Cybersecurity

EU Cyber Resilience Act (CRA) and Open Source

An introduction

Open Source @ Siemens 2024

Francesco Negosanti – Siemens SI BP CYS

SIEMENS

Goals and requirements of the CRA

🟠 Product related

🔵 Process / Organization / Tooling

🔵 🟠 Cybersecurity is taken into account in product **planning, design, development, production, delivery** and **maintenance** phase

🔵 🟠 All **cybersecurity risks** are documented

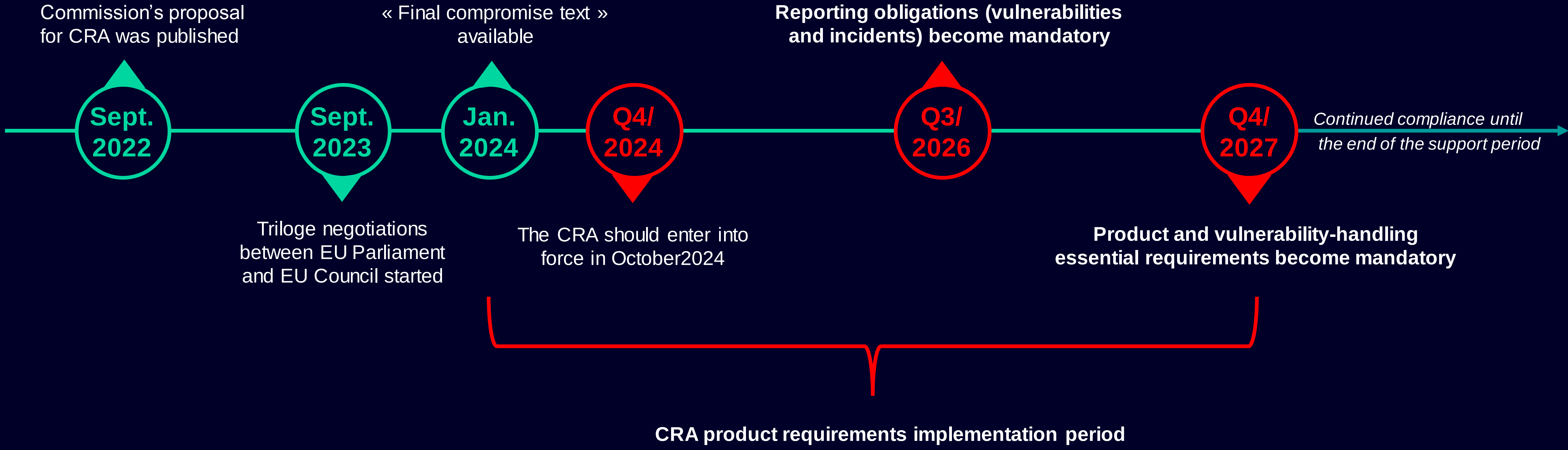
🔵 🟠 **Clear and understandable instructions** for the use of products with digital elements

🔵 Manufacturers will have to **report actively exploited vulnerabilities and incidents**

🔵 🟠 Once sold, manufacturers must ensure that for the **expected product lifetime** or for a period of five years (whichever is the shorter), **vulnerabilities are handled effectively**

🔵 🟠 **Security updates** to be made **available for at least five years.**

EU Cyber Resilience Act
Implementation timeline



Sept. 2022

Commission’s proposal for CRA was published

Sept. 2023

Triloge negotiations between EU Parliament and EU Council started

Jan. 2024

« Final compromise text » available

Q4/ 2024

The CRA should enter into force in October2024

Q3/ 2026

Reporting obligations (vulnerabilities and incidents) become mandatory

Q4/ 2027

Product and vulnerability-handling essential requirements become mandatory

Continued compliance until the end of the support period

CRA product requirements implementation period

EU Cyber Resilience Act (CRA)

✓ *Products*

Timeline

- Entry into force not before October/2024
- Product-related requirements applicable 36 months after
- Vulnerabilities and incidents reporting obligations applicable 21 months after

Focus

- Products with digital elements (whether hardware products or software products)
- Remote data processing solutions are in scope if linked to a product
- Products components are also in scope (including open-source)

Aim

- Security is taken into account in planning, design, development, production, delivery & maintenance phases
- All security risks are documented
- Clear instructions for use of the products
- Vulnerability handling during support period
- Regular security updates

Addressees

- **Manufacturers (including of open-source)**
- Distributors
- Importers

Implementation

- Risk-based regulation: the implementation of the requirements must be proportionate to the risks, the intended purpose and the environment of use of the product
- Role of European Harmonized Standards for presumption of conformity
- Different categories of products (default, important and critical products)

Obligations

- Risk assessment on each product
- Compliance with essential requirements (Annex 1.1 and 1.2)
- Technical documentation
- Due diligence on components sourced from third parties
- Determine security support period (minimum 5 years)
- Comply with reporting obligations

What is at stake for Open-Source?

“Free and open-source software” means software the source code of which is openly shared and which is made available under a free and open-source license which provides for all rights to make it freely accessible, usable, modifiable and redistributable;

The CRA applies to economic operators only in relation to products with digital elements made available on the market, hence supplied for distribution or use on the Union market **in the course of a commercial activity.**

The CRA final compromise, as agreed by the Commission, Parliament and Council, has clarified that **“the provision of free and open-source software products with digital elements that are not monetized by their manufacturers is not considered a commercial activity”**

So, what are the consequences on manufacturers of hardware and software products and for the Open-Source community?

What is at stake for the manufacturers of products which includes Open-Source components?

Due diligence: manufacturers shall exercise due diligence **when integrating components** sourced from third parties in a manner that such components do not compromise the cybersecurity of the product with digital elements… **including when integrating components of free and open-source software** that have not be made available on the market in the course of a commercial activity.

- ✓ *Verifying the components receives **regular security updates**, such as checking security updates history*
- ✓ *Verifying the components is **free from vulnerabilities** registered in the European vulnerability database or other publicly accessible vulnerability databases*
- ✓ *Carrying out **additional security tests***

Manufacturers shall, upon identifying a vulnerability in a component, including in an open-source component, report the vulnerability to the person or entity manufacturing or maintaining the component and address and remediate the vulnerability

- ✓ *In accordance with the vulnerability handling essential requirements in Section 2 of Annex I*

__SBOM__, security updates, policy on coordinated vulnerability disclosure…

Upcoming European Standards on vulnerability handling!

What is at stake for the manufacturers of Open-Source software? (1)

- **First piece of legislation addressing and recognizing the role played by open-source:**
  - *The application of the CRA should **take into account the nature of the different development models** of software distributed and developed under free and open-source software licenses.*

- **The initial CRA proposal raised concerns that "commercial" would be interpreted broadly – hampering the role of Open-Source and innovation in general:**
  - **Essential clarifications** regarding the development of open-source software products and whether these should be considered as a commercial activity or not have been provided:
    - *The mere fact that an open-source software product received **financial support by manufacturers** or that manufacturers contribute to the development of such a product **should not in itself determine that the activity is of commercial nature**;*
    - *The development of products qualifying as free and open-source software by not-for-profit organizations should not be considered a commercial activity **as long as the organization is set up in a way that ensures that all earnings after cost are used to achieve not-for-profit objectives;***

What is at stake for the manufacturers of Open-Source software? (2)

- **Open-Source foundations and associations recognize that major improvements were made by the EU when agreeing on the final text**

  - ## What can be an Open-Source commercial activity?

    - ***Charging a price for the Open-Source product, but also charging a price for technical support services*** *when this does not serve only the recuperation of actual costs;*
    - ***An intention to monetize****, for instance by providing a software platform through which the manufacturer monetizes other services, by requiring as a condition for use the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, or by accepting donations exceeding the costs associations with the design, development and provision of a product…*
    - ***The sole act of hosting products on open repositories****, including through package managers or on collaboration platforms, does not in itself constitute making available on the market of a product;*

What is at stake for the manufacturers of Open-Source software? (3)

For Free and Open-Source software that is intended for commercial activities…

The role of the open-source software steward

- ‘open-source software steward’ means any legal person, other than a manufacturer, which has the **purpose or objective to systematically provide support on a sustained basis for the development of specific products** with digital elements qualifying as free and open-source software that are intended for commercial activities, and ensures the viability of those products;
  - Open-source software stewards shall put in place and document in a verifiable manner a **cybersecurity policy** to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product;
  - The steward shall **notify any exploited vulnerability** contained in the product with digital elements;
  - The steward shall **cooperate with the market surveillance authorities**, at their requests, with a view to mitigating the risks posed by a product with digital elements qualifying as free and open-source software

What is at stake for the manufacturers of Open-Source software? (4)

- **Still, significant amount of work is expected: the CRA is the first legislation regulating the software industry… it goes beyond the open source community.**
  - **The upcoming CRA guidelines, secondary legislation and European standards will have to ensure that the legal requirements align with technical and operational best practices;**
  - **OSS steward: brand new term and regime – future guidelines should assists these stewards – which entities and organizations are eventually in scope and will have the obligation to nominate an OSS steward?**
  - **What does "making available on the EU market" exactly means for free and open-source software products? OSS is typically published at global level, not in a particular region;**
  - **Shall free and open-source communities take part in the CRA standardization activities (CEN and CENELEC)? How can we best bring together these two communities?**

SIEMENS

Thank you!

Any question?

SIEMENS