Les entreprises du numérique ouvert

Anticipating the Cyber Resilience Act: The CNLL presents its practical guide

Anticiper le Cyber Resilience Act : Le CNLL présente son guide pratique

05 décembre 2024
11:30 - 11:50

Summary

- Introduction (5') - Stéfane Fermigier (CNLL)
- Presentation of the recommandations (10') – Benjamin Jean (Inno³)
- Questions and Answers (5')

Les entreprises du numérique ouvert

Introduction

Stéfane Fermigier (CNLL)

Context of the CRA

- **Objectives**: Strengthen cybersecurity of digital products for consumers and businesses across the EU
- **Scope**: Introduces mandatory security requirements for hardware and software throughout their lifecycle
- **Timeline**:
  - First public draft in 2022
  - Met with initial incredulity, then sheer panic, by the European Open Source business ecosystem (CNLL, APELL...)
  - Adopted on November 20, 2024, incorporating some feedback from Open Source stakeholders
  - Entry into force: December 10, 2024
  - 36-month transition period for compliance (until December 11, 2027)

Impact on Open Source

- End of the principle of absence of liability outside a commercial relationship, which has traditionally underpinned most Open Source licences and business models
- **Exemptions** for « non-commercial » projects; **stringent demands** for economically integrated Open Source products ; **business model disruption** for OSS vendors
- Up to 30 % development costs increase for OSS vendors
- Requirements include : detailed technical documentation, vulnerability management, CE marking, and SBOM production

Objectives of the Guide

- The guide has been commissioned by the **CNLL** (Free software and open digital entreprises Union), with the following o**bjectives** :
  - **Clarify** Requirements: Tailored guidance for the Open Source ecosystem on CRA compliance.
  - Actionable **Solutions**: Concrete, achievable recommendations to integrate CRA mandates into existing processes.
  - Promote **Dialogue**: Foster collaboration between Open Source communities, industry players, and legislators.

Available at https://cnll.fr/publications
under the Creative Commons By-SA 4.0 license

Presentation of the recommandation

Benjamin Jean (Inno³)

Scope

Regulation of products with digital elements : The CRA applies to :

- '**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;
- '**which is made available on the market**': intended to be distributed or used on the Union market in the course of a commercial activity on a commercial basis. used on the EU market in the course of a commercial activity, whether in return for payment or free of charge; or against payment or free of charge ;
- '**the intended or reasonably foreseeable use of which involves a direct or indirect connection, whether direct or indirect, logical or physical, to a device or network**": i.e. a connection between electronic information systems or components via a device or network.

Application to Open Source software:

- **Exclusion from application of the CRA in the absence of commercial activity** (distribution not for profit, funding provided by donations or grants, no associated paid services, research)
- **Application of the CRA limited to the version's products used in a commercial activity**

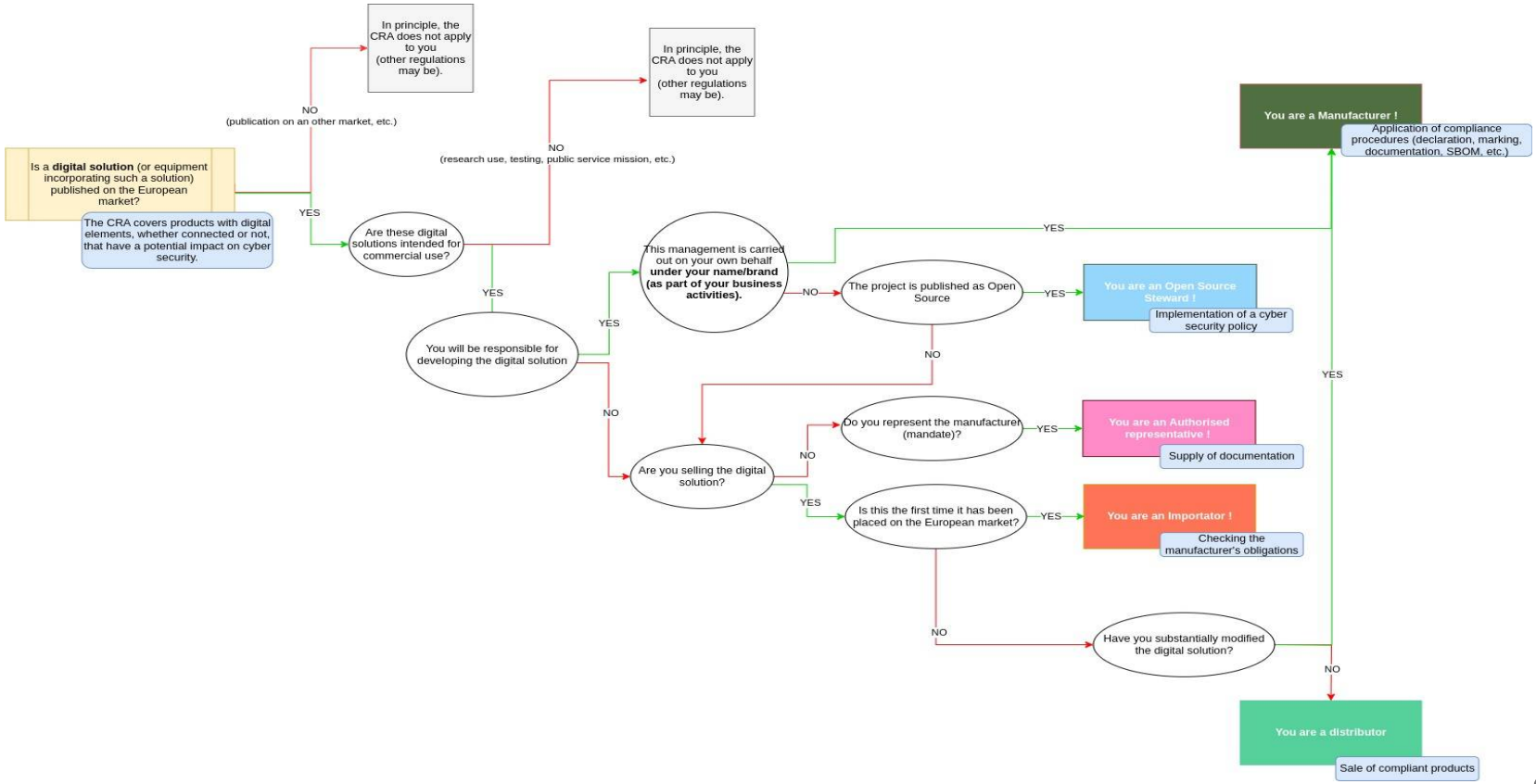
Actors subject to the CRA

- **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, monetisation or free of charge';*
- **Open source 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';*
- **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';*
- **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 naturalor legal person established outside the Union';*
- **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';*

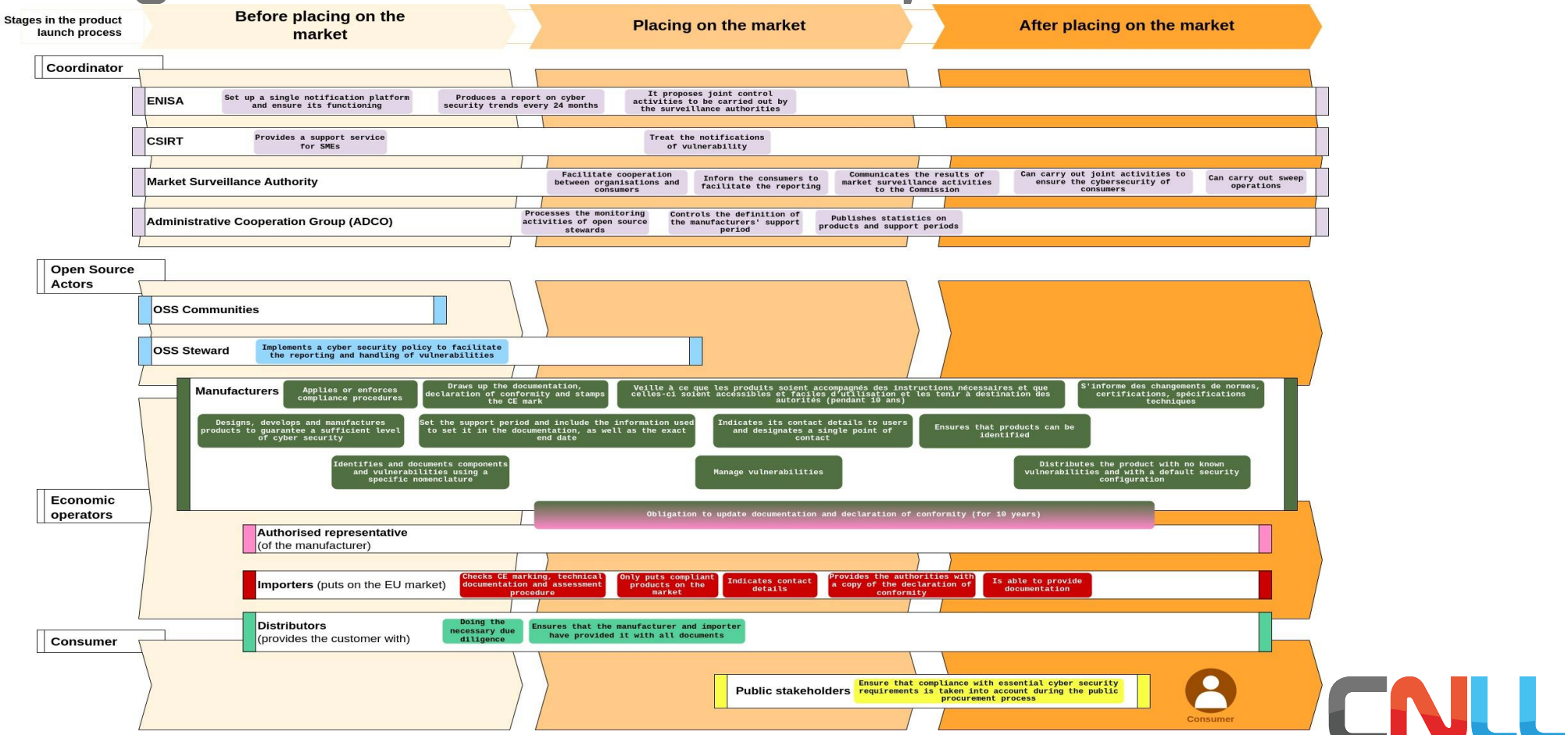
+ administrations

+ contractors and subcontractors

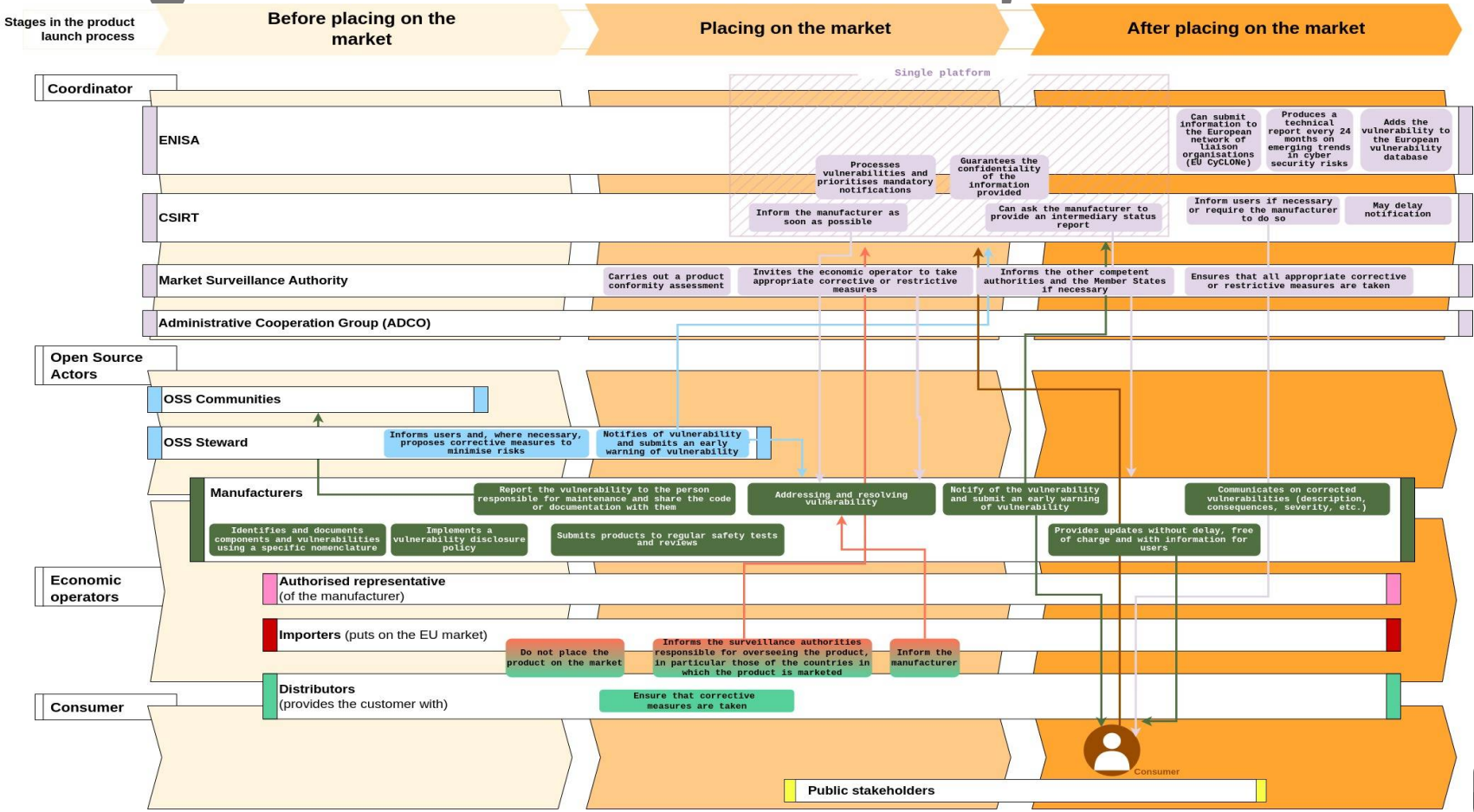
Application of the CRA to Open Source actors



Obligations of the actors subject to the CRA



Obligations of the actors subject to the CRA



Technical documentation as compliance tool

By making the provision of an SBOM almost mandatory, **the CRA aims to make the digital ecosystem ecosystem more resilient and spread best practice from the Open Source ecosystem**.

SBOMs must :

- fit into a potentially complex supply chain by **standardising SBOM formats**
- be **as qualitative and exhaustive as possible** in order to cover the widest range of risks.

There are two main standards for creating SBOMs:

- **SPDX** : developed by legal compliance players under the aegis of the Linux Foundation,
- **CycloneDX** : developed by the security industry under the aegis of the OWASP Foundation (Open Worldwide Application Security Project).

CRA only covers first-level dependencies, whereas good practice aims for greater exhaustiveness

Regulation and sanctions

The CRA establishes a coordinated approach by **designating several regulatory**:

- Market surveillance authorities
- The European Union Agency for Cybersecurity (ENISA)
- Administrative cooperation group (ADCO)
- Computer Security Incident Response Team (CSIRT)

The CRA sets out different ceilings depending on the types of breaches of obligations and the players involved:

- Manufacturer obligations: up to 15 000 000 or up to 2,5 % of the its total worldwide annual turnover
- EU conformity declarations, CE marking, technical documentation… : up to 10 000 000 or up to 2 % of the its total worldwide annual turnover
- The supply of incorrect, incomplete or misleading information to notified bodies: up to 5 000 000 or up to 1 % of the its total worldwide annual turnover

The sanctions provided for in the CRA are significant, but the Regulation leaves the Member States some leeway, as is the case with the GDPR.

Exception for Open Source Steward & micro/SMEs

The virtues associated with the CRA

Security attestation programmes:

- The Commission should be able to **establish voluntary security attestation programmes**
- They would be **accessible to any person or entity developing or using this type of software**, including third-party manufacturers who integrate the products, end users and public administrations in the European Union.
- Regulation authorities can be refered or can refered to themselves for security compliance.
- **Using the open source way of working to improve security**

Personna

		Operators named in the CRA				
		Manufacturer	***Open source steward***	***Authorised representative***	***Importer***	***Distributeur***
Distributor of hardware integrating Open Source components	*Persona #4.1*	(X)				X
Publisher of an Open Source solution	*Persona #4.2*	X				
Contributor to an Open Source Foundation project marketed in Europe	*Persona #4.3*				X	
Open Source solutions **integrator** (with modification)	*Persona #4.4*	X				
Company **operating** SaaS services based on an internal digital solution	*Persona #4.5*	(X)				
Company **using** modified Open Source software	*Persona #4.6*	(X)				

Sigle	***Signification***
X	Probable CRA qualification
(X)	Qualification possible according to specific contexts defined by the CRA

Les entreprises du numérique ouvert

CUBE inno

Q&A

Download the PDF

Download the sources

Stéphane Fermigier (CNLL) & Benjamin Jean (Inno³)

For more informations

The guide is available on : https://cnll.fr/publications/

Sources are available on : https://code.inno3.eu/ouvert/guide-cra

Join the mailing list : mission-cra-cnll@framagroupes.org

Thank you !

Download the PDF

Download the sources