

Cyber Resilience Act

Overview of Articles 1-34

Navigating the horizontal cybersecurity requirements for products with digital elements in the European Union market.



Co-funded by the
European Union



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

WHAT IS THE CYBER RESILIENCE ACT?

EU Regulation

- Unified cybersecurity rules for digital products.

Digital Scope

- Applies to products with digital elements placed on the EU market.

Full Lifecycle

- Covers the entire product lifecycle (design → development → post-market).

Risk Reduction

- Aims to reduce vulnerabilities and cyber risks across the internal market.

Chapter I

General Provisions

CHAPTER I: FOUNDATIONS (ART 1-3)

What does it concern?

Establishes rules for placing products with digital elements on the market to ensure essential **cybersecurity requirements**.

What products are covered?

Products whose intended or reasonably foreseeable use involves a **direct or indirect logical or physical data connection** to a device or network – in the context of commercial activity

A green thought bubble with a small tail pointing towards the 'What products are covered?' section.

Exclusions where equivalent sector-specific EU legislation applies (e.g. medical devices, aviation, vehicles).

CHAPTER I: KEY DEFINITIONS (ART 3)

- **Product with digital elements**

- a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately

- **Manufacturer**

- 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, monetization or free of charge

- **Intended purpose**

- the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation

- **Vulnerability**

- a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat

CHAPTER I: MARKET ACCESS & CATEGORIES (ART 4-8)

Essential Requirements:

Products with digital elements shall be made available on the market only where they meet –at least- cybersecurity requirements set out in Annex I

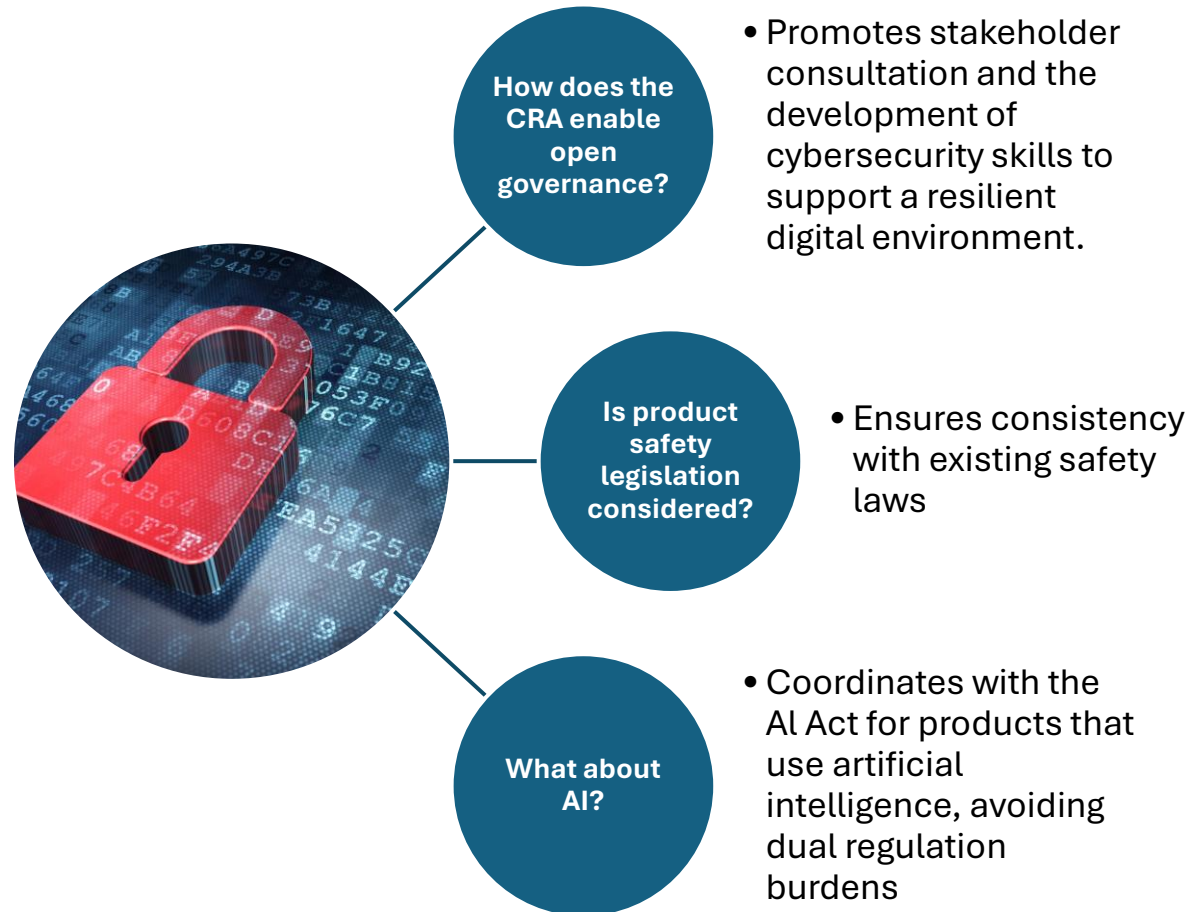
Categories:

Differentiates between standard products, Important Products (Class I and II), and Critical Products, based on cybersecurity risk.

Free Movement:

Products meeting these requirements may not be restricted on cybersecurity grounds by Member States.

CHAPTER I: COMPLEMENTARY PROVISIONS (ART 9-12)



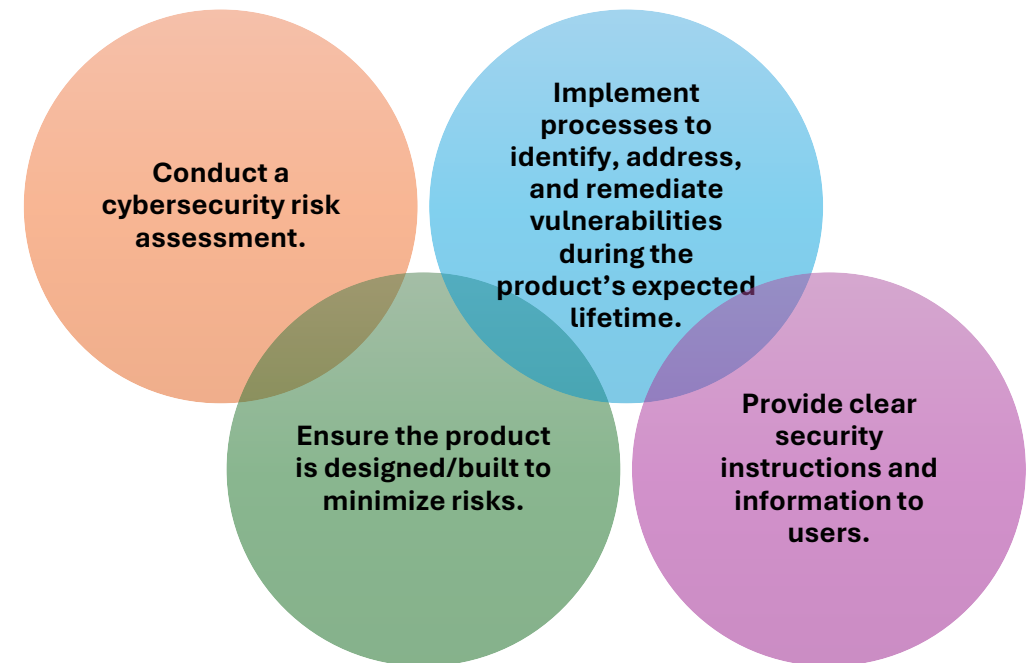
Chapter II

Obligations of Economic Operators

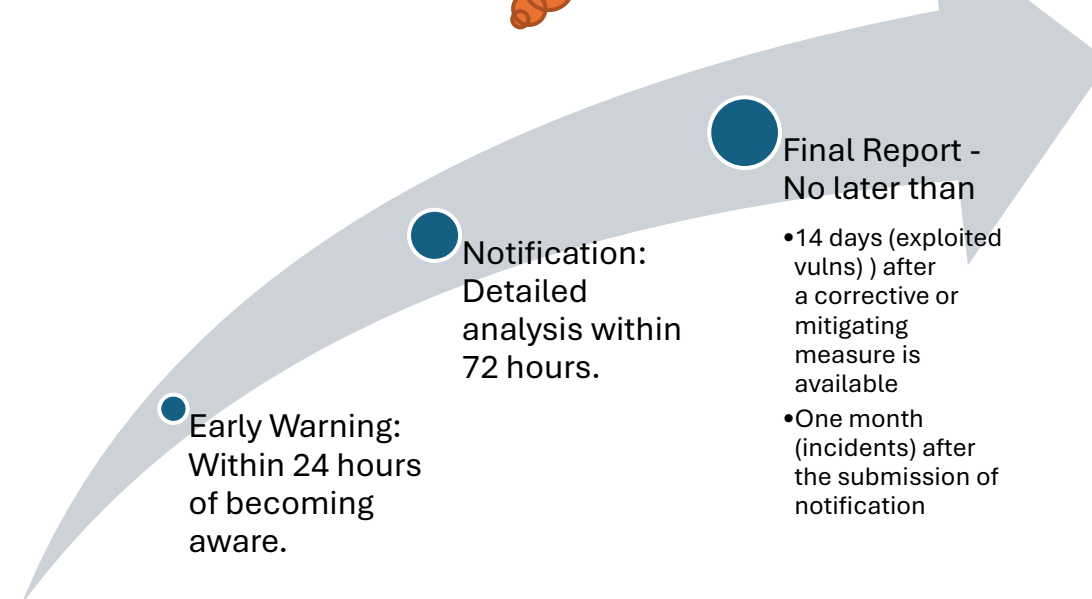
CHAPTER II: MANUFACTURERS (ART 13)

**I am a manufacturer.
What are my responsibilities?**

The manufacturer bears the primary responsibility for the cybersecurity of the product:



CHAPTER II: INCIDENT REPORTING (ART 14-17)



CAUTION: Failure to report can lead to significant fines.

CHAPTER II: EXTERNAL OPERATORS (ART 18-19)

Authorized Representatives

- Non-EU manufacturers must appoint a representative in the Union to handle compliance and communicate with authorities.

Importers

- Must verify that the manufacturer has followed the rules before placing the product on the EU market.

CHAPTER II: SUPPLY CHAIN (ART 20-23)

Distributors (Art 20):

- Act with "due care" to ensure products bear the CE mark and documentation. When Importers become

Obligations (Art 21, 22):

- If an importer or distributor places a relevant product under its name or trademark or modifies a product significantly, they take on full manufacturer responsibilities.
- Also, any natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification shall be considered to be a manufacturer for the purposes of this Regulation.

Identification (Art 23):

- Operators must be able to identify who supplied them and who they supplied for 10 years.
- They are required to assist and provide information to market surveillance authorities

CHAPTER II: OPEN SOURCE (ART 24-26)

- **The CRA introduces the concept of the "Open-Source Software Steward":**
 - Stewards must establish security policies for their projects.
 - Security attestation systems to prove the code follows best practices.
 - Exemptions exist for purely non-commercial, hobbyist development.

Open-source software steward

a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products

Chapter III

Conformity of the Product

So how do we demonstrate compliance..?

Presumption of Conformity

- Products following "harmonized standards" or EU cybersecurity certificates are assumed to be compliant with the CRA.

EU Declaration

- A formal document stating the product meets all requirements.
- It must be kept updated and available for 10 years after the product is sold.

CHAPTER III: CE MARKING RULES (ART 29-32)

- **The Label:**

- The CE mark must be visible on the product or packaging.

- **Procedures** (Art 32):

- Standard products: Self-assessment.
- Important/Critical: Third-party audits or certifications required.



CHAPTER III: FINAL PROVISIONS (ART 33-34)

- **SME Support (Art 33):**
 - The Commission and Member States must provide guidance - awareness and lower fees for micro/small businesses to help them comply.
 - Provision of regulatory sandboxes to facilitate development, design, validation and testing for compliance.
- **Mutual Recognition (Art 34):**
 - Agreements with non-EU countries to recognize each other's security tests.

Thank you!

Evgenia Lada

National Cybersecurity Authority of Greece

e.lada@cyber.gov.gr