

EOLE 2024

15th edition

Navigating the New EU Regulatory Landscape in Open Source

29 November 2024

Turin



Schedule

1 – CRA and Open Source

🕒 10:00 – 12:00

2 – AI Act and Open Source

🕒 13:30 – 15:30

3 – Open Science and Open Source

🕒 16:00 – 17:30

4 – Going on a broader level (competition law, Market regulation, etc)

🕒 17:30 – 18:30

1 – CRA and Open Source

🕒 10:00 – 12:00

Speaker

- *Benjamin Jean, inno³*
- *Moderators : Arthur Hamonic and Clémence Lascombes (inno³)*

Summary

- Presentation of the interest of the subject and the study carried out in France on behalf of the CNLL (30')
- Shared discussions with the workshop participants in order to identify and specify the areas of work to be carried out collectively (30')
- Design of sub-groups and work by sub-groups based on a shared analysis framework (30')
- Summary of contributions and conclusion (30')

Presentation of the interest of the subject and the study

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

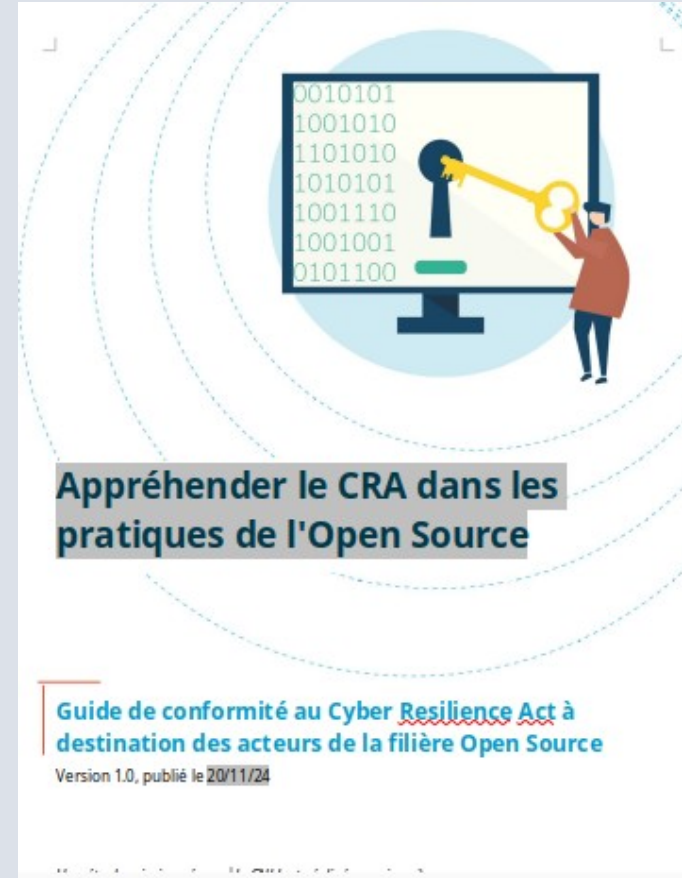
Cyber Resilience Act :

- **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 enterprises Union)
- Objectives: clarify the relationship between the CRA and the specific practices of the Open Source industry



Scope 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 »;

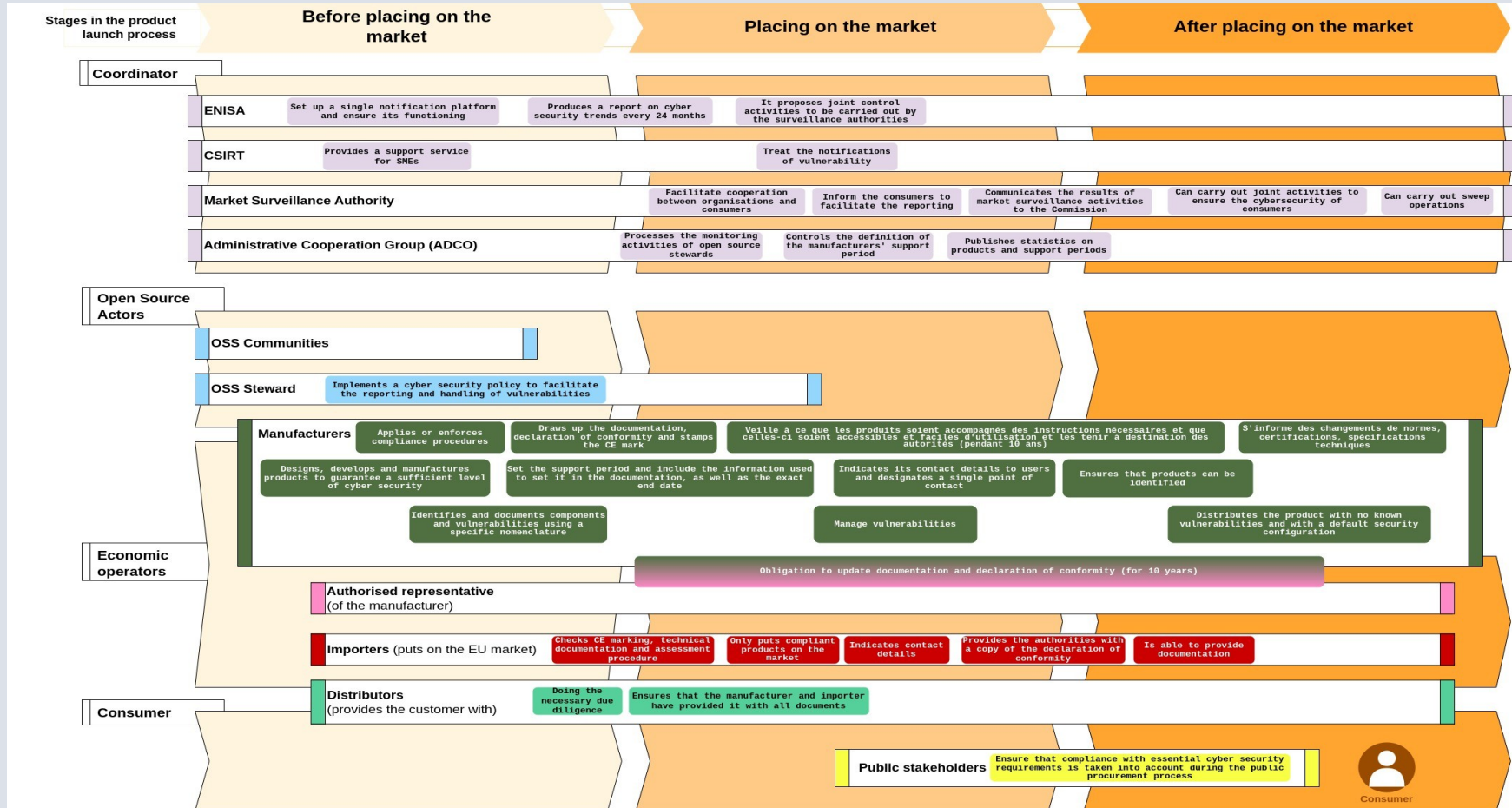
Open source steward: « a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities,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

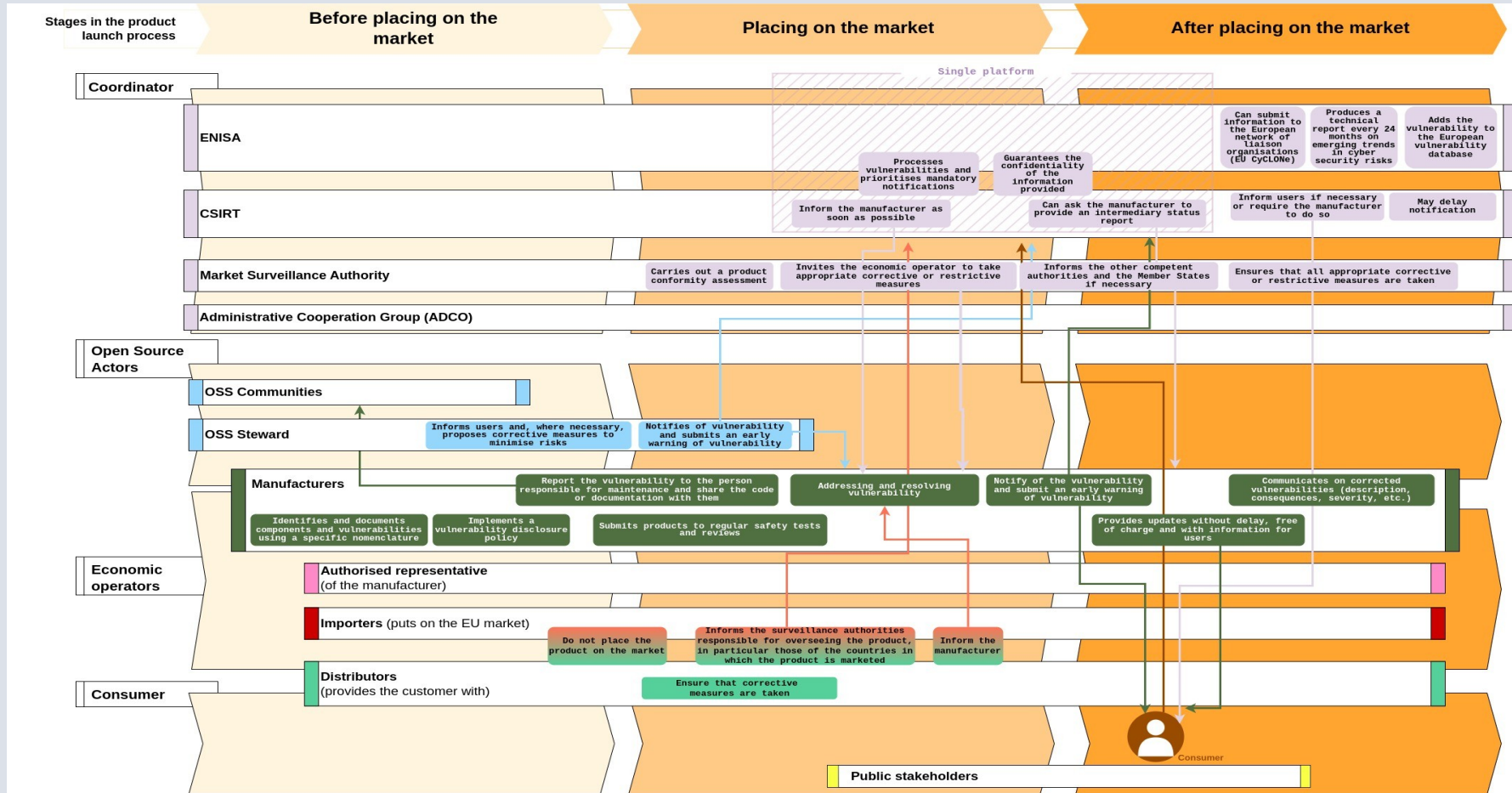
Importer: « a natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union; »;

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; »;

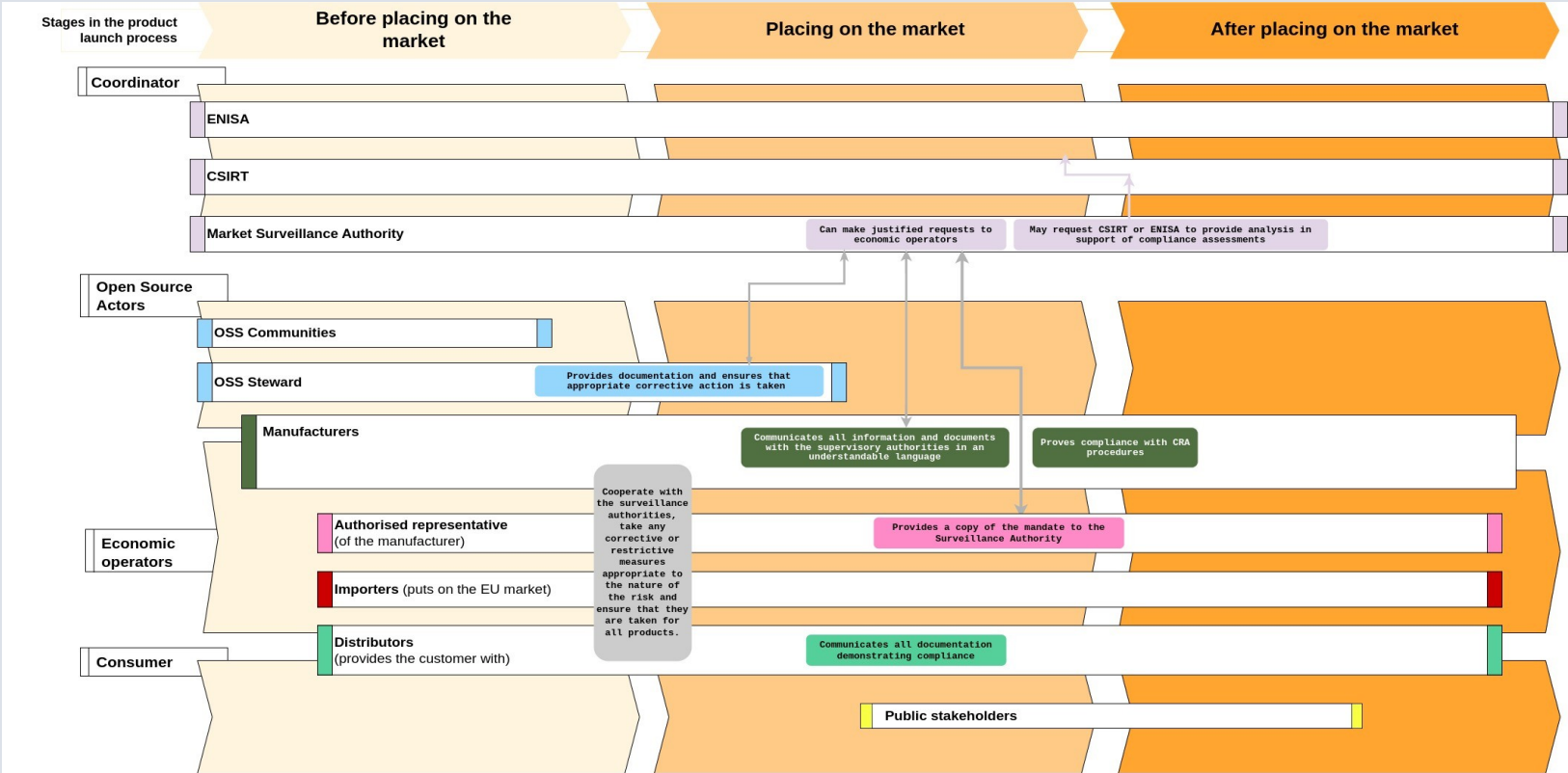
Obligation of actors subject to the CRA



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

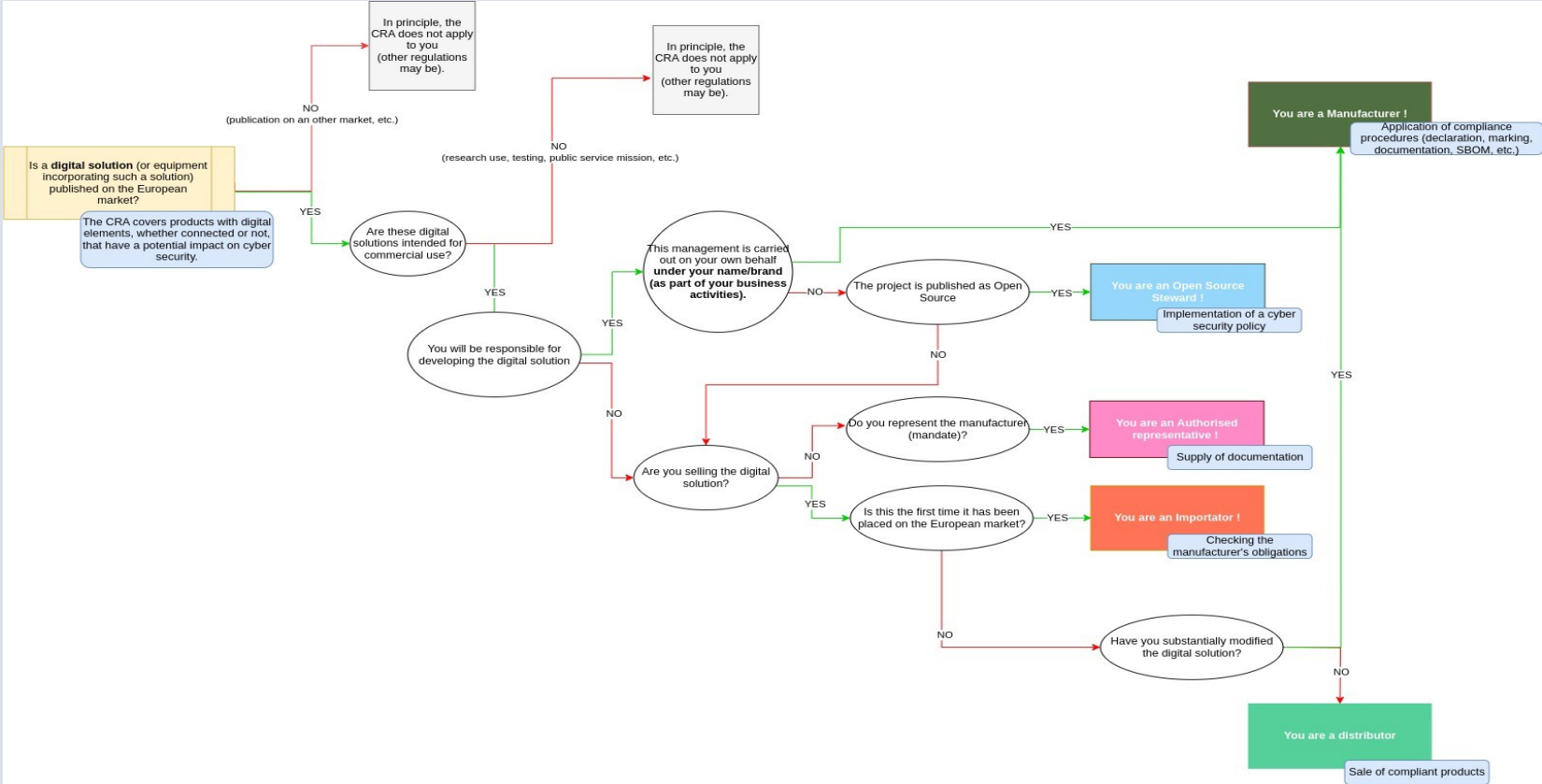
Manufacturer:

- 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

Application of the CRA to Open Source actors



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:




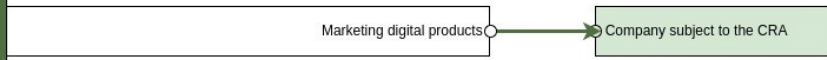
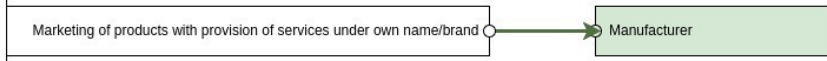
- The Commission should be able to **establish voluntary security attestation programmes**
- They would be **accessible to any person or entity developing or using this type of software**, including third-party manufacturers who integrate the products, end users and public administrations in the European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

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
	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
	<ul style="list-style-type: none">• Applying due diligence to integrated third-party components,• Adapt due diligence to the level of cybersecurity risk of each component,• Possible verification measures :<ul style="list-style-type: none">◦ 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
	<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">◦ 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.




Article 251:
Article 351


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
	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 <ul style="list-style-type: none">• Applying due diligence to integrated third-party components.• Adapt due diligence to the level of cybersecurity risk of each component,• Possible verification measures :<ul style="list-style-type: none">◦ 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 <ul style="list-style-type: none">• 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:<ul style="list-style-type: none">◦ 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.

Article 3(1):
Definitions
Recital 15




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						
	Scope						
	<table border="0"><tr><td>Contribution to software</td><td>→</td><td>Simply contributing to software does not trigger the CRA</td></tr><tr><td>Marketing digital products on the European market</td><td>→</td><td>Company subject to the CRA</td></tr></table>	Contribution to software	→	Simply contributing to software does not trigger the CRA	Marketing digital products on the European market	→	Company subject to the CRA
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						
	<table border="0"><tr><td>Marketed in Europe under the brand name of the American foundation</td><td>→</td><td>Importer</td></tr></table>	Marketed in Europe under the brand name of the American foundation	→	Importer			
Marketed in Europe under the brand name of the American foundation	→	Importer					
	Obligations						
	With importer status						
	<ul style="list-style-type: none">• 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.						






Recital 18
Article 2

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 <table border="1"><tr><td>If the product is for the exclusive internal use of the public authority only</td><td>Public players subject to the CRA, but not the company</td></tr><tr><td>If placed on the market</td><td>Company subject to the CRA</td></tr></table>	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		
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 <table border="1"><tr><td>If the substantially modified product is marketed</td><td>Manufacturer</td></tr></table>	If the substantially modified product is marketed	Manufacturer				
If the substantially modified product is marketed	Manufacturer						
	Obligations <table border="1"><tr><td>For the public sector</td><td><ul style="list-style-type: none">Ensure that compliance with essential cyber security requirements is taken into account during the public procurement process.</td></tr><tr><td>Use of the solution developed by an informal community</td><td><ul style="list-style-type: none">Applying due diligence to integrated third-party components.Adapt due diligence to the level of cybersecurity risk of each component.Possible verification measures :<ul style="list-style-type: none">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.</td></tr><tr><td>Market launch of the open source solution</td><td><ul style="list-style-type: none">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:<ul style="list-style-type: none">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.</td></tr></table>	For the public sector	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Applying due diligence to integrated third-party components.Adapt due diligence to the level of cybersecurity risk of each component.Possible verification measures :<ul style="list-style-type: none">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	<ul style="list-style-type: none">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:<ul style="list-style-type: none">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.
For the public sector	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Applying due diligence to integrated third-party components.Adapt due diligence to the level of cybersecurity risk of each component.Possible verification measures :<ul style="list-style-type: none">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	<ul style="list-style-type: none">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:<ul style="list-style-type: none">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.						




Article 351:
Article 5
Recital 15

Example

	Online 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						
	Scope						
	<table border="1"><tr><td>If the SaaS solution is not directly linked to the product or is not essential for the product's functionality</td><td>→</td><td>Company not subject to the CRA but to the NIS2 directive</td></tr><tr><td>If the SaaS solution directly serves the digital product and is designed to support its functionality</td><td>→</td><td>Company subject to the CRA</td></tr></table>	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
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						
	<table border="1"><tr><td>Market launch of the substantially modified Open Source solution</td><td>→</td><td>Manufacturer</td></tr></table>	Market launch of the substantially modified Open Source solution	→	Manufacturer			
Market launch of the substantially modified Open Source solution	→	Manufacturer					
	Obligations						
	<p style="text-align: center;">If it has manufacturer status</p> <ul style="list-style-type: none">• 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:<ul style="list-style-type: none">◦ 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.						

Recital 12
Article 2
Article 22

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						
	<table border="1"><tr><td>If the solution is only used to offer services</td><td>→</td><td>Company not subject to the CRA</td></tr><tr><td>If the Open Source solution is marketed</td><td>→</td><td>Company subject to the CRA</td></tr></table>	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
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						
	<table border="1"><tr><td>If marketing the solution under its own name/brand</td><td>→</td><td>Manufacturer</td></tr></table>	If marketing the solution under its own name/brand	→	Manufacturer			
If marketing the solution under its own name/brand	→	Manufacturer					
	Obligations						
	If it has manufacturer status						
	<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">◦ 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.						



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

<i>Sigle</i>	<i>Signification</i>
X	Probable CRA qualification
(X)	Qualification possible according to specific contexts defined by the CRA

Part 2 - workshop

1) Shared discussions in order to identify and specify the areas of work to be carried out collectively

2) Work by sub-groups based on a shared analysis framework

3) Global summary of contributions and conclusion

Any question ?

Shared discussions in order to identify and specify the areas of work to be carried out collectively

Shared discussions with the workshop participants in order to identify and adapt the areas of work to be carried out collectively (30')

Areas to be discussed:

- 1) What application of the CRA in the context of administrations activities? What about their obligation to apply the CRA in their relations with third parties?
- 2) What are non-commercial activities therefore excluded from the CRA
- 3) How can an Open Source players apply their obligations to widely dispersed 'customers'/users?
- 4) Is the condition of control, i.e. publication under the brand name or under the name of the manufacturer, in line with/adapted to the uses of Open Source (as Elastic Search for example)?
- 5) What choice of SBOM standard and what expectations?
- 6) How can we systematise/accompany the upstream contributions?
- 7) How these new responsibilities can be implemented in the Open Source policy of an OS publisher/integrator?
- 8) Other ?

Work by sub-groups based on a shared analysis framework

Design of sub-groups and work by sub-groups based on a shared analysis framework (30')

Instructions:

- 1) Defining small working group with one referent on one of the previous topic (10')
- 2) Discussing about the topic(10')
- 3) Summarizing few reflexions to the other groups (10')

Working group 1:

- Subject :

Working group 2:

- Subject :

Working group 3:

- Subject :

Summary of contributions and conclusion

Summary of contributions and conclusion (30')

Summary:

- Working group 1:
- Working group 2:
- Working group 3:

Conclusion

-

Thanks you for your attention !

For further question, contact us at eole2023@inno3.fr