Implementing the EU Cyber Resilience Act: Workstreams and Key Outcomes

Open Source Software Stewards and Manufacturers Workshop
Linux Foundation Europe & OpenSSF, 10 December 2024
Mirko Boehm

THE LINUX FOUNDATION | Europe

EU Cyber Resilience Act

The EU acts to strengthen the approach to cybersecurity regulation at union level. The CRA aims to achieve 3 policy goals:

- To reduce vulnerabilities in digital products,
- To ensure cybersecurity is maintained throughout a product's life cycle and
- To enable users to make informed decisions when selecting and operating digital products

The CRA establishes horizontal mandatory cyber-security requirements for all digital products (software and/or hardware).

The EU intends to play a leading international role in cybersecurity regulation.

Products with digital elements (PDE)

Software

…the part of an electronic information system which consists of computer code

Free and open source software

… is openly shared and … made available under a free and open-source licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable

Hardware

… a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data

Proprietary

(all other licensing schemes)

Provisioning PDE versus ‘making available’

‘…the provision of PDE qualifying as FOSS’

should not be considered to be a commercial activity

- CRA distinguishes “the provision of products with digital elements qualifying as free and open-source software” from “placing on the market”
- Anybody may provision PDE, however doing to in the course of a commercial activity “makes it available on the market”

‘making available on the market’

means the supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge

‘placing on the market’:

means the first making available of a product with digital elements on the Union market

Manufacturers and OSS stewards

Manufacturer:
full range of obligations

…means any 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 his or her name or trademark, whether for payment, monetisation or free of charge

Open source software steward:
light-touch regulatory regime

…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

IS THIS "OPEN SOURCE EXCEPTION"
HERE IN THE ROOM WITH US NOW?
imgflip.com
wiseGEEK

Coverage of free and open-source software (sic!)

(recital 18) “Free and open-source software is developed, maintained and distributed openly…”

“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”

“the provision of products with digital elements qualifying as free and open-source software that are not monetised by their manufacturers should not be considered to be a commercial activity”

Other key concept highlights

- Substantial modifications means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements
- CE marking means 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… (stewards cannot apply CE marks)
- Conformity assessment means the process of verifying whether the essential cybersecurity requirements set out in Annex I have been fulfilled
- 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 licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable

Process obligations for manufacturers

- Perform cybersecurity risk assessment covering the whole product life cycle
- Perform due diligence when integrating 3rd party or open source software into your PDE
- Report identified vulnerabilities back to upstream vendors/stewards, ideally in machine readable format
- Provide security updates for 5 years (or longer) and keep them available for 10 years (or longer)
- Manufacturers should draw up SBOMs but are not required to make them available to the general public
- Provide documentation to consumers about the risk assessment and conformity, in clear, understandable language for 10 years or more
- Apply the CE mark to demonstrate conformity
- Make PDE clearly identifiable
- Provide a single point of contact for cybersecurity inquiries
- Demonstrate conformity at the request of market surveillance authorities
- Communicate the ceasing of operations in the EU market to market surveillance authorities

Reporting obligations for manufacturers

- Manufacturers should notify actively exploited vulnerabilities
- … as well as severe incidents
- via a single reporting platform to a national CSIRT of their choice and ENISA
- Information to be shared in an European vulnerability database
- Vulnerabilities discovered in good faith (intrusion tests, review) do not need to be reported
- Manufacturers may apply for brief delays, e.g. if a fix is forthcoming
- Manufacturers should establish a vulnerability disclosure policy for reporting and inquiry by consumers

- Report actively exploited vulnerabilities
  - with an early warning within 24h of identification
  - with a full notification within 72h
  - following up with a final report within 14 days
- Report severe indicidents
  - with an early warning within 24h of identification
  - with a full notification within 72h
  - following up with a final report within 1 month
- On an actively exploited vulnerability or severe incident …
  - inform the affected users of the PDE
  - provide guidance on risk mitigation and corrective measures to users

Obligations for stewards

- Put in place and document a cybersecurity policy to foster the development of a secure product and effective handling of vulnerabilities
- Cooperate with MSA on the mitigation of vulnerabilities on their request
- Be prepared handle MSA requests to the project/community timely and diligently
- Participate in voluntary cybersecurity attestation programmes

Notable: Stewards have no obligations towards manufacturers!

Individual developers and upstream contributions

- Individual developers (hobbyists, occasional contributors, as long as participation remains non-commercial) are exempt
- Contributing to projects where you don't have responsibility is exempt (the upstream project takes responsibility)
- Individual developers may be manufacturers (e.g., one-person businesses) ~~or stewards (e.g., long-term maintainers)~~
- Be aware: Projects grow from ideas to large communities or businesses - hobbyists and small communities may become manufacturers or stewards

Corner case: OSS without stewards

- Not every project must have a steward
- Projects maintained by individuals without intentions to monetize or groups of hobbyist developers release OSS without a steward

Manufacturers decide which OSS to integrate into their products, but are responsible for due diligence (“is this component fit for purpose, can I assume responsibility for cybersecurity implications?”.

Corner case: OSS without a manufacturer

- OSS may be released directly by upstream projects for end-user consumption
- In such cases, consumers receive OSS without the maintainer’s responsibility for a support period, security fixes, …

LibreOffice
The Document Foundation

The EC may have accepted this situation as a rare corner case, however there is uncertainty if that was intended or not.

Manufacturers: Software updates, support period

- Manufacturers must supply vulnerability fixes throughout the support period
- Products should be designed to support software updates, especially for consumer products, ideally automated
- End of support must be communicated on the device without restricting the functionality available to the user
- Security updates must be provided separately from functionality updates
- Support period should be no less than 5 years
- …, unless the product has a shorter lifetime
- …, or more if a longer lifetime can be reasonably expected

Essential cybersecurity requirements: Basics

Products shall

- Be designed and developed in accordance with essential requirements
- Be made available on the market without known exploitable vulnerabilities,
- Be made available on the market with a secure by default configuration
- Be designed so that vulnerabilities can be addressed through security updates
- Ensure protection from unauthorised access,

...and more.

Essential cybersecurity requirements: Cascade

- Manufacturers should develop *all* digital products according to the essential CRA requirements,
  - since less critical devices may serve as a springboard for security attacks.
- Stricter requirements are applied to devices targeted at vulnerable consumers (like children’s toys),
- Even stricter regime to devices where exploits can cause wider damage (network routers, operating systems).

Essential cybersecurity requirements: Boundaries

- Member states cannot impose additional cyber-security requirements on market access.
- They may however define additional rules for the operation of devices in specific fields within the scope of union law.
- National security remains the responsibility of the member states, they may
    - impose additional requirements for defence
    - or national security purposes.
- More specific regulations may take precedence (medical devices, automotive, marine equipment, aviation, …), however EU "should harmonise" as they are updated (e.g., radio equipment directive).

Standards development in support of the CRA*

- A draft standards development request for 41 standards is being prepared
- Many of the CRA implementation details will be defined in standards
- There will be 3 main groups of standards:
    - Horizontal standards for security requirements relating to the properties of products with digital elements
    - Horizontal standards for vulnerability handling requirements
    - Vertical standards for security requirements relating to the properties of PDE
- LF Europe is engaged in European standards development

* currently a draft request from EC to CEN/CENELEC

What if the CRA is an opportunity for OSS?

As the largest global open source foundation, the Linux Foundation already is a successful steward for open source projects.

- The regulatory push for more refined cyber security practises provides us with an opportunity to shape community processes:
  - New/updated supply chain management guidelines
  - Data formats and tooling
  - Project management and governance
- Timeframe: CRA implementation period (now…2027)

The LF aims to be the best Open Source Software Steward on the planet!

Leading by example: Yocto, Zephyr, CIP, ...

- Many LF projects already have a strong cybersecurity posture
- The CRA codifies many practises the community has called for for some time
  - Long-term security updates for products
  - Better transparency about vulnerabilities and mitigation
  - Separate, free-of-charge security updates
  - ...
- To be released: Pathways to Cybersecurity Best Practices in Open Source: How the Zephyr,Yocto, and Civil Infrastructure Platform Projects are Closing the Gap to Meeting the Requirements of the CRA

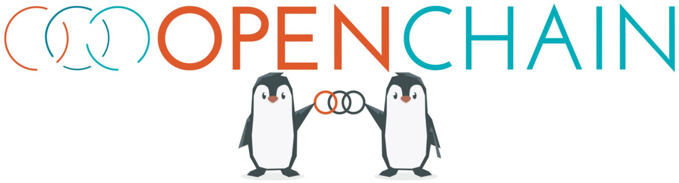
CRA implementation: Work streams

Consider: The CRA is an EU market regulation - it affects all open source projects and manufacturers active there!

- Formalize community specifications: Elevate existing cybersecurity best practises and guidelines to formal specifications, e.g. through PAS (JDF/OpenSSF)
- Provide community guidance: Create awareness of the required changes through research, whitepapers, training (LF Research, LF Education)
- Processes and tooling: Deploy processes and tooling across the LF project portfolio and to manufacturers to support CRA obligations (OpenChain, SPDX, LFX, ...)

Workstream: Formalize community specifications

- Community specifications or guidelines need to be formalized into standards so that they can be adopted for CRA compliance
- Leading example: OpenChain
  - OpenChain ISO/IEC 5230: The international standard for open source license compliance programs
  - OpenChain ISO/IEC 18974: The industry standard for open source security assurance programs
- Next: OpenSSF best practices, score card, ...



BUILDING TRUST IN THE SUPPLY CHAIN SINCE 2016

Related LF projects: OpenChain, OpenSSF, Joint Development Foundation

Workstream: Provide community guidance

- Aligning cybersecurity across the ecosystem depends a lot on guidance, awareness building and training
- First step: LF Research report on the state of the art of cybersecurity and the gap to the CRA (intended to be published in January 2025)
- To be decided: training program, educational materials, best practises guidelines (e.g., Certified Open Source Developer for Enterprise (CODE))

THE LINUX FOUNDATION | Research

Related LF projects: LF Research, LF Education, TODO Group

Workstream: Processes and tooling

- CRA compliance requires a steward to handle vulnerability reporting, release documentation, … in a unified and documented manner
- Required: Document formats and profiles, process specifications, tooling and application support across projects

Related LF projects: OpenChain, SPDX, LFX, ORT

Challenges

- Diverse LF project portfolio, strong autonomy of the projects WRT their development practises
- Manufacturers wish for unified processes, however open source ecosystem is diverse, decentralized
- Horizontal collaboration between various open source organisations difficult so far
- Difficult choice for LF as the largest foundation: Bear the cost to the benefit of the whole ecosystem, or have others co-opt our efforts

Community/manufacturer relationship

- The upstream project hosts open source projects under neutral governance
- Maintainers form the TSC usually as an additional role in their day job
- Contributors usually work downstream or in service businesses
- Remember: Open Source Maintainers Owe You Nothing

Photo by Daniel Funes Fuentes on Unsplash

Collaborative lifecycle support

- The best way to ensure the viability of an open source dependency is to participate in the governance of the project
- Through participation in governance, members gain influence on the long-term project roadmap and the contribution process
- By identifying their essential dependencies and engaging with their stewards, manufacturers are able to ensure maintenance throughout the required support period

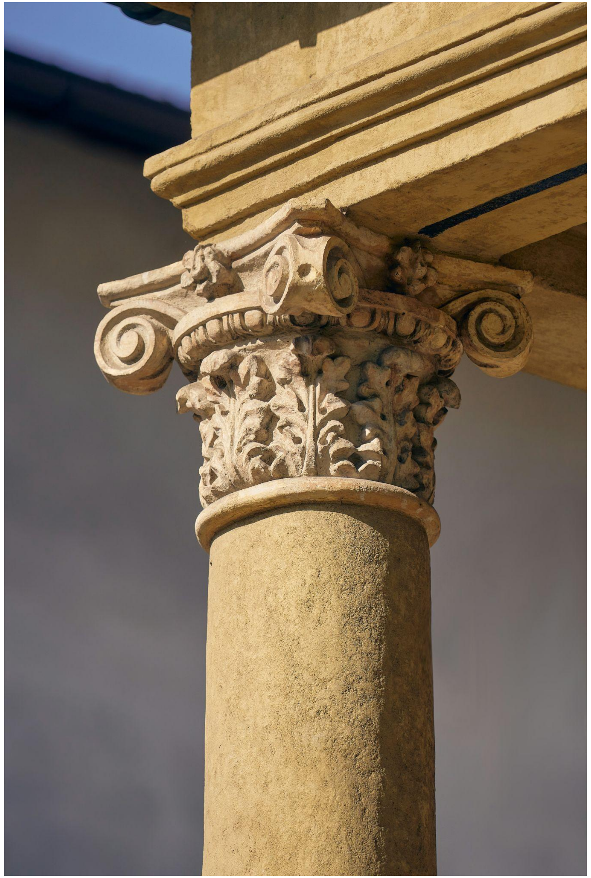


Photo by Jakub Pabis on Unsplash

THE LINUX FOUNDATION | Europe

Need for more explicit governance norms

Explicit posture regarding own roles: Do you act as a steward (provision of open source software without introducing products into the market) or a manufacturer (providing commercial products that possibly integrate OSS or proprietary components)

Explicit policies on releases: When is a release made? E.g., are only tagged versions or individual changes to main a released version?

Debates on “does this take into account the historically grown characteristics nature of some open source communities, e.g. the peculiar setup of Debian”? - however: The CRA contains guidance about what regulators think a reasonable setup for a steward should look like. This implicitly says “change your ways, or take responsibility for the consequences”

Outlook

- CRA legislative status: proposed on 15 September 2022 by the European Commission, approved by European Parliament on 12 March 2024, adopted by the European Council on 10 October 2024, published in the EU Official Journal on November 20, 2024
- The CRA is the first union-level regulation that models open source software stewards separately from manufacturers
- Many implementation details to be decided during the upcoming development of harmonised standards, Linux Foundation participates as a stakeholder

Timeline

- Vulnerability reporting obligations become effective after 21 months (Q3/2026?)
- The remaining obligations become effective after 36 months (Q4/2027?)

Thank you!

mirko@linuxfoundation.eu

THE LINUX FOUNDATION | Europe