SECURE
Cyber Resilience for SMEs

CRA101: Understanding CRA Obligations

20/10/2025

Funded by the European Union

EU Funding Statement: Funded by the European Union under GA No 101190325. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Industrial, Technology and Research Competence Centre.
Neither the European Union nor the granting authority can be held responsible for them.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC disclaimer: The project is supported by the European Cybersecurity Competence Center and its members

DISCLAIMER

This document contains material, which is the copyright of certain SECURE contractors, and may not be reproduced or copied without permission. All SECURE consortium partners have agreed to the full publication of this document if not declared "Confidential". The commercial use of any information contained in this document may require a license from the proprietor of that information. The reproduction of this document or of parts of it requires an agreement with the proprietor of that information.

This document is part of Deliverable D4.1 'Guidelines and Materials for SMEs CRA Compliance' of the SECURE Project.

First author: *Centre for Cybersecurity Belgium (CCB)*

Second author: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Table of contents

List of Tables and Figures

Abbreviations

CAB – Conformity Assessment Body

CE - Conformité Européenne, or European Conformity

CRA – Cyber Resilience Act

CSIRT – Computer Security Incident Response Team

CVD – Coordinated Vulnerability Disclosure

ENISA – European Union Agency for Cybersecurity

EU – European Union

EU DoC – European Union Declaration of Conformity

NB – Notified Body

PDE – Product with Digital Elements

SBOM – Software Bill of Materials

SME – Small and Medium Enterprise

SPOC – Single Point of Contact

Introduction

The European Union (EU) **Cyber Resilience Act** (CRA), Regulation (EU) 2024/2847, was adopted with the aim of enhancing the cybersecurity readiness and resilience of the EU digital market in light of growing cybersecurity challenges. By introducing harmonised rules and clear minimum cybersecurity requirements, the CRA intends to reduce vulnerabilities and safeguard both consumers and businesses. Although this milestone regulation entered into force in December 2024, it opts for a phased implementation, allowing for a transition and adaptation period from 2024 to 2027. Concretely, the CRA lists obligations for manufacturers, importers and distributors of products with digital elements (PDEs). **Article 13 and Annex I** of the CRA list the essential cybersecurity requirements manufacturers must comply with, both when bringing their PDEs onto the EU market and throughout the entire lifecycle of the PDE. Part I of the Annex I requirements focuses on the PDEs' properties, part II focuses on vulnerability handling. Beyond the CRA's Annex I, and Article 13 however, other requirements are imposed – for example, regarding information and user instructions (Annex II), reporting obligations (Article 14-17), and conformity (Article 27-32). In a preliminary effort to translate the key legal obligations into tangible guidance, **this guideline offers a simplified overview[1] of the obligations**, separated into **five sections**, to be considered **at minimum**. The aim is to enhance the accessibility of the regulation and improve awareness and understanding at a basic level, in particular for Small- and Medium Enterprises (SMEs), in line with the **SECURE project**[2] objectives. For technical guidance and tools on the implementation of these stipulations in practice, further materials are made available on the **SECURE open repository** on a rolling basis.

Timeline of the CRA:

- Entry into force: 10 December 2024
- Reporting obligations apply: 11 September 2026
- Full application CRA requirements: 11 December 2027

[1] This is a non-exhaustive list meant to simplify the CRA obligations and does not include the exceptions considered under the CRA. Only the primary obligations are included to provide an overview. They have been selected based on a close reading of the CRA legislative text.

[2] The 'Strengthening EU SMEs Cyber Resilience' (SECURE) project offers financial support and guidance for SMEs to comply with the CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Understanding CRA Obligations - CRA 101

1. Cybersecurity Risk Assessment

In order to comply with the obligation to ensure that your PDE "has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I"[3] – i.e. guaranteeing "an appropriate level of cybersecurity based on the risks"[4] – a cybersecurity risk assessment *must* be carried out. This assessment must be **documented**[5] and **regularly updated** throughout the so-called 'support period'[6].

Concretely the risk assessment should, at least, include[7]:

1) An **analysis of the cybersecurity risks** considering:
   - The PDE's intended purpose and foreseeable use;
   - Conditions of use (e.g., operational environment, assets to be protected).

2) A **clarification, explanation, and/or justification** of
   - The application of cybersecurity by design[8] – i.e. how is this applied?
   - The applicability (or non-applicability) of the requirements in Annex I, Part I, to the PDE – i.e. are, and in what manner, the security requirements applicable?
   - The application and implementation of the vulnerability handling requirements[9] – i.e. how are the vulnerability handling requirements applied?

When a PDE contains components sourced from third parties, the CRA expects you to exercise **due diligence** to safeguard the cybersecurity of the final product. This may mean, for example, reporting a vulnerability that you have identified to the manufacturer of that component and further

[3] Art. 13(1), CRA.
[4] Annex I, Part I(1), CRA.
[5] Technical Documentation: clarified under point 5.
[6] Support period: clarified under point 2.
[7] Art. 13(3), CRA.
[8] Annex I, Part I(1), CRA.
[9] Annex I, Part II, CRA.

addressing it. In order to do so, a Software Bill of Materials (SBOM)[10] and a coordinated vulnerability disclosure (CVD) policy for suppliers should be maintained and kept available for market surveillance authorities upon their request.

2. Vulnerability handling and security updates

As stated in Article 13(8), manufacturers must ensure that the vulnerabilities of the PDE and its components are – "handled effectively and in accordance with the essential requirements set out in Part II of Annex I"[11] throughout the support period.

This means, amongst other things[12]:

1) **Identifying and documenting vulnerabilities** – i.e. drawing up the SBOM (at least for top-level dependencies) and keeping it available to provide to market surveillance authorities upon request[13];
2) Addressing and remediating vulnerabilities without delay – i.e. **providing security updates** without undue delay and free of charge (with advisory messages for users):
    - Each security update released during the support period must remain available for at least 10 years after release, or for the remainder of the support period, whichever is longer[14].
3) Regularly **reviewing and testing** the product security;
4) **Sharing information** about fixed (and potential) vulnerabilities, their impacts and severity, user instructions for remediation, contact addresses for vulnerability reporting, as well as establishing and enforcing a CVD policy.

The '**support period**' mentioned above "reflects the length of time during which the product is expected to be in use"[15] and should proportionally consider user expectations, the PDE's nature (purpose), and relevant Union law.

[10] A formal record of details and supply chain relationships of components included in software elements of PDEs (Art. 3(39), CRA).
[11] Art. 13(8), CRA.
[12] Annex I, Part II, CRA.
[13] Sharing it with users is optional.
[14] Art. 13(9), CRA.
[15] Art. 13(8), CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Concretely, when defining your support period, it should be:

- At least five years (unless the product's lifetime is shorter than five years, in which case, the support period equals the product's lifetime);
- Clearly specified (end date: month and year) at the time of purchase/on the packaging/in digital form (when reached, users should ideally be notified)[16].

The determination and definition of the support period should be included in the Technical Documentation[17].

3. User information, instructions and Single Point of Contact

Following Article 13(14-18) and Annex II, manufacturers *must*, at minimum, **clearly inform users** by including on paper/digitally:

- Details of the manufacturer (name, registered trade name or trademark, postal address, email address or digital contact, website);
- Details of the PDE (name, type, intended purpose, security environment and security properties, essential functionalities, possible cybersecurity risks, technical security support provided, end-date of support period);
- Detailed instructions or link thereto (regarding measures for secure use, possible data security effects due to product changes, installing security updates, secure decommissioning and user data removal, security updates default installation settings);
- A Single Point of Contact (SPOC) must be appointed to allow users to:
    - Communicate directly and rapidly with the manufacturer through their preferred means of communication (not limited to automated tools);
    - Report vulnerabilities;
    - Locate the CVD policy.
- Links (if applicable) to the CVD policy, the EU declaration of conformity (EU DoC)[18], the SBOM (if made available for users).

[16] Art. 13(19), CRA.

[17] Technical documentation: clarified under point 5.

[18] EU DoC : clarified under point 5.

The user instructions should be available in an easily understandable language, online or on paper, for at least ten years or the support period (whichever is longer).

4. Reporting obligations: vulnerability and incident reporting

Regarding reporting[19], the table below provides an overview of your obligations. Thereunder, further clarifications are provided.

Table 1:
Vulnerability and incident reporting

Reporting	Vulnerabilities	Incidents
WHAT	*Must:* 'actively exploited vulnerabilities' *May:* vulnerabilities (not actively exploited); cyber threats	*Must*: 'severe incidents' *May*: incidents (non-severe); near misses
TO WHOM	CSIRT[20] Single reporting platform (ENISA) Impacted users	
HOW	1) Early warning notification (24h) 2) Vulnerability notification (72h) 3) Final Report (14 days)	1) Early warning notification (24h) 2) Incident notification (72h) 3) Final Report (1 month)

[19] Art. 14-17, CRA.

[20] Art. 3(51), CRA: 'CSIRT designated as coordinator' means a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555.

4.1. What

According to the definitions set out in Article 3 of the CRA,

- An 'actively exploited vulnerability' requires reliable evidence of exploitation by a malicious actor in a system without the owner's permission[21];
- An incident is considered 'severe' when it[22]:
    - Negatively affects or can affect the PDE's ability to protect the availability, authenticity, integrity, or confidentiality of data or functions; or
    - Has led or can lead to the introduction/execution of malicious code in the product or in the network and information systems of a user.

4.2. To whom

The Computer Security Incident Response Team (CSIRT) to be reported to is that of the Member State where the manufacturer[23]:

- Has its main establishment; or, if not determinable,
- Has the establishment with the highest number of employees.

If outside the EU, a fallback chain can be followed that considers the establishment of the manufacturer's authorised representative → importer → distributor → where the highest number of PDEs or users are located.

Notwithstanding several exceptions, all notifications will go through the single reporting platform, still to be established and maintained by the European Union Agency for Cybersecurity (ENISA), and will be disseminated to other CSIRTs and market surveillance authorities through an electronic notification end-point.

[21] Art. 3(42), CRA.

[22] Art. 3(44), CRA; Art. 14(5), CRA.

[23] The CSIRT is typically the national CERT: Computer Emergency Response Team.

Impacted users (and, where appropriate, all users) must also be notified about vulnerabilities/incidents and user actions, preferably in machine-readable format. CSIRTs may inform users if the manufacturer fails to do so[24].

4.3. How

There are several differences in the reporting on vulnerabilities and incidents.

Vulnerabilities

1) **Early warning notification**: should be submitted at the latest within 24 hours of becoming aware and should indicate, if applicable, the Member States where the PDE is available.
2) **Vulnerability notification**: should be submitted at the latest within 72 hours of becoming aware and should include:
    - General information of the PDE;
    - General nature of the vulnerability;
    - Corrective or mitigating measures taken or that can be taken by users;
    - Sensitivity of the notified information.
3) **Final report**: should be submitted no later than **14 days** after corrective/mitigating measure and should include:
    - Description – severity and impact;
    - Information on malicious actor if applicable;
    - Details on security update or other corrective measure available.

Incidents

1) **Early warning notification**: should be submitted at the latest within 24 hours of becoming aware and should indicate,
    - If applicable, the Member States where the PDE is available;
    - Whether there is suspicion of it being caused by unlawful or malicious acts.

[24] Art. 14(8) CRA.

2) **Incident notification**: should be submitted at the latest within 72 hours of becoming aware and should include:
    - General information about the nature of the incident;
    - Initial assessment of the incident;
    - Corrective or mitigating measures taken or that can be taken by users;
    - Sensitivity of the notified information.
3) **Final report**: should be submitted within one month after incident notification submission and should include:
    - Description – severity and impact;
    - Type of threat or root cause likely to have caused incident;
    - Applied and ongoing mitigation measures.

5. Conformity assessment

Depending on the standards currently under development as well as existing European and international cybersecurity standards, a presumption of conformity[25] with the essential requirements of Annex I is likely to apply. Beyond this, however, the CRA mandates an EU declaration of conformity, CE marking[26] and specific conformity assessment procedures.

5.1. EU declaration of conformity (EU DoC)

Drawn up by the manufacturer, the EU DoC[27] confirms that the essential cybersecurity requirements have been met. The model structure can be found in Annex V of the CRA. The simplified EU DoC can be found in Annex VI. It must be made available in the languages required by the Member State in which the PDE is placed on the market.

[25] Art. 27, CRA.

[26] Conformité Européenne (European Conformity) marking.

[27] Art. 28, CRA; Annex V-VI, CRA.

5.2. CE marking

To allow consumers to identify PDEs that meet the CRA requirements and make informed decisions when purchasing and using such PDEs, a CE marking must be "affixed visibly, legibly and indelibly"[28]. This can be on the product itself, its packaging, and/or the EU DoC[29] [30].

5.3. Conformity assessment procedures

Depending on the classification of the PDEs falling under the CRA's scope, specified in Annex III and IV of the CRA, different assessment procedures have been set out[31]. An overview of which procedure can be applied per product class can be found in table 2 on the page below.

[28] Art. 30(1), CRA.

[29] Art. 29-30, CRA.

[30] Additional rules apply if a Notified Body participates in the conformity assessment.

[31] Art. 32, CRA; Annex VIII, CRA.

Table 2:
Conformity assessment procedures

	Internal control self-assessment (module A)	Harmonised standards/ Common specifications (module A)	EU-type examination & EU-type conformity (module B & C)	Full quality assurance (module H)	European cybersecurity certification scheme
Standard products[32]	X				
Class I Important products[33]		X	X	X	X (level: substantial)
Class II important products[34]			X	X	X (level: substantial)
Critical products[35]					X (level: TBD[36])

The EU-type procedures and full quality assurance procedure are to be conducted by a notified body (NB), a third party conformity assessment body (CAB).

[32] Internal control (module A) is allowed; the presumption of conformity stems from applying harmonised standards/common specifications or an EU cyber certification scheme.
[33] Internal control (module A) is only allowed when harmonised standards/common specifications or an EU cyber certification scheme have been applied. If not (or only partly), third-party assessment is mandatory (module B and C, or module H).
[34] Only module B and C, module H, or an EU cyber certification scheme are allowed.
[35] If, under Art. 8(1) of the CRA, a delegated act is adopted, the EU cyber certification scheme can be used. If not, fall back to the Class II important products' rules.
[36] Assurance level to be set by delegated act.

A key component to assessing conformity is the **technical documentation.** Mandated by Article 31 of the CRA and Annex VII, the technical documentation is relevant to all previously discussed points, as it is to be drawn up before the PDE is placed on the market and continuously updated throughout the support period[37]. Bringing together the majority of CRA obligations, the technical documentation should therefore include[38]:

- General description of the PDE (intended purpose, software versions affecting compliance, evidence of external features, marking and internal layout for hardware products, user information and instructions);
- Description of the PDE's design, development and production, and vulnerability handling processes (e.g., system architecture description, SOBM, CVD policy, monitoring processes, etc.);
- Cybersecurity risk assessment;
- Support period definition and clarification;
- Applied harmonised standards (or parts thereof);
- Conformity testing reports and vulnerability handling reports;
- EU DoC copy.

A **simplified technical documentation** form is to be developed by the European Commission for microenterprises and small enterprises[39]. Moreover, Article 33 stipulates that both Member States and the European Commission are to provide **support for SMEs** – amongst others, in the form of guidance[40] and financial support opportunities.

The **SECURE Project** **offers financial support for SMEs required to comply with the CRA and provides guidelines and materials on a rolling basis aimed at assisting SMEs with CRA implementation**, such as this CRA101 guideline.

[37] Art. 31(2), CRA.
[38] Annex VII, CRA.
[39] Art. 33(5), CRA.
[40] Art. 26, CRA.

Conclusion

In an effort to provide an **accessible overview of the key obligations set out in the CRA**, this guideline focuses on **five components** of the CRA, to be considered at minimum: (1) Cybersecurity Risk Assessment; (2) Vulnerability handling and security updates; (3) User information, instructions and Single Point of Contact; (4) Reporting obligations: vulnerability and incident reporting; (5) Conformity assessment. It clarifies elements such as the support period, the EU declaration of conformity and CE marking, and the technical documentation. With an eye on **supporting SMEs in navigating the complex legal framework**, this guideline offers a summary of the key legal obligations that must be understood prior to their implementation. For practical guidance on how to further approach and implement these legal stipulations, as well as on particular elements of the CRA (e.g., SBOM, vulnerability management, etc.), additional technical guidelines and tools will become available on a rolling basis on the **SECURE open repository**, as the CRA implementation further develops. As next steps for SMEs, it is recommended to consult the other guidelines on the SECURE repository, such as the **CRA's Essential Cybersecurity Requirements: Annex I, Part I** for practical suggestions and recommendations on each of the Annex I stipulations, as well as the **CRA Methodological Compliance Assessment Framework** for a step-by-step toolkit and checklist on compliance with the CRA beyond Annex I.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE