle, SMEs should consider documenting the secure configuration enforced rules and if the product is tailor made, to offer an adequate agreement with its business users with relevant clauses.

In practice, the interpretation of these requirements need to be based on the risk assessment and will be at the discretion of the manufacturer, reflecting the nature of the product and the context in which it will be deployed.

4.1.2 Cybersecurity Risk Management

Cybersecurity risk assessment underpins the entire approach to cybersecurity laid out in the CRA, promoting a proactive approach to risk management justifying the cybersecurity measures as opposed to a compliance approach[16]. Risk assessment is a cornerstone of product security, providing a systematic way to identify, evaluate, and prioritize potential threats from the earliest stages of development through the entire product lifecycle. By continuously updating the risk assessment as the product evolves, organizations ensure that security measures remain robust and relevant, effectively protecting both the product and its users. This process not only guides the selection and rigor of security controls but also serves as the foundation for all subsequent security evaluations and decisions. Adhering to established good practices - such as those outlined in ISO 31000 or ISO 14971 - ensures a comprehensive and repeatable approach. Ultimately, risk assessment is not only essential for building secure products, but is also a mandatory prerequisite for regulatory compliance with the CRA and any other EU cybersecurity or safety regulation.

[15] BSI - Federal Office of Information Security in Germany (2025) Cyber Resilience Act, available at: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html#:~:text=Take%20cybersecurity%20into%20account,not%20have%20to%20be%20published., accessed on 21 July 2025

[16] Reference to risk management is also made in Recitals 37, 38, 39, 48 & 52 (referring to Union level coordinated security risk assessment of critical supply chains), 53, 55, 58, 114

Indeed, the CRA itself uses risk assessment techniques to define a number of product classes and to establish security requirements to reflect the level of risk associated with each product class. A risk assessment template is available in Appendix B of this document.

Moreover, risk assessment for PDE under the CRA is a product-specific assessment, going beyond individual project or an organisational risk assessments. To meet CRA requirements, the assessment must specifically address the security of:

- **end users security**, i.e. information and instructions to be provided to the user,
- **evaluate supply chain risks**, including vulnerabilities identified through the Software Bill of Materials (SBOM), 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 and considering the SBOM in the vulnerability management requirements discussed below, and
- **consider how the PDE or its connected devices could impact other** networks and products it interacts with, i.e. product design requirements discussed below.

This comprehensive perspective ensures that not only the product itself, but also its ecosystem and users, are protected from evolving threats, and that security controls are tailored to real-world interconnected risks.

The key references in the CRA text are:

- ➔ Article 3(37) and 3(38) define the concepts of ‘cybersecurity risk’ and ‘significant cybersecurity risk’ respectively.
- ➔ Article 13 provides explicit requirements on how manufacturers should undertake the risk management to ensure an appropriate level of security for their products with Paragraph 13(3) listing the components it shall include at least such as the risk analysis based on PDE intended purpose and reasonably foreseeable use, conditions of use such as operational environment or the assets to be protected and others.
- ➔ Annex I (point 2) establishes a number of essential cybersecurity requirements *on the basis of the cybersecurity risk assessment referred to in Article 13(2).*

4.1.3 Security objectives

Product security is a cornerstone of the Cyber Resilience Act (CRA), requiring organisations to embed robust security measures throughout the entire product lifecycle, from design and development to deployment and maintenance. Key areas include:

- **Identity and Access Management**: Ensuring that only authorized users and systems can access sensitive functions and data, reducing the risk of unauthorized access and misuse;
- **Logging**: Implementing comprehensive logging to monitor activity, detect anomalies, and support forensic investigations in case of incidents;
- **Data Security and Minimisation**: Protecting data at every stage and collecting only what's strictly necessary, which limits exposure and reduces compliance risks;
- **Backup and Secure Erasure**: Regularly backing up critical data and ensuring secure deletion when data is no longer needed, preventing data loss and unauthorized recovery;
- **Encryption**: Safeguarding information in transit and at rest, making data unreadable to unauthorized parties thus maintaining confidentiality.

By integrating these controls across the product's lifecycle, organizations can meet CRA requirements, enhance trust, and protect users from evolving and emerging cyber threats.

Annex I of the CRA, under point (2), lists specific security objectives that must be implemented by the manufacturer, but clarifies that the details of how these mechanisms are implemented will reflect the risk assessment carried out for the product. These control mechanisms include practices, procedures and technical measures - the most important mechanisms are briefly discussed below.

Requirements on the product design

The products shall:

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

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

These design requirements should be taken together with the secure by default configuration requirement.

As evidence of compliance with the above requirements, SMEs should incorporate, implement and monitor comprehensive product risk assessments, map risks to services and controls, assess the design documentation, code reviews, assure separate production and development environments, establish and monitor security baselines to find anomalies, enforce regular backups of software and data.

Measures to detect and eliminate vulnerabilities throughout the product lifecycle

The detection and elimination of vulnerabilities prior to the release of the software is a key requirement of the CRA

Products with digital elements shall:

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

Known vulnerabilities are listed in public vulnerabilities databases, for instance in the EU Vulnerability database[17] or the US National Vulnerability Database[18] or the vulnerability scanning tools (see Confirmate pentesting methodology for further details on vulnerability scanning and management).
When a vulnerability becomes known to have already been exploited for a cyberattack, the manufacturer must take the necessary measures to prevent it from being successfully exploited against the PDE before and after placing it on the market. Many hackers, even with no advanced skills, take advantage of unpatched yet known vulnerabilities by Zero-Day exploits.

(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;

The second part of the essential security requirements is entirely dedicated to vulnerability handling.

Once a vulnerability is identified, it is important to be scored for severity according to an accepted framework such as CVSS (Common Vulnerability Scoring System). Prioritization is done according to this score so that critical and actively exploited vulnerabilities are addressed with urgency. Remediation would typically be accomplished by releasing a patch or configuration change.

Under the CRA, manufacturers have a clear obligation to push these security updates to users without undue delay, using secure update mechanisms and to do so separately from feature updates. Updates must be provided free of charge, accompanied by clear advisory messages and, where feasible, enabled for automatic installation by default. This ensures that users are protected promptly, even if they do not act proactively. Best practice in the industry recommends Service Level Agreements (SLAs) for patch management. For example:

- 24 to 48 hours to patch critical vulnerabilities
- 7 days for high vulnerabilities
- 30 days for medium vulnerabilities

[17] Available at: https://euvd.enisa.europa.eu/
[18] Available at: https://nvd.nist.gov/

- 90 days for low vulnerabilities

Following remediation, continued monitoring is essential. Manufacturers should ensure patches have been effectively applied and monitor for any attempts to exploit any remaining vulnerabilities, this includes analyzing system logs and paying attention to intrusion detection alerts.

Pitfalls to be avoided:

- Delaying remediation until functionality updates
- Underestimating the severity of vulnerabilities
- Failing to inform users in a timely and understandable way.

Additionally, rushing patches without proper testing can introduce new issues or risks. Therefore, by combining prompt remediation, patch deployment and continuous monitoring, SMEs can establish a strong vulnerability management process that meets the CRA's essential cybersecurity requirements.

Recommended evidences to demonstrate compliance with the above requirements besides development and enforcement of relevant policy and procedures could include penetration tests (internal and by third-party), automatic security update mechanisms, code reviews, and most importantly, relevant (even proactive) updates in a timely manner, should a new threat or vulnerability become known, even if not exploited yet.

Technical requirements

Examples of typical measures to fulfill the CRA technical requirements are listed in all information security standards, including NIST SP800 or Cyber Fundamentals (CyFun) in their respective topic: Protect. Examples of specific measures are given below.

(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;

Relevant NIST Cybersecurity Framework recommended measures include:

- Require multifactor authentication;
- Enforce policies for the minimum strength of passwords, PINs, and similar authenticators;
- Periodically reauthenticate users, services, and hardware based on risk (e.g., in zero trust architectures);
- Ensure that authorized personnel can access accounts essential for protecting safety under emergency conditions.

(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;
Relevant Cyber Fundamentals guidance as measures include:

- Consider using encryption techniques for data storage, data transmission or data transport (e.g., laptop, USB);
- State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

Similar guidance could be found in other relevant standards:

(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;
(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);
(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

It is important to note that the CRA identifies WHAT needs to be done, but not HOW it should be done. The way in which these requirements are implemented is entirely at the discretion of the manufacturer although there is a clear expectation that the methods adopted are commensurate with the level of risk associated with the product.

SMEs could demonstrate compliance with the above requirements by empowering its products with digital elements with log functionalities allowing them to be integrated within the cybersecurity environment of their business users. The integration should also consider compatibility with centralized access control, regularly tested including penetration tests, and not the least - advanced cryptography.

Specific security measures for the SME to consider, at minimum, to satisfy the above requirements, include:

- Adopt identity, access control, authorisation, incident management policies and procedures.
- Implement dedicated safeguards to prevent unauthorized access, distortion, or modification of system data and audit records (e.g. restricted access rights, daily backups, data encryption, firewall installation).
- Implement integrity detection and reporting mechanisms.
- Activate multifactor authentication.

- Enforce policies for the minimum strength of passwords, PINs, and similar authenticators.
- Implement DDoS detection and response mechanisms.

Measures to minimise impact on the IT environment

There are two requirements that aim to minimise the impact of an incident or malfunction of the product on its environment, namely point (i) and (k) described below:

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

This requirement imposes that PDEs are not only secure for their account but also do not pose a threat to the availability of other devices or networks. It is similar to the Radio Equipment Directive, where devices are not to 'interfere with other devices or networks', requiring equipment to efficiently use the radio spectrum and meet electromagnetic compatibility standards, preventing harmful interference. Applied in cybersecurity, we could advise that PDEs are designed carefully to avoid excessive data, CPU or network consumption, for example, and have check points to avoid being used for a denial of service attack. In a Denial of Service attack, compromised PDEs could enter an army of bots (compromised devices), attacking simultaneously a network, website or application, taking down the product or network under attack.

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

Specific security measures for the SME to consider, at minimum, to satisfy the above requirements, include:

- Conduct a comprehensive product risk assessment since its inception phase, including considerations on the potential risks on the availability of services provided by other devices or networks due to the PDE or connected devices, and identifying mitigating measures to reduce the risk impact or probability.
- Implement dedicated safeguards to prevent unauthorized access, distortion, or modification of system data and audit records (e.g. restricted access rights, daily backups, data encryption, firewall installation).
- Implement DDoS detection and response mechanisms.

User-related controls

Additional two measures aim at empowering the user to manage its own security and data:

(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;

The techniques for detection of abnormal behavior indicating a cyberattack are mostly based on reviewing and analyzing logs of the products with digital elements in order to determine the type and vector of the attack and take appropriate measures to respond. This is usually done with automated tools for collecting and correlating logs, for which the products with digital elements must have the supporting functionality for recording and monitoring its activities.

(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.

Secure data removal techniques are diverse, according to the type of carrier (paper, drive, cloud) or sensitivity level (from generic data to customer history).

Specific security measures for the SME to consider, at minimum, to satisfy the above requirements, include:

- Integrate supporting functionality for recording and monitoring PDE activities.
- Integrate secure delete and data transfer functionalities, and an opportunity for the user to launch the process in an easy way.
- Use methods like full memory overwrite, encryption-based wiping, zero-fill, hardware-level deletion, or even physical destruction to ensure data is truly unrecoverable. It is crucial to identify all stored secrets before erasure, validate that data is gone, and revoke device certificates during the process.

CRA supposes that hackers may obtain important (or even confidential) information for planning their attacks, which they can extract from PDE to which they gain access after they are thrown out of use or replaced with others unless there is a secure mechanism for securely destroying the old data and sanitizing abandoned data storage.

4.2 Supply Chains and Third Parties Security

Manufacturers are responsible for the cybersecurity of the entire product they manufacture, including any embedded or integrated third-party components, such as software libraries, open-source modules and firmware. In particular, manufacturers must assess and manage risks originating from the supply chain, and must verify that third-party software complies with CRA requirements.

In practice, this means that any responsibility imposed on the manufacturer, must also be expected from the corresponding supply chain if it has an impact on the final product. Examples of expectations include but not limited to:

- Security by design and default;
- Extended length of support period (must be compatible with that of the final product);
- Vulnerability handling and disclosure;
- Incident handling (in as far as there is an impact on the manufacturer's product).

As a consequence, manufacturers will be expected to exercise due diligence in selecting suppliers and other third-party contributors to their products.

As part of this activity, manufacturers must maintain and provide a Software Bill of Materials (SBOM), listing all software components used, including third-party and open-source dependencies. The SBOM must be:

- Available in a machine-readable form upon request to customers and market surveillance authorities;
- Kept up to date and reflect all modifications throughout the product lifecycle.

Further details on the format (e.g. JSON) and elements (information) of the SBOM may be provided by the European Commission in the form of an Implementing Act.

In parallel, an insight of best practices and minimum requirements is provided by the US Cybersecurity and Infrastructure Security Agency (CISA) in its draft August 2025 Minimum Elements for a Software Bill of Materials (SBOM).

For SMEs manufacturing products covered by CRA, these evolving SBOM requirements from CISA shed light on the technical aspects and standards for SBOM maintenance. But the CISA details also introduce nontrivial operational complexity.

4.3 Vulnerability Management

Part II of the essential security requirements (Annex I of the CRA) deals with vulnerability handling requirements. There is some overlap here with the requirements of part I (e.g. the requirement that products with digital elements be made available on the market without known exploitable vulnerabilities). However, most of the requirements listed in this part of the annex are policy and procedure oriented and are explicitly targeting vulnerability management.

4.3.1 Identification & documentation

(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;

The requirement for producing a Software Bill of Materials (SBOM) is obligatory. Further information on how the concept of the SBOM relates to the CRA can be found in recitals 77, 118 and articles 13(24) of the CRA.

As discussed above, at the time of writing, there is no imposed format for such a document, nor indeed is there an accepted standard format, although article 13(24) enables the Commission, by means of implementing acts taking into account European or international standards and best practices, to specify the format and elements of the SBOM.

In addition, the manufactures shall *(3) apply effective and regular tests and reviews of the security of the product with digital elements;*

Here it is important to note that requirement (3) is to set up a comprehensive and periodic process of testing and reviewing, for both technical and organisational vulnerabilities and mis-configurations, irrespective of whether a vulnerability has been discovered or not.

4.3.2 Remediation

The PDE vulnerabilities need to be addressed or remediated without delay. This is needed to ensure that the product remain secure while on the EU market. In addition, the CRA specified that, where feasible, new security updates shall be provided separately from functionality updates. This could help address the difference in timing between product development and security maintenance.

4.3.3 Vulnerability disclosure & information sharing

There are three key requirements in this area:

(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;

Requirement (5) refers to coordinated vulnerability disclosure, which has a specific meaning in this context. The idea behind coordinated vulnerability disclosure (CVD) is fully described by ENISA[19]. In essence, CVD is a set of rules (e.g. policy) published by a manufacturer that allows external security experts with good intentions (could be 'ethical hackers' or vulnerability scanning services) to identify potential vulnerabilities in its systems or products, and provides a procedure (form, channel, contacts) to report the identified security weaknesses to the manufacturer. The CVD usually defines which systems fall in scope, under which condition the identification could be done (no law is breached, no harm is done, no data is leaked).

4.3.4 Managing security updates

The final requirements of part II deal with the management of security updates, ensuring that the remediation (security updates) discussed above is feasible through *mechanisms to securely distribute updates* for PDEs.

Furthermore, the security updates are to be free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken. All these with the objective to enable the users of PDEs to keep their products secure and take the necessary risk mitigation actions, when needed.

5. Conformity Assessment

5.1 Conformity assessment procedures

The conformity assessment procedures adopted by the CRA are based on the NLF[20] and circle around the principle of high-risk = high-assurance. Namely, default categories (not specifically referenced in the Regulation) are subject to self-assessment procedures, the Important I is based on harmonised standard or third-party assessment, Important Class II and Critical product are subject to third-party assessment and certification accordingly. The specific required for which classes of products - this is summarised in the following table. Detailed description of the Conformity Assessment procedures is available in the

[19] https://www.enisa.europa.eu/topics/vulnerability-disclosure

[20] The NLF (New Legislative Framework) clarifies the use of CE marking and creates a toolbox of measures for use in product legislation. The NLF consists of: Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products, Decision 768/2008 on a common framework for the marketing of products, which includes reference provisions to incorporate in product legislation revisions. In effect, it is a template for future product harmonisation legislation, Regulation (EU) 2019/1020 on market surveillance and compliance of products. For further details, please see the European Commission website: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

'CRA conformity process' chapter of the **CONFIRMATE D3.1 – Architecture for Automated CRA Conformance Assessment**, in CRA conformity process. The requirements are set out in article 32 of the Act. Annex VIII provides a detailed description of the conformity assessment procedures themselves.

The CRA recognizes and relies on the conformity procedures presented below.

5.1.1 Harmonised standards. These are officially recognised European standards that give presumption of conformity with specific legal requirements in EU legislation. These serve as prescriptive, auditable baselines for risk management, secure development and operational security.

These standards are still to be developed and recognized officially to presume conformity with the essential cybersecurity requirements. In February 2025, the EU Commission tasked the European Standardisation Bodies (CEN, CENELEC, ETSI) with developing 41 standards: 15 horizontal, which apply broadly to all PDEs, and 25 vertical, which are tailored to specific product types and risk classes. Horizontal standards address general security (Type A) and vulnerability requirements (Type B), while vertical standards provide detailed guidance for specific products, e.g. browsers, IoT devices (Type C), influencing whether manufacturers can self-assess or require third-party compliance, with the most sensitive standards developed under restricted conditions. A complete list of the standards can be found on the CEN/CENELEC web site[21].

The planning for the delivery of these standards is to deliver Type A standards and Type B standards for vulnerability handling by 30.08.26, all Type C standards by 30.10.26 and the remaining Type B standards by 30.10.27.

In addition to the harmonised standards directly supporting CRA compliance, manufacturers are encouraged to make use of leading industry standards when implementing the CRA requirements. Notable examples are listed in Appendix C.

5.1.2 Common specifications (adopted by EC Implementing Act) are detailed, practical guidelines from the European Commission to help manufacturers meet specific cybersecurity requirements, in the absence of harmonised standards or for areas not sufficiently addressed in a published harmonised standard, serving as a fallback option in such cases.

5.1.3 Certificates issued under a European cybersecurity certification scheme.

[21] Available at: https://www.cencenelec.eu/media/CEN-CENELEC/News/Newsletters/2025/m_606_work_programme_final.pdf

The key EU Certification Scheme that will support the CRA compliance is the EUCC (European Common Criteria). The EUCC is a voluntary-based Europe-wide cybersecurity certification scheme that allows for the certification of ICT products such as technological components (chips, smartcards), hardware and software. Building upon the existing twenty-years+ SOG-IS Common Criteria evaluation framework, it serves as a continuation and expansion (from 17 EU member states now to all 27 to adopt it). It proposes two levels of assurance based on the level of risk associated with the intended use of the product, service or process, in terms of probability and impact of an accident.
The European Commission has centralised all documents and guidance linked to EUCC[22]. Opting for a EU cybersecurity certification as a conformity assessment procedure brings the advantage of presumption of conformity with the CRA, even for high-risk categories, and enhances market credibility and customer confidence.

The EU Cybersecurity Act (EU 2019/881) sets up a shared framework for certifying cybersecurity across the EU. Under the Cyber Resilience Act (CRA), this framework becomes especially important for products that carry higher risks, those classified as **Important Class II** or **Critical** in Annex VIII. For these product classes, certification can serve as formal evidence of meeting 'substantial' or 'high' assurance levels.

5.2 Minimal required conformity assessment procedures

SMEs should meet at least the minimal required procedures set out in the CRA for their product category as explained in the Confirmate D3.1 – Architecture for Automated CRA Conformance Assessment document[23] **OR** any other more demanding procedure. The more demanding the assessment procedure is chosen, the more secure and trusted the PDE appears on the market, which could be a significant competitive advantage. For instance, if the PDE falls into the Default category, then the minimal required procedure is Module A, but the SME may choose any of the other more demanding procedures below. If a PDE is in Important Class I, then its manufacturing SME could self-assess against the harmonized standards for its product type if available, or if not available, then choose the next more demanding procedure – Module B+C or Module H. If a PDE is listed in Important Class II, then the minimal required procedures are two: “Module B+C” or Module H, both demanding third-party assessment.

[22] Available here: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en
[23] Available at https://confirmate-project.eu/materials/

The procedure options for specific products are summarised in the below table, with each check mark showing an option for the given category:

Type / product category	Default	Important class I	Important class II	Critical
Self-assessment (Module A – Internal Control)	✓			
Self-assessment against EU harmonised standard, common specifications (Module A – Internal Control)	✓	✓		
CAB assessment of design + Self-assessment of production (Module B+C)	✓	✓	✓	
Full CAB quality assurance (Module H)	✓	✓	✓	
EU cybersecurity certificate (CSA) at level 'substantial' or 'high'	✓	✓	✓	✓

Exception is made for open source products: *'Manufacturers of important products with digital elements qualifying as free and open-source software should be able to follow the internal control procedure based on module A, provided that they make the technical documentation available to the public'* (CRA recital 91).

5.3 CE marking and technical documentation

5.3.1 CE marking

The CE marking is defined in the CRA as: '*marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential cybersecurity requirements set out in Annex I and other applicable Union harmonisation legislation providing for its affixing'*

In general, the CE marking is required to attest to the fact that a product meets all applicable EU cybersecurity and safety requirements. In the context of the CRA, the CE marking should only be applied after (a) completing the relevant conformity assessment procedure and (b) drafting and signing the EU declaration of conformity.

The CE marking is subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008. The CE marking should be displayed visibly, legibly, and indelibly on the product and packaging or on the accompanying documentation (if physical marking is not possible).

Important note: *Not all products must have CE marking. It is compulsory only for most of the products covered by the New Approach Directives. It is forbidden to affix CE marking to other products. Please note that a CE marking does not indicate that a product has been approved as safe by the EU or by another authority. It does not indicate the origin of a product either*[24]*.*

[24] *See ful text and all CE mark format options at the European Commission website: https://single-market-economy.ec.europa.eu/single-market/goods/ce-marking_en*

5.3.2 Technical Documentation

Manufacturers are required to prepare and maintain technical documentation (as set in Annex VII of the CRA), demonstrating product compliance. This is mandatory for both self-assessment and third-party evaluation.

This documentation must include:

- General product description
- A description of the design, development and production of the product
- Initial and updated risk assessments
- Relevant information that was taken into account to determine the support period
- A list of the harmonised standards applied in full or in part to the product
- Test reports, inspection results, and standards applied
- Description of the conformity assessment procedure used
- A copy of the EU Declaration of Conformity
- Where applicable, the software bill of materials

For SMEs, an option for a simplified form of the Technical documentation will be made available in a Commission implementing regulation that is still to be published at the time of drafting this guide.

5.4 Declaration of conformity

The Declaration of Conformity (DoC) is a legal document asserting that a product fulfills the applicable essential cybersecurity requirements set out in Annex I of the CRA. It is drawn by the manufacturer after having successfully completed the appropriate conformity assessment procedures, must be signed by an authorized representative and made available to national market surveillance authorities.

The DoC should contain:

- Manufacturer’s name and address
- Product identification
- A statement of compliance with the CRA
- A list of relevant standards and conformity procedures used
- Reference to the EU-type examination (if applicable)
- Signature, date and contact details of the responsible person

The contents of the declaration of conformity are listed in Annexes V and VI of the CRA.

6. Reporting and Post-Market Obligation

6.1 Reporting obligations

In compliance with Article 14, SMEs are required to report both; 'actively exploited vulnerabilities' and 'severe incidents'. These are defined as follows:

- An Actively exploited vulnerability is a security flaw already used or under active malicious attack.
- A severe incident is an event impacting the product's confidentiality, integrity, availability, including malware introduction.

Article 14 of the CRA further describes a severe incident as an incident which (a) negatively affects or is capable of negatively affecting the ability of a PDE to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions, OR (b) has led or is capable of leading to the introduction or execution of malicious code in a PDE or in the network and information systems of a user of the product.
The reporting requirements for these two types of events differ as explained in the following sections. Details can be found in Article 14 of the CRA.

Besides the mandatory reporting of any actively exploited vulnerability and severe incident, CRA assumes voluntary reporting for any other incident or threat to the PDE too. The same procedure of reporting simultaneously to CSIRT and ENISA via the Single Reporting Platform applies.

6.2 Reporting procedure

All mandatory notifications are to be submitted through the future Single Reporting Platform[25] to ENISA and simultaneously to the CSIRT of the manufacturer's main EU establishment. Once the Single Reporting Platform (see below) is available, this will be achieved via a single notification to the platform.

Actively Exploited Vulnerabilities

The reporting of actively exploited vulnerabilities occurs in three separate steps:

- Step 1: Early-warning within **24 hours** of awareness. Where applicable, the Member States where the product has been made available should be identified at this stage.
- Step 2: Initial vulnerability report within **72 hours** of awareness, including:

[25] See article 16 of the CRA: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

- general information about the product, the nature of the exploit and the vulnerability concerned.
- Any corrective or mitigating measures taken, and corrective or mitigating measures that users can take.
- An assessment by the manufacturer of the level of sensitivity of the notified information

- Step 3: Final report no later than **14 days** after a fix's availability, including:
  - A description of the vulnerability, including its severity and impact;
  - Where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;
  - Details about the security update or other corrective measures that have been made available to remedy the vulnerability.

Severe Security Incidents

The reporting of severe security incidents also occurs in three separate steps, the essential difference being in the final step.

- Step 1: Early-warning within **24 hours** of awareness,including:
  - An opinion on whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate.
  - Where applicable, the Member States where the product has been made available.
- Step 2: Incident report within **72 hours** of awareness, including:
  - The nature of the incident
  - An initial assessment of the incident
  - Any corrective or mitigating measures taken, and corrective or mitigating measures that users can take
  - An assessment by the manufacturer of the level of sensitivity of the notified information.
- Step 3: Final report within **1 month** after the 72-hour notification, including:
  - A detailed description of the incident, including its severity and impact;
  - The type of threat or root cause that is likely to have triggered the incident;
  - Applied and ongoing mitigation measures.

User notification

For both types of incident, once aware of either vulnerability or incident, manufacturers must inform affected (and where appropriate all) users without delay, including risk mitigation advice in an easily automated, machine-readable format. If manufacturers fail to notify, the CSIRT may step in to inform users.

Voluntary reporting

Outside the scope of their notifying obligations, pursuant to Article 15, manufacturers are encouraged to voluntarily report any vulnerability and threat that may affect the cybersecurity of a PDE. Respectively, notifying incidents that are not severe is voluntary too.

This voluntary reporting mechanism could introduce a good practice for SMEs with an indirect positive effect for the manufacturer and its customers, increasing visibility on the threat and thus, preventing further incidents. In addition, where it is difficult to assess exactly whether a particular vulnerability is actively exploited, or an incident is severe, voluntary reporting seems to be the safe option.

6.3 Cooperation with EU & national Authorities

6.3.1 ENISA and CSIRTs on Vulnerability Handling

Manufacturers report actively exploited vulnerabilities and severe incidents to ENISA and the national CSIRT according to the provisions set out in Article 14 of the act. The requirements on the manufacturer are presented in section 5.2 of these guidelines.

6.3.2 National Market Surveillance Authorities

Market surveillance authorities are responsible for enforcing CRA obligations in each county. The way in which this applies to the CRA is explained in chapter V of the CRA.

The consequences for manufacturers are that they are obligated to:

- Cooperate during investigations, audits, and inspection;
- Provide documentation (e.g. SBOM, risk assessments, technical files) upon request;
- Inform MSAs of non-compliance and corrective measures, if applicable.

7. The steps for SMEs to implement the CRA

7.1 Initial Scope and Gap Assessment

The first step towards CRA compliance is to develop a clear understanding of what products fall within the scope of the CRA, what is the role of the organisation with relation the products in scope, and what requirements the products comply and do not comply with. This is achieved by performing a scope and gap assessment.

This document, together with the tools provided by the Confirmate project are there to support the initial analysis: scope, role identification, gap assessment and to monitor improvements over time as the non-compliant requirements are addressed by the organisation. In this sense, the gap assessment should be considered as a 'living document' in the sense that it should be updated on a regular basis to reflect progress made. In this way, the assessment will be an accurate reflection of where the organisation stands with respect to compliance at all times.

7.2 Developing an Implementation Plan

The implementation plan can be developed once the initial gap assessment has been carried out. Like the assessment itself, the plan should be considered as a document that evolves with time and takes account of lessons learned as the implementation project proceeds.

Where planning is concerned, the recommendation is to follow a 'rolling wave' approach, where activities for the next three months are planned to a high level of detail and activities beyond this are estimated on a best effort basis. Putting too much detail into plans that reach far into the future may be counter-productive as long-term activities tend to be modified to reflect lessons learned during the earlier phases of a project.

In all cases, should it not exist, the performance of a risk assessment should be prioritised as the results of this assessment will justify planned and implemented measures, and will allow the organisation to prioritise risks as efficiently as possible.

Where short-term planning is concerned, the recommendation is to keep activities simple, to have clear deliverables for each task and to keep the length of time allocated to any individual activity as short as possible. This avoids the problem of tasks that are always 90% finished, but never seem to get to 100%.

Last but not least, SMEs can take full advantage of resources developed specifically to support their compliance with the CRA under the Digital Europe Programme: our Confirmate project tools, referred in Appendix E and other projects, listed in Appendix F, as well as EU and National Support Resources for SMEs listed in Appendix D.

7.3 Staff Training and Awareness

Training and awareness programs are a key component of the plan to achieve compliance. Whilst every effort has been made to simplify the requirements of the CRA in these guidelines and in the accompanying tools, it is extremely important that staff develop and maintain a thorough understanding of the CRA and related policies.

Further guidance, tools and templates that SMEs could use in implementing essential security requirements and complying with the documentation requirements are listed in Annexes. The use of these resources is not mandatory, except for the Sample of Declaration of Conformity, but should be considered in the context of an organisation-wide plan.

8. Timelines and Transition Periods

The key dates in the implementation timeline for the CRA are as follows:

Date	Event
11.12.24	The CRA enters into force
11.06.26	Obligations for notifying conformity assessment bodies applicable[26]
30.08.26	Deadline for Type A standards and Type B harmonised standards for vulnerability handling
11.09.26	Reporting obligations for vulnerabilities and security incidents become applicable.
30.10.27	Deadline for remaining Type B harmonised standardised
11.12.27	Full application of the CRA

[26] This is an obligation on Member States and not on manufacturers

Appendix A: Simplified EU Declaration of Conformity

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: ...

Appendix B: Risk Assessment Template

The ENISA Interoperable EU Risk Management Toolbox provides a harmonised and EU-recognised methodology for this purpose. It is designed to support consistent implementation of risk management across the EU, incorporating ISO/IEC 27005, NIS2 and sector-specific practices. Note however that this toolbox was not specifically designed to meet the requirements of the CRA, but is to be considered as a general purpose tool covering many different application areas.

The toolbox includes standardised templates and guidance for:

- Asset identification and valuation
- Threat and vulnerability analysis
- Risk estimation and evaluation
- Definition of risk treatment and mitigation actions
- Integration with security controls required under CRA Annex I[27]

It supports both qualitative and semi-quantitative assessments and is interoperable with national and international methodologies. Use of this toolbox enables consistency, auditability and full traceability of security decisions in support of conformity assessments and technical documentation under the CRA.

[27] Note that this is not an explicit mapping to the controls of the CRA.

Appendix C: Relevant Standards

- ETSI TS 103 701, Annexes B & C can be used for structuring audit-ready technical documentation using ICS/IXIT templates
- **ISO/IEC 27001** - Information Security Management System (ISMS)
- **ISO/IEC 27701** - Privacy Information Management System (PIMS)
- ETSI EN 303 645 - Baseline Security Requirements for Consumer IoT, where Clauses 4–5 can be used for defining baseline security requirements
- **OWASP ASVS** – Application Security Verification Standard
- **CIS Benchmarks** - Secure Configuration Guidelines
- **IoT Security Foundation Guidelines** – IoT Device Security Best Practices
- **NIST SP 800-53** - **Security and Privacy Controls for Information Systems and Organizations.**
- **NIST SP 800-37** - Risk Management Framework (RMF), providing a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle.
- **The NIST Cybersecurity Framework (CSF)**, providing guidance on managing cybersecurity risks
- **IEC 62443 / ISA-62443** - Industrial Automation and Control Systems Security Standards
- **ISO 9001** - Quality Management System
- **CMMC** - Cybersecurity Maturity Model Certification
- **GDPR** - General Data Protection Regulation

Appendix D: EU and National Support Resources for SMEs

The European Commission, the EU Cybersecurity Agency (ENISA) and the European Cybersecurity Competency Centre (ECCC) all publish reports on cybersecurity, many of which provide guidelines that could be of use to SMEs implementing the CRA.

In particular, the Guidelines for Securing the Internet of Things (IoT)[28] sets the complete lifecycle security requirements, incl. from requirements and design, to end use delivery and maintenance, as well as disposal. The study is specifically developed to help IoT manufacturers, developers, integrators and all stakeholders that are involved to the supply chain of IoT to make better security decisions when building, deploying, or assessing IoT technologies.

In addition, the ENISA SME Cybersecurity Guide is tailored guidance for improving the cybersecurity of small organizations, including manufacturers.

At the national level, the mission of the National Cybersecurity Competency Centres is to boost research excellence and the competitiveness of the Union in the field of cybersecurity. A list of the centres has been published by the European Cybersecurity Competency Centre (ECCC)[29].

In addition to the competency centres, many EU member states have created a national cybersecurity agency. Whereas the competency centres concentrate on research and innovation, the cybersecurity centres tend to cover all aspects of cybersecurity (although detailed mandates differ between member states). Examples include:

- **Belgium**: CCB - Centre for Cybersecurity Belgium
- **Germany**: BSI – Federal Office for Information Security
- **France**: ANSSI – Agence nationale de la sécurité des systèmes d'information
- **Italy**: ACN – Agenzia per la Cybersicurezza Nazionale
- **Romania**: DNSC – Directoratul Național de Securitate Cibernetică

Last but not least, industry and professional organisations create resources to support their constituencies' understanding and compliance with the CRA. For instance, the Digital SME Alliance, ECSO (at the EU level) and Agoria,

[28] Available at: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[29] Available at: https://cybersecurity-centre.europa.eu/nccs-0_en

Appendix E: CONFIRMATE tools

Below is a short overview of the other guidance, training, tools and documentation, accompanying this document. All project materials are available on www.confirmate-project.eu/materials.

Part 1 Guidance and Methodologies

Pentesting methodology: developed and peer-reviewed document that aim to support SMEs in preparing for and completing an effective PDE pentesting aligned with the Cyber Resilience Act (CRA) requirements. Based on industry standards, it aims to summarize and provide an essential guide of what is needed and what could be expected as an outcome of a product Pentest, taking into consideration specific products, falling within a range of CRA categories.

D3.1 - Architecture for Automated CRA Conformance Assessment: detailed and comprehensive overview of the CONFIRMATE framework, outlining its intended functionality and structure clearly and methodically. The document introduces and clearly defines the conformity assessment process as stipulated by the CRA, offering readers foundational context on regulatory requirements. Subsequently, the deliverable illustrates precisely how end-users will engage with and benefit from the CONFIRMATE framework throughout their CRA conformity assessment processes.
Following the user-oriented description, the deliverable specifies the envisioned software architecture, detailing essential elements such as key components, modular divisions, and the interactions among these elements.

D2.2 - Evidence Data Model: a foundation for automatically collecting and assessing technical evidence across technologies, ensuring that the necessary information is efficiently captured and organized. By leveraging machine-readable formats, the model facilitates the integration of evidence into automated compliance tools, reducing the manual effort required for documentation and enhancing the accuracy of conformity assessments. Note, however, that this approach does not guarantee complete compliance with the CRA as some of the requirements are not transposable into automatic data collection methods. The evidence data model also enables and aligns with the creation of respective metrics, which are derived from the essential requirements of the CRA. These metrics provide quantifiable measures of compliance.

Part 2 Open-source automated compliance assessment tool

Confirmate proposes an open-source automation tool that streamlines CRA cybersecurity essential requirements conformity assessment by listing all essential cybersecurity requirements and metrics, automatically comparing security settings with CRA

specifications, and determining individual needs for action. Its intuitive dashboards and structured capabilities help organisations quickly identify the CRA essential cybersecurity requirements implemented and those to assess or to implement, saving valuable time in compliance checks while providing clear, actionable insights for continuous compliance and improvement.

In addition, documentation tools such as the:

- D2.2 – Evidence Data Model, enabling the automation of compliance verification through a structured approach to evidence collection and assessment.
- D3.1 – Architecture for Automated CRA Conformance Assessment, a document providing a detailed and comprehensive overview of the CONFIRMATE framework, outlining its intended functionality and structure, introducing the conformity assessment process and illustrating how end-users will engage with and benefit from the CONFIRMATE in the CRA conformity assessment process.

Part 3 CONFIRMATE trainings and workshops

The list is a living document, with a series of upcoming training and workshops planned until July 2026.

CRA Compliance Intro: All You Need to Know About the EU Cyber Resilience Act (CRA)[30] is a comprehensive overview of the key principles and obligations of the CRA. The video explains how the CRA impacts manufacturers, importers, distributors, and open-source software stewards by outlining roles and responsibilities, risk-based product classifications (Default, Important, and Critical), as well as security requirements, CE marking, and conformity assessments. It also covers crucial topics such as vulnerability disclosure, incident reporting, Software Bill of Materials (SBOM), enforcement timelines, and penalties for non-compliance.

Pentesting Methodology explained[31]

As part of the Cyber Resilience Act (CRA) compliance training series, this module provides a comprehensive, step-by-step guide to penetration testing methodology for products with digital elements. It is designed for manufacturers, SMEs, and cybersecurity teams seeking to meet CRA requirements effectively and efficiently. The training covers the five key phases of CRA-aligned penetration testing and explains how to plan, conduct, and report tests in line with CRA standards. It also clarifies the compliance requirements for Important Class I, Important Class II, and default category products.

[30] Available on YouTube https://youtu.be/-QbPlFVobNw

[31] Available on YouTube: https://youtu.be/wpJluHL9IlQ

Appendix F: Other EU projects' tools

Together with CONFIRMATE, a set of additional EU projects to support SME compliance with the CRA were launched. Each project has a different angle, originates from a different set of countries, and creates complementary resources and tools. The list of the projects running in 2025-2026 period, gathered by CyberStandEU[32] is:

1. CRA-AI: Project CRA-AI develops an AI-powered platform to help SMEs achieve and maintain compliance with the EU Cyber Resilience Act, uniting cybersecurity experts from six EU countries.
2. CURIUM: CURIUM develops the Compliance Continuum, a set of tools to automate and simplify EU Cyber Resilience Act (CRA) compliance. By offering cybersecurity assessments, risk management, and vulnerability testing, it helps SMEs reduce costs, accelerate certification, and strengthen Europe's digital security ecosystem.
3. OSCRAT: OSCRAT develops free, open-source tools to help European SMEs, policymakers, and industry associations achieve compliance with the Cyber Resilience Act (CRA) and strengthen cybersecurity practices.
4. OCCTET: OCCTET is an EU-funded project developing an open-source toolkit to help SMEs automate Cyber Resilience Act (CRA) compliance for open-source software. The toolkit includes a compliance checklist, automated evaluation tools, a federated database, dependency analysis tools, and reporting resources.
5. CYBERFORT: CYBERFORT helps SMEs meet Cyber Resilience Act (CRA) requirements by offering tailored tools, expert guidance, and training. Through an open platform and collaboration with cybersecurity firms, authorities, and industry stakeholders, it strengthens cyber resilience and awareness across Europe.
6. TRUSTBOOST: TrustBoost is an EU-funded project (Grant Agreement No. 101158687) supported by the European Cybersecurity Competence Centre. Its mission is to strengthen cybersecurity, resilience, and compliance across the EU by driving collaboration on certification and adherence to key EU legislations.
7. CRACoWi: CRACoWi (Cyber Resilience Act Compliance Wizard) is an EU project creating a digital assistant to help SMEs, manufacturers, distributors, and importers meet Cyber Resilience Act (CRA) standards, ensuring product security from design to post-market stages.
8. CRACY: CRACY (CRA made Easy) helps European SMEs meet Cyber Resilience Act (CRA) requirements by simplifying compliance for products with digital elements, promoting best practices and more secure products and services.

[32] Availbale at: https://cyberstand.eu/events/impacting-cra-defining-standards-future

Appendix G: Relation to Other EU Legislation

Whilst it is not possible to give a complete discussion in this document on the relation of the CRA to other EU legislation, some of the more important links are mentioned below:

1. *The New Legislative Framework (EC/2008/765 & EC:2008/768):* The CRA builds upon the NLF and essentially extends the framework to cover products with digital elements. This is described in detail in section 4.1 of these guidelines.
2. *Cyber Resilience:* Both the NIS2 Directive and the DORA regulation aim to improve cyber resilience across the EU. They set cybersecurity risk management and incident reporting of entities with relation to their essential services. The CRA complements these initiatives by imposing security requirements related to the products with digital elements, feeding into the EU product regulation framework.
3. *The Radio Equipment Directive (RED) (Directive 2014/53/EU)* focuses on safety, electromagnetic compatibility, and interoperability of radio-equipped products. The CRA focuses on cybersecurity and convers a broader scope (including software, not only IoT). It replaces the RED delegated act for cybersecurity.
4. *The Machinery Regulation (Regulation (EU) 2023/1230)* covers health and safety when using machinery. This is complementary to the CRA, which applies to digital components of machinery. Both regulations apply simultaneously.
5. *EU GDPR:* The CRA builds upon the GDPR requiring protection and minimisation of any data (personal or not) processed by products with digital elements placed on the EU market.
6. *The AI Act* (Regulation (EU) 2024/1689) regulates the trustworthiness and safety of (AI) systems. It applies to high-risk AI functionality, whereas the CRA applies to cybersecurity of the product itself. A high-risk AI system must comply with both the AI Act and with CRA cybersecurity requirements.
7. *EU Digital Services Act (DSA) and Digital Markets Act (DMA)* enforce platform accountability and content moderation (DSA) and market fairness for gatekeepers (DMA). The CRA does not directly overlap with these regulations, but it does apply to the software used by the platforms and backend systems.
8. *Cybersecurity Act (CSA)* (Regulation (EU) 2019/881): The CRA refers to certification schemes developed under the CSA under the requirements for conformity assessment (see section 4 of these guidelines for details).