Breakout session CW2

Cyber Resilience Act (CRA) and impact on open source actors

CNLL
Les entreprises du numérique ouvert

CUBE inno

2nd june 14:00 to 16:00

Agenda

- 14:00 – 14:10 **1 | Welcome & setting the scene**
- 14:10 – 14:30 **2 | Round table: where do you stand on the CRA?**
- 14:30 – 15:05 **3 | CRA in 2026: what has changed since last year**
- 15:05 – 15:30 **4 | From theory to practice — the LibreOffice use case**
- 15:30 – 15:50 **5 | Workshop: breakout groups**
- 15:50 – 16:00 **6 | Restitution, wrap-up & next steps**

Stéfane Fermigier
Abilian (CEO) and CNLL (Chairman)

1 | Welcome & Setting the Scene

One year after the OW2con'25 CRA breakout

Where we were in June 2025

- CRA freshly adopted – focus on raising awareness and decoding roles (manufacturer / steward / importer / distributor).
- Many open questions; standardisation not started; no official Commission interpretation.
- Breakout groups around three challenges: “Am I concerned?”, adapting OS processes & tooling, and ecosystem advocacy.

Where we are in June 2026

- First binding deadline is now close: vulnerability & incident reporting from 11 September 2026.
- The European Commission published draft guidance (3 March 2026) – the most reliable interpretation to date.
- The CNLL × inno³ compliance guide reached v2.0; a v3 is anticipated after the final guidance.
- We move from theory to practice: a real compliance programme is under way with LibreOffice / TDF.

2 | Round table: where do you stand on the CRA?

Where do you stand on the CRA?

First, a quick round table :

- Which hat(s) do you wear? : manufacturer, steward, distributor, contributor, just a user, or not sure
- Are your products in scope? : commercial activity, connected product, community vs. enterprise build
- Where are you today? : not started, mapping roles, building documentation, or ready

Share one question :

- One CRA question from your own practice : what worries you most? (SBOM, vulnerability reporting, CE marking, support period, governance) We'll keep them visible and revisit them in the workshop.

Stéfane Fermigier
Abilian (CEO) and CNLL (Chairman)

Benjamin Jean
Inno³ (CEO)

3 | CRA in 2026: what has changed since last year

Access to « CRA compliance guide for Open Source Industry players »

What has changed since OW2con'25

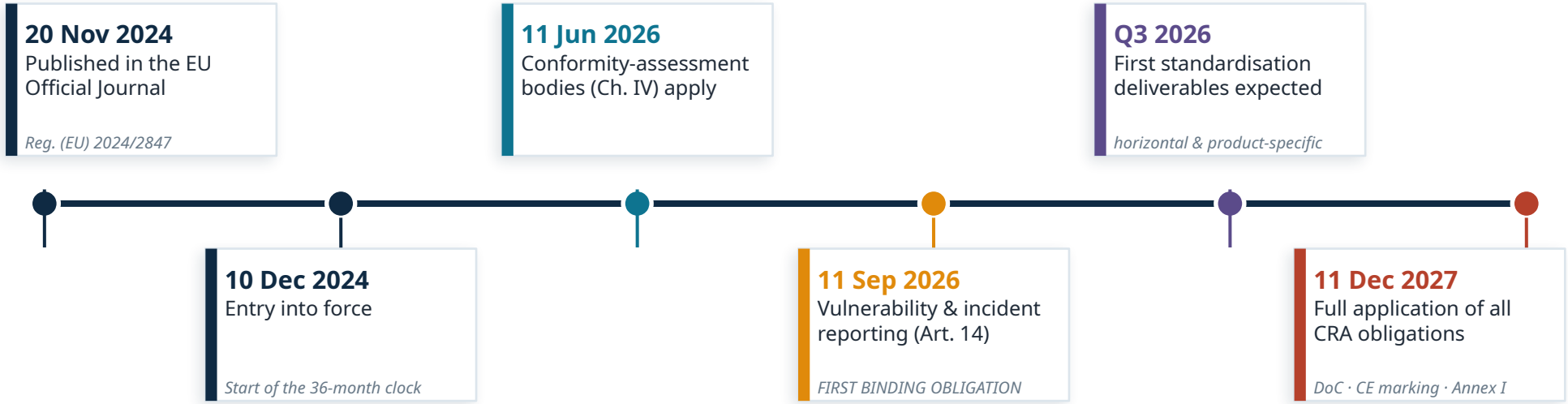
The clock is ticking :

- First binding deadline now close: vulnerability & incident reporting from 11 September 2026 (24h / 72h / 14-day)
- Full application of all CRA obligations on 11 December 2027 (DoC, CE marking, Annex I)
- Standardisation under way - first deliverables expected Q3 2026; the v2.0 CNLL/inno³ guide is out (v3 to follow)

European Commission guidance – 3 March 2026 :

- **Confirms** the guide's reading: commercial activity = monetisation; stewards are not manufacturers; contributors are excluded; per-product dual-track (community vs. enterprise)
- **Clarifies** : remote data processing, substantial modifications, flexible support periods, and 'known' vulnerabilities - no duty to upstream patches
- **Still open** : non-rivalry of FOSS, de-facto control via forges, concrete SME use cases, and SBOM depth — inno³ & CNLL contributed to the EU consultation

Timeline


20 Nov 2024
Published in the EU Official Journal
Reg. (EU) 2024/2847
10 Dec 2024
Entry into force
Start of the 36-month clock
11 Jun 2026
Conformity-assessment bodies (Ch. IV) apply
11 Sep 2026
Vulnerability & incident reporting (Art. 14)
FIRST BINDING OBLIGATION
Q3 2026
First standardisation deliverables expected
horizontal & product-specific
11 Dec 2027
Full application of all CRA obligations
DoC · CE marking · Annex I

Reporting duties from 11 September 2026 (Art. 14)

24h

Early warning

To the relevant CSIRT (and ENISA), via the single reporting platform, on becoming aware of an actively exploited vulnerability or severe incident.

72h

Full notification

Detailed notification including technical indicators, severity and impact, and any corrective/mitigating measures taken.

14 days

Final report

After a corrective measure is available (vulnerabilities). For severe incidents: within one month.

What it means in practice

- A single EU reporting platform operated by ENISA; designate your national CSIRT (ANSSI/CERT-FR is the coordinator CSIRT, while market surveillance of all products with digital elements falls to the ANFR with technical support from ANSSI).
- Applies to products made available on the market – including those placed before Dec 2027.
- Good news for FOSS: a CNA's existing CVE workflows can largely be adapted; no obligation to get patches accepted upstream first.

Context

Context :

- Regulatory approach of the European Union internal market
- NIS (2016), Cybersecurity Act (2019), NIS 2 (2022)
- Proposal of the CRA then new adapted version in response to feedback from open source players

Cyber Resilience Act :

- **Objectives** : strengthen the security of digital products for the benefit of consumers and businesses throughout the European Union
- **How ? :** by introducing new cyber security requirements for any product hardware and software products throughout their lifecycle.
- **When ? :** published the 20th of november 2024 : Economic players will have 36 months to adapt to the new requirements after the entry into force which begin the twentieth day following the publication (until 11 December 2027).

Objectives of the guide

Guide’s objectives :

- The guide has been commissioned by the CNLL (Free software and open digital entreprises Union)
- Objectives: clarify the relationship between the CRA and the specific practices of the Open Source industry

.

Version:

- Version 2.0 (9th of December)
- Available FR on https://code.inno3.eu/ouvert/guide-cra and EN for the Version 1.1

Être prêt pour intégrer le Cyber Resilience Act dans sa pratique Open Source

Guide de conformité au Cyber Resilience Act
à destination des acteurs de la filière Open Source

Version 2.0, publié le 09/12/25

Une étude commandée par le CNLL et réalisée par inno³, diffusée sous licence libre pour être largement partagée et améliorée.

Scope of of the CRA

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

1) ‘**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;
2) ‘**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 12, whether in return for payment or free of charge; or against payment or free of charge ;
3) ‘**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* »;

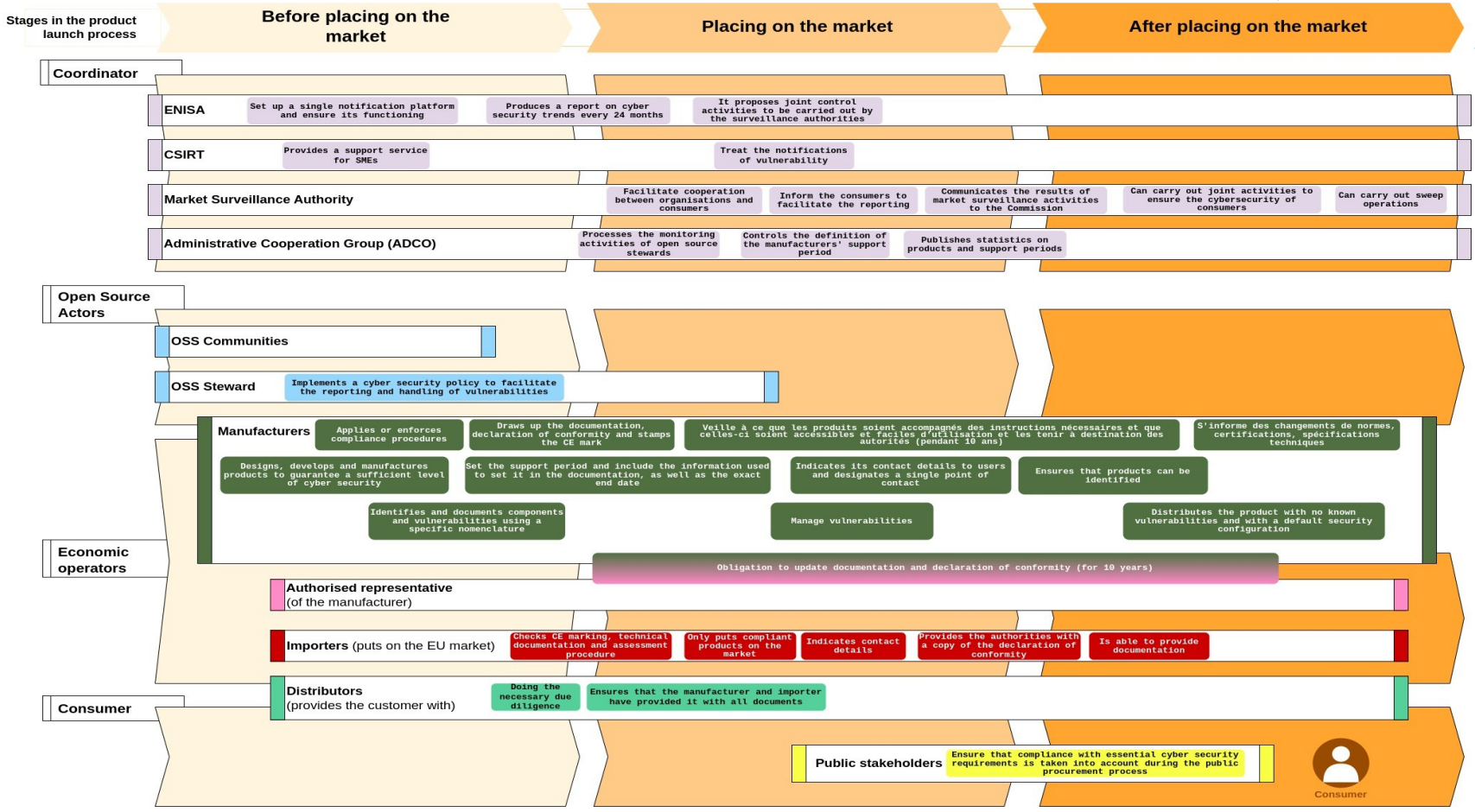
Authorised representative: « *a natural or legal person established within the Union who has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks;* »;

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;* »;

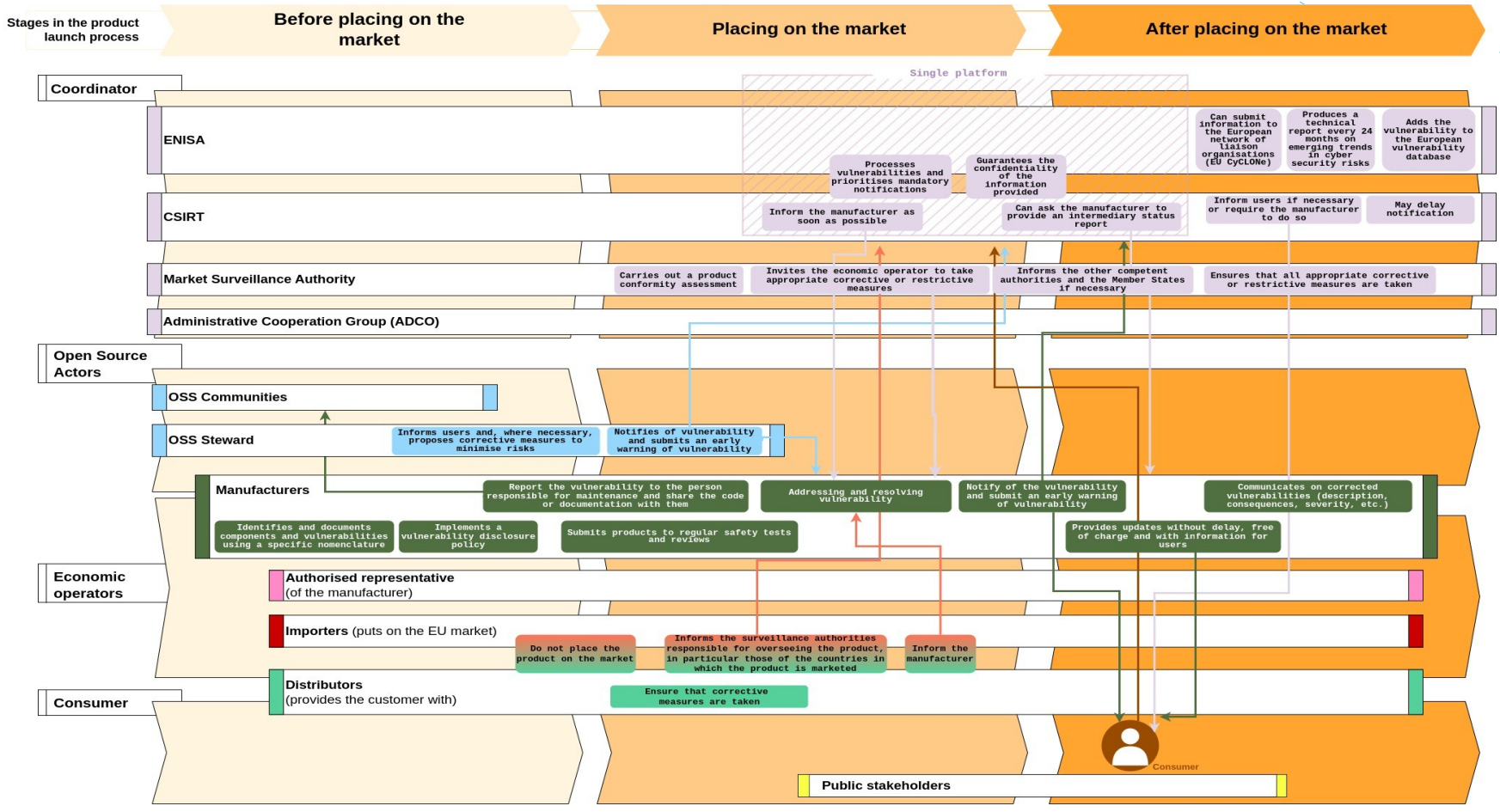
Distributor: «*a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties*; »;

And there contractors...

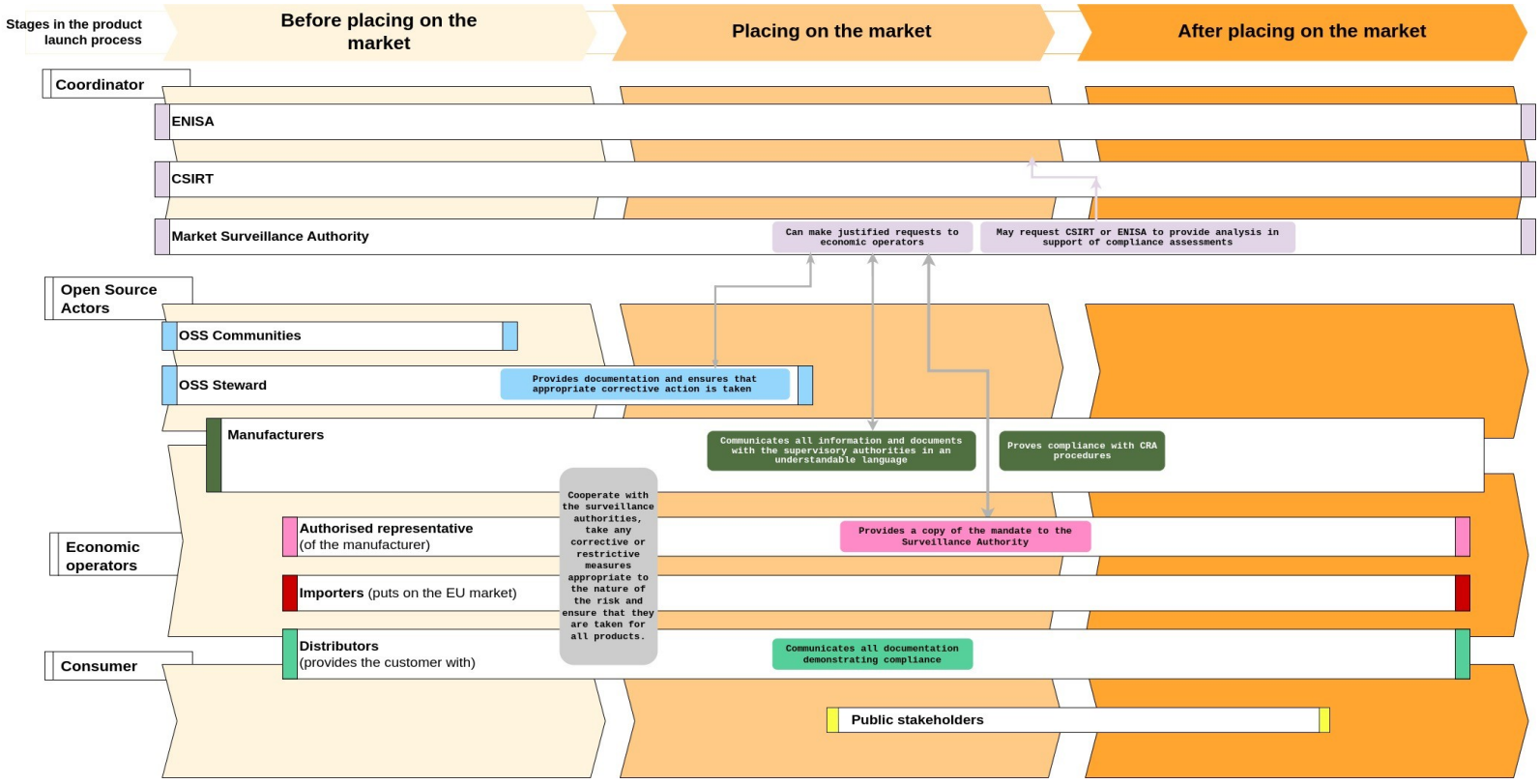
Obligation of actors subject to the CRA



Obligation of actors when vulnerabilities are detected



Obligation of actors subject in case of request, application, assessment



Application of the CRA to Open Source actors

.

Manufacturer:

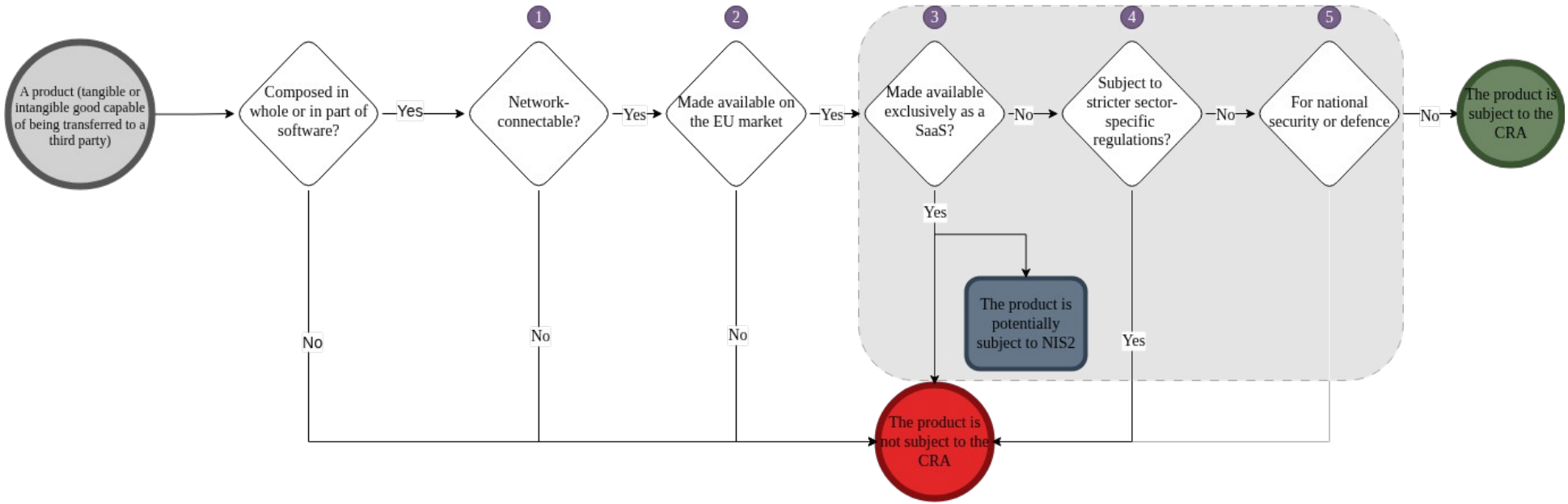
- only the economic players who have legal and certainly technical control (although this is not specifically mentioned in the CRA) over the development of the product. This exclude people who contribute to the development of free and open software that is not under their responsibility (contribution to others'project)
- Difficulties to apprehend how the manufacturer will fullfil their informations obligation (communication on the project's website, mailieng list etc.).
- Assistance period of 5 years which seems complicated in open source context

Distributor:

- software forges (Github, Gitlab, etc.) seem a priori to be excluded (they don't make the product available on the EU market in the economic sense)
- But marketplaces involved in the distribution of software are considered as distributors

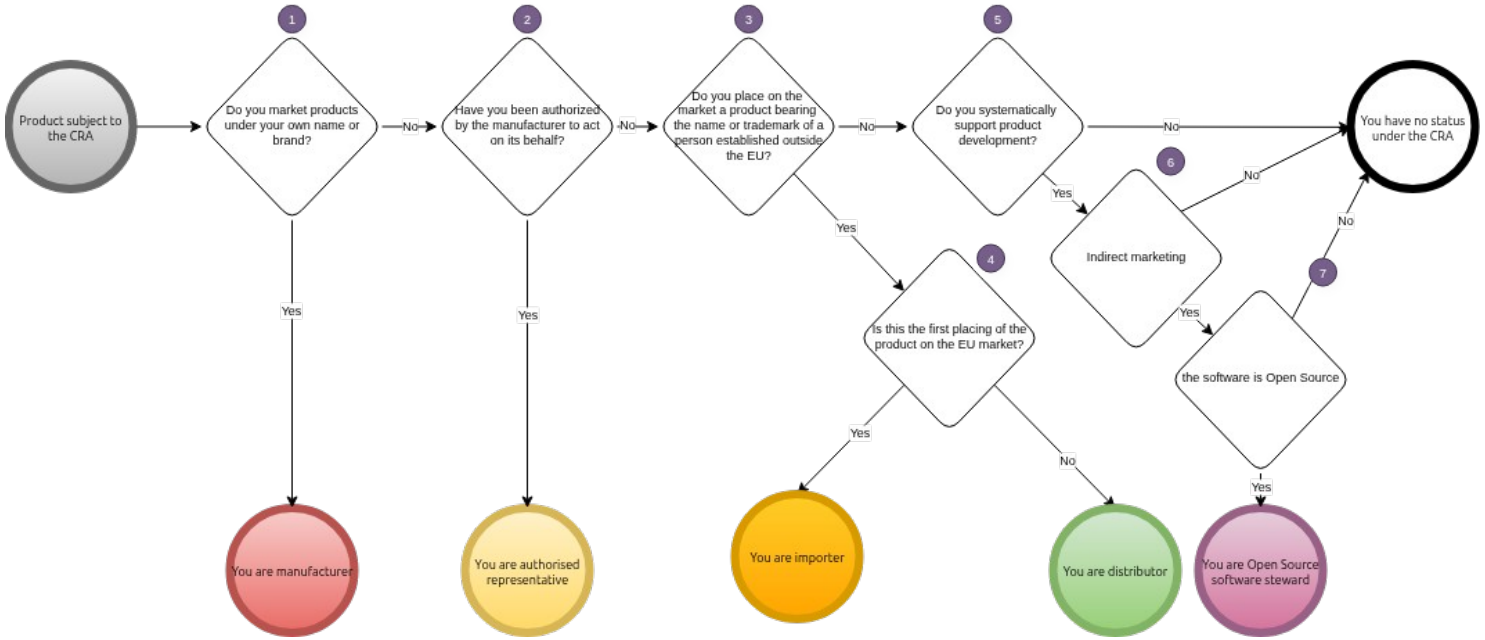
The link between the product and any commercial activity – intent.

Is the product concerned?



The link between the product and any commercial activity – intent.

My activity



Why should the Cyber Resilience Act encourage the use of Open Source in research establishments? Inno³ website : https://inno3.fr/blog/pourquoi-le-cyber-resilience-act-devrait-favoriser-lopen-source-dans-la-valorisation-au-sein-des-etablissements-de-recherche/

Technical documentation as compliance tool

.

Technical documentation : the various economic operators affected by the Regulation will be obliged to archive and preserve evidence of compliance with their obligations. The CRA therefore lays down a strong obligation in terms of the technical documentation associated with the product :

- General description of the product
- Description of design and manufacture
- Cybersecurity risk assessment
- Information on the support period
- List of standards and certifications applied
- Compliance test reports
- EU declaration of conformity
- SBOM (voluntarily or at the request of the regulator)

Technical documentation as compliance tool

.

SBOM : the SBOM has to be a machine-readable document that enables users, suppliers and regulators to know exactly which software components are present in a product.

In practice, all manufacturers of digital products, whether Open Source or proprietary, will be required under the CRA to:

- When there is vulnerabilities : **identify and document vulnerabilities and product components, in particular by drawing up a SBOM**
- **Provide this SBOM when requested by the supervisory authorities**
- **Share information on where it can be consulted** when the manufacturer decides to make it available to the user.

CRA is also **encouraging public administrations to extend compliance their own missions**, which will undoubtedly lead in time to a requirement to be included in all public contracts, following the example of American practices

Articulation with the practices of the Open Source ecosystem

- 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

.

Regulation authorities :

- 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)

Regulation and sanctions

.

Sanctions :

- The CRA sets out certain criteria to be taken into account when deciding the amount of administrative fines:
  - **the nature, seriousness and duration** of the infringement and its consequences ;
  - **any previous administrative fines imposed** on the same economic operator for a similar infringement;
  - **the size and market share** of the economic operator committing the infringement
- 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.

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**

Benjamin Jean
Inno³ (CEO)

4 | From theory to practice - the LibreOffice use case

Scope of the CRA

.

Context : inno^3 accompanies TDF qualified as Manufacturer (and/or OSS Steward for other components) for LibreOffice : “product with digital elements placed on the market”, and helps it for the signing of the EU Declaration of Conformity and the affixing of the CE marking. The methodology and the resulting deliverables are produced so that they can be publicly shared and reused by other open-source organisations.

Methodology :

- **Phase 1 : 3 workshops with TDF team**
  - Product security-by-design baseline
  - CI/CD and infrastructure; vulnerability handling; incident reporting (Art. 14)
  - User-facing information (Annex II); Manufacturer / Steward qualification
- **Phase 2 : Drafting of the technical file, DoC, VHP, user documentation**
- **Phase 3 : TDF affixes CE marking**

Define a CRA compliance diagnostic : SECTION A. Product Security by Design (CRA Art. 13 §§1 to 5)

A1. Risk Assessment (Art. 13 §§2 to 3) :

- Has a cybersecurity risk assessment been conducted for LibreOffice? Methodology used ? Risk assessment documented and maintained as part of the technical documentation?

A2. Secure Design and Development :

- Cybersecurity integration into design and development? Secure coding guidelines or standards?

A3. Vulnerability Handling, process (Art. 13 §6, cross-refs Section C2) :

- Current vulnerability handling process?

A4. Software Bill of Materials (SBOM) :

- SBOM currently generated? Format (SPDX or CycloneDX)? SBOM covers transitive dependencies? Frequency / automation of SBOM generation?

A5. Security Updates and Support (Art. 13 §8) :

- Policy for providing security updates? Distribution mechanism?

A6. Technical Documentation, Conformity Assessment, DoC and CE Marking (Art. 13 §§7 to 14, Art. 32, Annex V, VII, VIII) :

- Policy for providing security updates? Distribution mechanism?

Define a CRA compliance diagnostic : SECTION B. Vulnerability and Incident Reporting to ENISA / CSIRT (CRA Art. 14)

B1. Identification and internal workflow :

- Process for identifying actively exploited vulnerabilities? Process for identifying severe incidents (Art. 23)?

B2. Timelines :

- 24h early warning capability? 72h full notification? 14-day final report?

B3. Authority designation and platform registration :

- ENISA single reporting platform awareness? National CSIRT designation (BSI / CERT-Bund)?

B4. User notification :

- Process for notifying affected users? End-users vs downstream distributors?

B5. CNA leverage :

- Existing workflows adaptable to ENISA reporting? Current CVE load per year?

Define a CRA compliance diagnostic : SECTION C. Essential Cybersecurity Requirements (CRA Annex I)

C1. Security Properties (Annex I §§1 to 13 of Part I) :

- Protection from unauthorised access,
- Confidentiality,
- Integrity.

C2. Vulnerability Handling (Annex I Part II §§1 to 7) :

- Identify and document,
- Effective and regular tests,
- Public disclosure

Define a CRA compliance diagnostic : other

SECTION D. Information and Instructions to the User (CRA Annex II) :

- Manufacturer identity
- Single point of contact for cybersecurity
- ...

SECTION E. Additional Context and Infrastructure :

- CI/CD pipeline?
- Compliance certifications
- ...

SECTION F. Manufacturer / OSS Steward Qualification :

- Manufacturer, Steward, or both?
- “Placed on market” vs “made available”?
- ...

5 | Workshop: breakout groups

How the workshop works

Format :

- Three groups · ~20 min discussion · 5 min report-back each · appoint a note-taker
- Capture notes on the shared pad; we project the restitution table

Each group brings back :

- 1 key insight · 1 open question · 1 concrete next step

Workshop — three breakout groups

Group 1 — Am I Concerned? Understanding My Role & Obligations.

Focus Questions: How do I determine if the CRA applies to my OS activities? Which economic operator role(s) might I fit (Manufacturer, Steward, Importer, Distributor, or outside scope)? What are the immediate vs long-term obligations for that role? Using CNLL/inno³ scenarios as a starting point.
Facilitator: Benjamin Jean (inno³).

Group 2 — Technical Deep Dive: Adapting OS Processes & Tooling.

Focus Questions: What practical changes are needed in development lifecycles (SDL)? How to effectively implement SBOMs (tools, standards like SPDX/CycloneDX)? Best practices for vulnerability management and coordinated disclosure in an OS context? What tools are emerging (e.g., from OCCTET) or needed?
Facilitator: Stéfane Fermigier (Abilian / CNLL).

Group 3 — Reuse & Ecosystem: Building on the LibreOffice Path.

Focus Questions: Could a shared, open compliance template (like the one built with LibreOffice) help your project? What would you need from it? How do we collectively engage standardisation bodies (CEN/CENELEC/ETSI) and shape CRA implementation in favour of FOSS?
Facilitator: Arthur Hamonic (inno³).

Stéfane Fermigier
Abilian (CEO) and CNLL (Chairman)

6 | Restitution, wrap-up & next steps

Restitution — what each group brings back

Each group reports back :

- Group 1 — Role & obligations: insight … / open question … / next step …
- Group 2 — Processes & tooling (SBOM, vulnerabilities): insight … / open question … / next step …
- Group 3 — Reuse & ecosystem (LibreOffice path): insight … / open question … / next step …

Then :

- We consolidate the open questions and next steps into the report and the CNLL × inno³ working-group roadmap.

What next — and how to join us

.

What next ?

The working group led by the CNLL and inno³ will continue to meet over the coming months to develop aspects not yet covered by the guide :

- implementation of the CRA within **community projects, public procurement or research establishments;**
- illustrate these elements by **developing concrete use cases** involving several players and service providers within a complex product

As this group is open, don't hesitate to join us!

Annexes

Example

Librebox Company

Hardware distribution

Description

As part of my commercial activities, I distribute (on a rental basis) hardware that incorporates software that is partly Open Source and partly proprietary. I also use service providers who use Open Source software developed by third parties to design, develop or manufacture software that I then market under my own name or brand.

Answer to CRA

Scope

Article 2§1 : Article 3§1

Hardware products distributed as part of a commercial activity	Company subject to the CRA (not its service providers)

Qualification under the CRA

Products integrated without modification	Distributor
Calling on service providers to design, develop or manufacture products	Manufacturer

Obligations

If it has distributor status

- Applying due diligence to integrated third-party components,
- Adapt due diligence to the level of cybersecurity risk of each component,
- Possible verification measures :
  - Check that the manufacturer of the component complies with the regulation (e.g. presence of CE marking),
  - Confirm that the component receives regular security updates,
  - Ensure that there are no vulnerabilities in public vulnerability databases (such as the EU's),
  - Perform additional safety tests if necessary.

If it has manufacturer status

- Apply the CRA's conformity procedures for the product(s),
- Obtain a declaration of conformity and apply the CE mark,
- Design and produce the product with a sufficient level of cyber security:
  - No known vulnerabilities,
  - Security by default,
  - Appropriate controls,
  - Protection of data confidentiality and integrity,
  - Possibility for users to delete their data.
- Maintain accurate documentation, including an SBOM (Software Bill of Materials),
- Update this documentation for 10 years after it has been launched on the market,
- Report any detected vulnerabilities or incidents to the authorities and stakeholders,
- Correct vulnerabilities and provide patches for at least 5 years after market launch.

Example

Freesoft Company

Open source solution provider

Description

I publish an Open Source solution under my name/brand and offer complementary services. I use Open Source software published by other companies or by an informal community within my solution.

Answer to CRA

Scope

Marketing digital products → Company subject to the CRA

Article 351: Définitions
Recital 15

Qualification under the CRA

Marketing of products with provision of services under own name/brand → Manufacturer

Obligations

When using open source solutions published by other companies or by an informal community

- Applying due diligence to integrated third-party components,
- Adapt due diligence to the level of cybersecurity risk of each component,
- Possible verification measures :
  - Check that the manufacturer of the component complies with the regulation (e.g. presence of CE marking),
  - Confirm that the component receives regular security updates,
  - Ensure that there are no vulnerabilities in public vulnerability databases (such as the EU's),
  - Perform additional safety tests if necessary.

When the Open Source solution is launched on the market

- Apply the CRA's conformity procedures for the product(s),
- Obtain a declaration of conformity and apply the CE mark,
- Design and produce the product with a sufficient level of cyber security:
  - No known vulnerabilities,
  - Security by default,
  - Appropriate controls,
  - Protection of data confidentiality and integrity,
  - Possibility for users to delete their data.
- Maintain accurate documentation, including an SBOM (Software Bill of Materials),
- Update this documentation for 10 years after it has been launched on the market,
- Report any detected vulnerabilities or incidents to the authorities and stakeholders,
- Correct vulnerabilities and provide patches for at least 5 years after market launch.

Example

Directlibre Company

Contributor

Description

I contribute to Open Source software developed under the leadership of an American Open Source Foundation, which I import into the European market under its brand name.

Answer to CRA

Recital 18
Article 2

Scope

Contribution to software	Simply contributing to software does not trigger the CRA
Marketing digital products on the European market	Company subject to the CRA

Qualification under the CRA

Marketed in Europe under the brand name of the American foundation	Importer

Obligations

With importer status

- Check the CE marking, the technical documentation and the assessment procedure,
- Only launch compliant products on the market,
- Provide contact details,
- Keep a copy of the declaration of conformity available for the authorities,
- Be able to provide documentation,
- Inform the authorities and the manufacturer in the event of vulnerabilities.

Example

Consultime Company

Integrator

Description

I'm integrating a digital solution to meet my client's needs as part of a public procurement contract. To do this, I'm using an existing Open Source solution developed by an informal community of major users, which I'm modifying substantially. I'm thinking about launching this solution to market.

Answer to CRA

Scope

Article 3§1:
Article 5
Recital 15

If the product is for the exclusive internal use of the public authority only	Public players subject to the CRA, but not the company
If placed on the market	Company subject to the CRA

Qualification under the CRA

If the substantially modified product is marketed	Manufacturer

Obligations

For the public sector

- Ensure that compliance with essential cyber security requirements is taken into account during the public procurement process.

Use of the solution developed by an informal community

- Applying due diligence to integrated third-party components,
- Adapt due diligence to the level of cybersecurity risk of each component,
- Possible verification measures :
  - Check that the manufacturer of the component complies with the regulation (e.g. presence of CE marking),
  - Confirm that the component receives regular security updates,
  - Ensure that there are no vulnerabilities in public vulnerability databases (such as the EU's),
  - Perform additional safety tests if necessary.

Market launch of the open source solution

- Apply the CRA's conformity procedures for the product(s),
- Obtain a declaration of conformity and apply the CE mark,
- Design and produce the product with a sufficient level of cyber security:
  - No known vulnerabilities,
  - Security by default,
  - Appropriate controls,
  - Protection of data confidentiality and integrity,
  - Possibility for users to delete their data.
- Maintain accurate documentation, including an SBOM (Software Bill of Materials),
- Update this documentation for 10 years after it has been launched on the market,
- Report any detected vulnerabilities or incidents to the authorities and stakeholders,
- Correct vulnerabilities and provide patches for at least 5 years after market launch.

Example

Oneline Company

Saas Operator

Description

I'm the SaaS operator of a digital product designed on the basis of an Open Source solution from an American publisher that I've substantially modified.

Answer to CRA

Recital 12
Article 2
Article 22

Scope

If the SaaS solution is not directly linked to the product or is not essential for the product's functionality	Company not subject to the CRA but to the NIS2 directive
If the SaaS solution directly serves the digital product and is designed to support its functionality	Company subject to the CRA

Qualification under the CRA

Market launch of the substantially modified Open Source solution	Manufacturer

Obligations

If it has manufacturer status

- Apply the CRA's conformity procedures for the product(s),
- Obtain a declaration of conformity and apply the CE mark,
- Design and produce the product with a sufficient level of cyber security:
  - No known vulnerabilities,
  - Security by default,
  - Appropriate controls,
  - Protection of data confidentiality and integrity,
  - Possibility for users to delete their data.
- Maintain accurate documentation, including an SBOM (Software Bill of Materials),
- Update this documentation for 10 years after it has been launched on the market,
- Report any detected vulnerabilities or incidents to the authorities and stakeholders,
- Correct vulnerabilities and provide patches for at least 5 years after market launch.

Example

Sportsfree Company

Merchandise seller

Description

I use an Open Source solution, fully configured to meet my needs, to sell my products online. I would like to market this solution.

Answer to CRA

Scope

Article 2

If the solution is only used to offer services	Company not subject to the CRA
If the Open Source solution is marketed	Company subject to the CRA

Qualification under the CRA

If marketing the solution under its own name/brand	Manufacturer

Obligations

If it has manufacturer status

- Apply the CRA's conformity procedures for the product(s),
- Obtain a declaration of conformity and apply the CE mark,
- Design and produce the product with a sufficient level of cyber security:
  - No known vulnerabilities,
  - Security by default,
  - Appropriate controls,
  - Protection of data confidentiality and integrity,
  - Possibility for users to delete their data.
- Maintain accurate documentation, including an SBOM (Software Bill of Materials),
- Update this documentation for 10 years after it has been launched on the market,
- Report any detected vulnerabilities or incidents to the authorities and stakeholders,
- Correct vulnerabilities and provide patches for at least 5 years after market launch.

		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

The virtues associated with the CRA

.

What next ?

The working group led by the CNLL and inno³ will continue to meet over the coming months to develop aspects not yet covered by the guide :

- implementation of the CRA within **community projects, public procurement or research establishments;**
- illustrate these elements by **developing concrete use cases** involving several players and service providers within a complex product

As this group is open, don't hesitate to join us!