Be ready to integrate the Cyber Resilience Act into your Open Source practice

Cyber Resilience Act Compliance Guide for Open Source Industry Players

Version 1.0, published on 18/12/24

A study commissioned by the CNLL and carried out by inno³, distributed under an open licence so that it can be widely shared and improved.

Contents

Version	Date	Author	Comments
1.0	18/12/24	Inno³	First version.

Acknowledgements and credits

Since 2010, the CNLL (Union des entreprises du logiciel libre et du numérique ouvert) has served as the representative organisation in France for companies in the Open Source sector. Its objective is to unite free software companies in a spirit of community and shared values, with the aim of representing and defending the free software and Open Source industry in France. In line with its remit, the CNLL has commissioned inno³ to produce a guide to raising awareness of the CRA for Open Source stakeholders.

⇒ Please visit https://cnll.fr for more information.

inno³ is an independent consultancy specialising in open models, operating at the crossroads between the private sector (industry and the social economy), the public sector (government and local authorities) and the community. The firm employs a multidisciplinary team that is actively engaged in raising awareness of open and collaborative models. Inno³ is a founding member of the OpenSource-Experts initiative, which aims to provide key accounts with access to Open Source expertise from a number of specialist players.

⇒ Please visit https://inno3.fr for more information.

Coordination and editing

The main editors are Benjamin Jean (CEO, inno³) and Arthur Hamonic (PhD student and junior consultant, inno³). The illustrations and visualisations were produced by Clémence Lascombes (project manager, inno³).

The editorial and coordination team comprises up of Stéfane Fermigier (CNLL co-president) and Catherine Nuel (CNLL project manager).

Monitoring Committee and contributions

A monitoring committee participated in the various discussions, and provided input on the form and content of the project. The committee is comprised of technical experts, legal experts and representatives from the Open Source community: Cedric Temple (Bluemind), Clément Oudot (Worteks), Florent Zara (Eclipse Foundation), Gaël Blondelle (Eclipse Foundation), Pierre-Yves Gibello (OW2), Simon Urli (xwiki), Victor ROLAND (Obéo), Vincent Picavet (Oslandia), Vincent Pouzol (Systerel) and Yannick Moy (AdaCore).

The results of this study were presented at the European Opensource & Free Sofware Law Event on 29 November 2024 in Turin and include a number of remarks and comments from European lawyers and experts. The document also includes contributions from Frédéric Duflot, a cybersecurity specialist and co-founder of Examin.

1.1 | Legal information

This guide and its accompanying illustrations are available for use under a [Creative Commons By-SA 4.0](#) licence. This licence allows for optimal dissemination and facilitates updates.

It is available on the CNLL website (https://cnll.fr/publications) and the various resources that make it up are published individually on [inno³'s gitlab](#).

Please direct any queries regarding the sponsoring organisations to: [hello@inno3.fr](#) and [contact@cnll.fr](#).

The fonts used are Roboto (by Christian Robertson, released under [Apache-2.0](#)) and [Mina](#) (©2015 Mina Project Authors, released under [SIL Open Font License 1.1](#)). The illustration used on the cover (illustration of the cybersecurity concept) is licensed under the [Free Digital License](#).

Foreword

Against a backdrop of growing vulnerability of European society to cyber risks, the European Commission presented the Cyber Resilience Act (CRA) in September 2022. The CRA is an ambitious regulation aimed at improving the cybersecurity and cyber resilience of digital products marketed within the European Union. The text was formally adopted in 2024 and introduces strict obligations for economic players concerned, as well as enshrining the principle of "by design" digital security at every stage of the product lifecycle.

The CRA represents a significant step forward in enhancing digital security across Europe. However, it also presents a number of notable challenges, particularly for the Open Source industry, which represents 10% of the European IT sector. The intense debates that have marked its development have highlighted a conceptual gap between those responsible for the regulation within the Commission and the practical and economic realities of the professional Open Source sector. While the final text includes exemptions for non-commercial, not-for-profit Open Source projects, it nonetheless imposes complex requirements for products and services incorporating Open Source software within a very broadly defined economic framework. The new regulations require detailed technical documentation, rigorous vulnerability management, a declaration of conformity and CE marking, and the production of a Software Bill of Materials (SBOM). These obligations necessitate significant adaptations while preserving the fundamental principles and ethical values of Open Source. The technical, organisational and financial challenges will have a significant impact on industry players, potentially leading to demotivation for some.

Aware of these challenges, the CNLL (Union des entreprises du logiciel libre et du numérique ouvert) and inno³ have joined forces to create this practical guide. This guide has been developed to assist Open Source players in complying with the CRA. It is based on a collaborative approach and has been informed by in-depth discussions with technical, legal and economic experts within the industry. The objective is to provide practical, appropriate tools to help organisations meet these challenges while also highlighting the intrinsic strengths of Open Source software in building a safer, more resilient digital environment.

The objective of this guide is to:

- Clarify the main requirements of the CRA and their specific application to Open Source practices.

- Provides concrete, achievable recommendations for integrating these new obligations into existing processes.

- Facilitating a shared understanding of the challenges of the CRA within the Open Source ecosystem, combining theoretical insight with practical feedback.

- Propose methods for positively influencing the interpretation and implementation of the Regulation's requirements at the European level.

This work is based on a study carried out by inno³, supplemented by two scoping and feedback meetings and a workshop that brought together key players from the CNLL, members of the association and external partners.

This document represents an invitation to continue the dialogue between legislators, industry and Open Source communities with a view to ensuring a balanced and sustainable implementation of the CRA's objectives. It may also be subject to further development to incorporate new specificities and feedback from our members, as well as from major users, public administrations and other contributors.

The CRA represents a significant shift for Open Source software companies in Europe. It marks the end of the principle of no liability outside of a commercial relationship, which has previously formed the basis of many Open Source software publishers' business models. Despite this, the CNLL aims to provide Open Source companies with the tools to transform this regulatory challenge into an opportunity. This will be achieved by identifying and adopting practices that strengthen the trust and resilience of their products and services.

Stefane Fermigier

Co-chairman of the CNLL

2 | Introduction

2.1 | Increasingly regulated digital environment

Over the past ten years, the European legislator has produced a number of regulations[1] aimed at providing a framework for and supporting the uses and practices of "economic operators" as part of its regulatory approach[2] to the European Union (EU) internal market in digital matters. Among these, the Cyber Resilience Act (CRA)[3] has the objective of enhancing cybersecurity for the benefit of consumers and businesses. The EU is using this policy to support the development of a society based on a **strong and trusted digital environment that puts people first**.[4] This is achieved by combining technical, economic and human considerations.

The CRA was published in the EU's Official Journal on 20 November 2024. Its aim is to strengthen the cybersecurity and cyber resilience of connected software products (and hardware that includes digital elements). In light of these developments, Europe is reiterating the growing importance of cybersecurity for the continent's economy. The extensive digitisation of businesses and public services has heightened the risk of cyber attacks, underscoring the need for robust measures to protect against such threats.

The Regulation, which has a far-reaching scope[5], focuses on three key areas:

#1	Guaranteeing **the safety** of products **"in principle"** when they are placed on the market and throughout their life cycle;
#2	Ensure the delivery of products while **limiting** potential **security breaches**;
#3	**Improving the level of information available** to users and businesses.

This text is supplementary to the 2016 *Network and Information Security (NIS)*[6] and 2022 (NIS2)[7] directives, which require essential and large entities to adopt significant security measures. It is also based on the 2019 Cybersecurity Act[8], which represents a significant step forward in the construction

---

1   See "A Europe fit for the digital age", https://commission.europa.eu/.
2   The concept of regulation, as formalised in economic law, is a process that guides and supervises the behaviour of economic players (including companies) in order to achieve general interest objectives, while adapting to market developments. In this way, regulation is not merely about setting standards; it also includes monitoring, encouraging and penalising mechanisms to ensure that markets function properly and consumers are protected.
3   Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products incorporating digital elements and amending Regulation (EU) 2019/1020.
4   Declaration on Digital Rights and Principles: EU values and citizens at the heart of the digital transition, Council of the European Union, Press release, 15 December 2022 09:30, https://www.consilium.europa.eu/ which is also found in Article 1 of the IA Act of 13 June 2024.
5   For further details on this topic, please refer to Regulation (EU) 2022/2554, also known as the DORA (Digital Operational Resilience Act). This regulation is dedicated to the digital operational resilience of entities in the financial sector.
6   Directive (EU) 2016/1148
7   Directive (EU) 2022/2555
8   Regulation (EU) 2019/881

of a unified European cybersecurity strategy. This strategy strengthens ENISA's role as a permanent agency designed to support all Member States and introduces a cybersecurity certification framework.

The Cyber Resilience Act is designed to enhance the security of digital products as a whole, and **applies to all products made available on the European market as part of a commercial activity.** While the initial versions did not take into account the specific features inherent in Open Source projects, which are by their very nature open to commercialisation issues, the text evolved after numerous players in the sector highlighted the challenges of applying the CRA in the decentralised context of Open Source. Consequently, a number of adaptations have been incorporated, including several forms of exception or limitation for the benefit of non-commercial, not-for-profit projects published under a free or Open Source licence[9]. Following the publication of the Regulation in the Official Journal, the phase of support has commenced. This will involve the production of best practice guides and the standardisation of procedures, with the ultimate goal of ensuring a uniform and flexible application of the law[10].

2.2 | Challenges facing digital and Open Source players

The Regulation was formally adopted on 10 October 2024 and published in the Official Journal of the European Union, with an effective date of 10 December 2024. The economic players concerned (businesses, but potentially also public or not-for-profit players with an economic activity) are then required to comply with certain critical obligations (notification of actively exploited vulnerabilities and serious incidents) within a transition period of 21 months (until 10 September 2026) and to adapt to all the other requirements of the text within a further transition period of 36 months (until 10 December 2027). These requirements include, for example, the implementation of security as a matter of principle[11] and transparency vis-à-vis consumers. **This is a crucial juncture for the French and European digital ecosystem, which must anticipate and adopt new practices to ensure compliance in a timely manner.** In addition to the entities directly regulated by the regulator, all the concepts introduced by the Regulation will gradually have to be incorporated into contracts with commercial partners[12], suppliers, subcontractors, end customers, and even consumers.

As participants in a broader production and supply chain, all those involved in the utilisation, development or integration of Open Source software **may be directly or indirectly affected by the Regulation**. Furthermore, all Open Source stakeholders, whether economic or not, have a clear interest

---

9   Article 2 of the Regulation defines free and Open Source software as software 1) the source code of which is openly shared and 2) 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;
    Any public software distributed under a Free *Software Definition* or Open Source *Definition* licence therefore falls within this definition.

10 This co-construction project was anticipated by Open Source players, who have coordinated their efforts within the *Open Regulatory Compliance Working Group* (https://orcwg.org/) under the aegis of the Eclipse Foundation, and will be directly involved as members of the European Commission's *CRA Expert Group on Cybersecurity of Products with Digital Elements*.

11 Or "by design", in the sense that design naturally incorporates these concepts. See 3.3.1 Implementing a high level of cybersecurity for products.

12 It will be a requirement for companies supplying software products to provide precise documentation detailing their level of security, the technical support offered by the supplier and the installation of security updates. Furthermore, they will be required to share and correct any vulnerabilities identified in the Open Source projects used, maintain an up-to-date inventory of the Open Source components employed, and so forth.

in proactively preparing for the entry into force of a Regulation that is likely to open up significant opportunities for them. This is an **opportunity for proactive engagement with a regulator that has identified cybersecurity as a priority for the coming years** and is planning a series of measures to support free and Open Source software, as well as micro, small and medium-sized enterprises. Furthermore, it presents an opportunity for all regulated players **to make more regular and sustained contributions**, which will foster new collaborative relationships and practices.

However, there is still a need to **clarify the relationship between these Regulations and the specific practices of the Open Source industry**. While some situations can be fully assimilated to the practices of commercial solution manufacturers, the Open Source model opens up a **wide range of implications** that can have a significant impact on competition law, public procurement practices and so on. This is particularly due to the **decentralised nature of the model and the fact that intellectual property rights are free to use**. Firstly, the product is not necessarily, directly or indirectly, sold to third parties[13] (or may be sold by someone other than the publisher). Secondly, there is no automatic overlap between the party producing the code and the party (or parties) controlling its use. Furthermore, Open Source practices facilitate the adaptation and modification of published products, which can sometimes result in a blurring of the boundaries between manufacturers, publishers and distributors/integrators.

2.3 | Aims of raising awareness of the CRA

This guide to implementing the CRA has been developed to provide support to CNLL members and, more widely, French digital businesses that develop or incorporate free and Open Source software into their products and/or services. It provides a summary of the impact of the CRA and a practical interpretation of the main expectations of the European legislator. The objective is to **equip industry stakeholders with the knowledge and tools to identify and implement suitable Open Source management processes within their organisations**, in line with the specific and complementary cybersecurity expectations set out in the Regulation. This includes, for instance, the compilation of Software Bill of Materials and vulnerability management.

Given the length of the Regulation, this guide does not aim to be exhaustive. Instead, it provides an overview of the Regulation in a few dozen pages. It is intended to be shared widely within the professional Open Source ecosystem, in particular to facilitate dialogue with the European legislator. Please note that this document may be updated at a later date to include specific details for certain categories of Open Source users and contributors, such as large-scale users and public authorities[14].

---

13 Not every activity is necessarily "commercial" for the purposes of the CRA, even if it is provided by an economic player (see in particular recitals 15, 16, 18 and 20).

14 It should also be noted that Article 5 of the CRA encourages public authorities to extend compliance with its provisions to their public procurement contracts, following the example of US practices such as the Executive Order on Improving the Nation's Cybersecurity, Briefing Room, Presidential Actions, 12/05/2021, https://www.whitehouse.gov.

3 | Explanation of the obligations and expectations of the Regulation

To facilitate comprehension of the CRA and its anticipated outcomes, this section initially delineates its primary stipulations, subsequently evaluating the prerequisites and procedures for its implementation in Open Source contexts.

3.1 | Scope of the CRA

3.1.1 Regulation of products with digital components

The CRA applies to "*products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.*".

In order for the CRA to apply, three cumulative conditions must be met :

1. "**products with digital elements**" : such as a software solution or hardware that incorporates software. Article 2 of the CRA applies to software that has been "*designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions*"[15]. It also applies to all software or hardware components that are placed on the market separately and which interact with the aforementioned software.

2. "**made available on the market**": the product is intended for distribution or use on the EU market as part of a commercial activity[16], whether in return for payment or free of charge.

3. "**the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network**" : this includes both products explicitly designed or marketed for such use (e.g. a Wi-Fi router) and those for which connection to a network is a logical consequence of the product's operation (e.g. a smartphone can be used to access IoT services). This encompasses connections to other devices (whether software or hardware) or to a network (which is, by definition, connected to other devices), and may be via cables or software.

---

15 Article 3 Definition defines remote data processing as: " *data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions*". It should be noted that Article 26 of the Regulation states that the Commission will provide guidance on the concept of remote data processing and free and Open Source software.

16 Commercial activity being understood as the supply of goods in the context of an economic activity, see article 2.2 "Making available on the market" of the Blue Guide https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en

This wording is intentionally comprehensive to encompass the majority of products likely to introduce cybersecurity risks. However, it excludes non-obvious scenarios where a product has been significantly altered from its anticipated applications.

> **Please note that the CRA :**
> - differentiates between standard digital products and **important and critical products** (see Annexes I, III and IV) subject to more stringent requirements (not yet defined) and conformity assessment processes that will have to be carried out by a third party.
> - specifically excluded from the scope of this Regulation:
>   - Those for which other European texts specify the applicable regimes (see Article 2 Scope).
>   - Those for which **special regulations** ensure a level of protection identical to or higher than that provided for by the CRA.

3.1.2 Application of the CRA to Open Source software

| *Exclusion from application of the CRA in the absence of commercial activity*

In contrast to the definitions of Open Source (https://opensource.org/osd) and free software (https://www.gnu.org/), which neither exclude nor discriminate against commercial exploitation, the CRA makes a clear distinction between Open Source software used in support of a commercial activity and Open Source software published without being connected to a commercial activity.

The CRA's approach is to apply the cybersecurity requirements of the Regulation **only to products distributed in a commercial context**. A product is deemed to be engaged in commercial activity when it is **monetised by its original manufacturer**. However, it is possible to contribute to Open Source software without being in a commercial context[17]. In European law, the qualification of an activity as commercial is based on the concept of **economic activity**, as defined by the Court of Justice of the European Union (CJEU) as "*any activity consisting in offering goods or services on a given market*". It would seem that certain activities of economic actors (irrespective of their legal status and method of financing) may be considered non-commercial, particularly if it can be demonstrated that:

1. **distribution is free of charge and not for profit**[18] (i.e. with no direct financial consideration and no intention of profit);

---

17 It should be noted that these elements are reiterated in Recital 18 of the CRA: " *In relation to economic operators that fall within the scope of this Regulation, 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. […] Furthermore, the supply of products with digital elements qualifying as free and Open Source software components intended for integration by other manufacturers into their own products with digital elements should be considered to be making available on the market only if the component is monetised by its original manufacturer. For instance, the mere fact that an Open Source software product with digital elements receives financial support from manufacturers or that manufacturers contribute to the development of such a product should not in itself determine that the activity is of commercial nature*". "*This Regulation does not apply to natural or legal persons who contribute with source code to products with digital elements qualifying as free and Open Source software that are not under their responsibility*".

18 See in particular Recital 18: "*Finally, for the purposes of this Regulation, the development of products with digital elements qualifying as free and Open Source software by not-for-profit organisations should not be considered to be a commercial activity provided that the organisation is set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives*".

2. **funding is provided by donations or grants** (for Open Source projects supported by voluntary contributions or public grants with no revenue from the sale of products or services);

3. **the absence of associated paid services** (associated services such as technical support, training, hosting or customisation).

In conclusion, it would appear that certain practices of Open Source players fall outside the scope of the new CRA requirements, given the absence of commercial activity. This particularly applies to Open Source software distributed for testing purposes, for exclusive reseCRAh purposes, and so on, provided that there is no monetisation likely to be associated with making the software available. In this case, the initial release of the software in Europe will not be considered a placing on the market under the CRA.

It is recommended that the application of the CRA be assessed on a product-by-product and activity-by-activity basis. This will enable us to determine which products are "made available on the market" and which are not. The timeframe and the roles involved may vary.

/ *Application of the CRA to commercially-used products*

In accordance with the principle that "free" does not necessarily imply "free of charge", numerous activities associated with Open Source software are conducted on a commercial basis. A variety of business models are associated with the development of software under Open Source licenses. Each situation must be assessed against the CRA's criteria. Nevertheless, some initial applications appear to emerge organically.

- **Direct commercial activity:**

  ○ Under the **dual licence business model** (the code is subject to two licences, one being Open Source – generally relatively restrictive: GPL-3.0 or AGPL-3), The most widely used today is 0, followed by the other, which is commercial.

  ○ in the **case of subscriptions or additional guarantees** designed to facilitate the use of Open Source solutions;

  ○ when **centralisation is operated in parallel by the publisher** via a SaaS and/or marketplace service (sale of plug-ins, etc.);

  ○ and, finally, as part of **complementary services operated independently of the distribution of the software**.

- **Indirect commercial activity**, i.e. activity carried out by the re-users of the community-developed solution: this is the case for Open Source software, which is developed on a community basis to meet the needs of players (private or public) who can either distribute it as part of their commercial activity (in which case they will be subject to the CRA) or simply use it to support their activity.

Table 1Examples of commercial activities involving application of the CRA, from those most specific to Open Source (left) to those closest to traditional business models (right).

Products or services using the software	Software services	Software as a service (Saas) offers	Subscription	Alternative proprietary licences
Their economic activity requires that the software exists and is properly maintained: *OpenStack, Linux kernel, etc.*	Contributors to the software sell services based on it, using their expertise (support or training): *PostGreSQL, QGIS, etc.*	The company that develops the software alternatively offers a SaaS service based on its own software: *Wordpress, Dolibarr, etc.*	A subscription gives you access to easy updates and support: *RHEL, Jboss, etc.*	Publishers alternatively sell proprietary licences (dual licensing or freemium offer): *Alfresco, MySQL, etc.*

If multiple versions of the same Open Source software are made available under different conditions (some of which may be associated with a commercial activity while others are not), it may be possible to apply the same logic currently used to determine whether an economic player is liable for certain responsibilities or legal guarantees. This could involve distributing the software by version, type of provision (commercial activity or not) and associated users. This approach ensures that **users of a specific software version are covered by the CRA's guarantees as long as that version is subject to commercial activity.**

3.2 | Players involved in the CRA

3.2.1 Economic operators concerned by the CRA

The Regulation applies **to all economic players, regardless of their legal status or method of financing.**

In line with established principles of regulating the internal market, the Regulation differentiates between various economic operators, each with distinct responsibilities. These include **the manufacturer, the authorised representative, the importer and the distributor.** It should be noted that certain roles not defined by the CRA (notably that of the manufacturer's suppliers and subcontractors) will not be **directly regulated, but will be subject to indirect regulation through the contractual relationship linking them to the manufacturer or importer. Public authorities** (in the European sense of the term, i.e. all public players) will also play an active role in strengthening this framework, since Article 5(2) of the CRA stipulates that "*where products with digital elements that fall within the scope of this Regulation are procured, Member States shall ensure that compliance with the essential cybersecurity requirements set out in Annex I to this Regulation, including the manufacturers' ability to handle vulnerabilities effectively, are taken into consideration in the procurement process*".

Secondly, the specific role of "*Open Source software steward*" has been introduced to provide a preferential framework for industrial Open Source communities, which are considered essential for the sustainable development of free and open products intended for commercial use. A strict application of the CRA would have unintended consequences that are contrary to the EU's objectives

and the current structure of the ecosystem. Therefore, they benefit from "lighter" regulatory obligations that allow them to be involved in the regulation of the CRA while taking account of their specific nature. This allows stewards of Open Source software to continue supporting the development of Open Source software for their members' commercial activities, **provided they provide the necessary information and security to ensure full CRA compliance. The steward does not affix the CE mark to products supported in this way,** acting upstream of the market launch.

All of these operators are subject to a number of additional obligations. It is therefore the responsibility of operators to ascertain whether they fall into one of the following categories and to ensure that they comply with the underlying obligations. **In accordance with the definitions of each economic operator, a single entity may not assume multiple roles for a single product. However, a single entity may assume different roles for multiple products.**

3.2.2 Application of the CRA to Open Source players

The Open Source development model is particularly horizontal, which means that the traditional Open Source players (publishers, integrators, trainers, hardware manufacturers, major users, contributors, etc.) can assume one of the roles defined above, depending on the situation.

In particular, this will depend on the degree of control exercised over the digital product and the type of monetisation involved.

| *Manufacturer qualification*

The role of manufacturer is widely defined and can encompass a variety of scenarios encountered in Open Source.

The manufacturer is a:

- 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;

By identifying the manufacturer through its brand name, the Regulation aims to impose its most significant obligations on the economic actors who oversee the design, production and marketing of products. Consequently, only **those economic operators who have legal control over the product development process**[19] will be considered manufacturers. This indicates that those **who contribute to the development of free and Open Source software for which they are not responsible**[20] are not subject to the CRA (in either their capacity as manufacturer or distributor). This distinction will certainly be central in its application to research centres, for which it will certainly be necessary to

---

19 It should be noted that the CRA does not specifically address situations of technical or material control, whereas it is possible to provide exclusivity and control over the development of the software solely through control of the platform hosting the code (whether this involves limiting access, contributions or changes to the project).

20 See in particular Recital 18: "*This Regulation does not apply to natural or legal persons who contribute with source code to products with digital elements qualifying as free and Open Source software that are not under their responsibility*".

distinguish between software that is subject to economic development (internally or through maturation by SATTs, for example), which will a priori be fully subject to the constraints of the CRA, and software that is essentially distributed in open source as part of the organisation's missions, which will a priori be excluded from this framework.

The lack of direct financial transactions between the manufacturer and the users of the software subject to the CRA will undoubtedly present challenges in ensuring compliance with certain information obligations. Nevertheless, such a situation will be evaluated in line with the specific Open Source context. It is reasonable to assume that information via traditional information and communication channels would be deemed sufficient (project website, mailing list for developers and/or the user community, etc.).

/ Distributor qualification

Given their role in the dissemination of Open Source software, including commercial software, software forges (such as GitHub and GitLab) appear, at first glance, to fall outside the scope of the CRA. This is because they do not intend to make their products available on the EU market in an economic sense.

Conversely, marketplaces involved in the distribution of software would appear to meet the criteria for classification as **distributors**[21].

/ Open Source software steward qualification

Open source software stewards are:

- **legal entities**;

- **other than manufacturers**;

- whose mission is to provide **systematic and ongoing support** for the development of open source software;

- **that are used in commercial activities** by other organisations.

In contrast to the manufacturer, who promotes the product under their own name or brand, the open-source software steward's responsibility is to provide support for the development and viability of open-source products. As the roles of open-software steward and manufacturer are mutually exclusive for the same product, only the role of manufacturer will apply if the criteria for this designation are met.

A review of the Regulation and its recitals reveals that the concept seems sufficiently broad to encompass the main foundations, including the Eclipse Foundation, the Linux Foundation, the Apache Foundation, OSGeo and OW2. However, a case-by-case analysis will be essential to understand the specific role and influence (economic and political) of the companies involved. It seems likely that the

---

21 To this end, see in particular Recital 20: "*The sole act of hosting products with digital elements on open repositories, including through package managers or on collaboration platforms, does not in itself constitute the making available on the market of a product with digital elements. Providers of such services should be considered to be distributors only if they make such software availableon the market and hence supply it for distribution or use on the Union market in the course of a commercial activity*".

application of the CRA will encourage the porting of Open Source projects by such foundations. There is a risk, as has already been demonstrated, that certain economic operators will seek to abdicate their responsibilities while retaining significant control over software design. It should be noted, however, that this would then result in them reverting to the role of manufacturer or distributor, depending on whether or not they market the product under their own name or brand – it is therefore highly likely that foundations, such as the Mozilla foundation dedicated to Firefox software, which employ their own developers will be considered as manufacturers under the CRA.

Finally, this qualification does not extend to the informal governance of Open Source communities, which frequently operate through decentralised porting by their members. Similarly, the role of "fiscal hosts" (such as the Open Collective project) will undoubtedly require reevaluation in light of the individual responsibilities that the CRA is likely to entail.

Summary of qualifications in an Open Source context with regard to commercial activities

The following table illustrates the various economic activities presented above, showcasing the diverse range of stakeholders (including manufacturers, distributors, Open Source software stewards, and more) who may be engaged under the CRA.

Table 2Proposed qualification of economic operators under the CRA.

Products or services using the software	Software services	Software as a service (Saas) offers	Subscription	Proprietary licences
Their economic activity requires that the software exists and is properly maintained: OpenStack, Linux kernel, etc.	Contributors to the software sell services based on it, using their expertise (support or training): PostGreSQL, QGIS, etc.	The company that develops the software alternatively offers a SaaS service based on its own software: Wordpress, Dolibarr, etc.	A subscription gives you access to easy updates and support: RHEL, Jboss, etc.	Publishers alternatively sell proprietary licences (dual licensing or freemium offer): Alfresco, MySQL, etc.
Open Source software steward	Manufacturer	Manufacturer	Manufacturer	Manufacturer
Manufacturer (if marketing under their name)	Importer (if first marketed in the EU)			
Importer (if first marketed in the EU)	Distributor (if third party)			
Distributor (if third party)				

In an Open Source context, it is possible to have a greater degree of shared responsibility than in closed models.

- **In the context of Open Source software, where there is no single manufacturer**, responsibility for compliance and marketing under a brand or name is not explicitly taken on by any party. This is particularly the case when the software is produced by a developer or a

community of developers, or even a not-for-profit organisation, without any commercial intention or specific brand.

- **Additionally, a variety of distributors may be considered manufacturers** (even in the context of free distribution) when they adapt the software to the extent that it is deemed substantial under the CRA.

3.3 | Obligations under the CRA

The CRA imposes a wide range of obligations on all economic operators, who in turn impose similar commitments on their subcontractors (in particular, designers) and partners. In order to ensure transparency and compliance, these obligations may also be reinforced through contractual agreements, particularly in the context of public procurement contracts, given the obligation on public authorities to be proactive in applying the principles of the CRA.

3.3.1 Implementing a high level of cybersecurity for products

The CRA requires the **design, development and production of the product to be carried out in a manner that ensures a sufficient level of cybersecurity.**

The initial step is to exercise **due diligence** when integrating components obtained from third parties. While the Regulation does not define this due diligence obligation, it appears to encompass a non-exhaustive set of actions aimed at mitigating potential safety risks. This may entail considering the number of maintainers of the component in use, conducting tests, monitoring the availability of regular updates, and so forth. To the greatest extent possible, it will rely on the due diligence work carried out by the manufacturers of these components. In this context, the manufacturer may still place a product on the market without all third-party components having a certificate of conformity, provided that they verify the requirements of each integrated component. The objective of the attestation programme established by the CRA is to streamline the marketing process[22].

Secondly, the manufacturer is required to conduct or have conducted (depending on the classification of the product)[23] a **conformity assessment** of the product, which must be considered throughout its life cycle. This encompasses the planning, design, development, production, delivery and maintenance phases of the product[24]. To perform this assessment, Annex 1 of the Regulation outlines a series of critical cybersecurity requirements related to the product's attributes: absence of known vulnerabilities, default security configuration, robust control mechanisms, data confidentiality and integrity protection, and user-friendly data deletion capabilities[25].

Main contacts:

- Manufacturer;

---

22 See 3.4.2Support associated with the CRA
23 As mentioned in paragraph 3.1.1Regulation of products with digital components
24 Article 13(2)
25 6.1.1Cybersecurity requirements relating to the properties of products with digital elements

- Open Source software stewards in the case of Open Source software intended for commercial activities.

Subsequent managers :

- Distributor;

- **Importer.**

3.3.2 Declaration of conformity and CE marking

In order to affix a CE marking, a declaration of conformity must be provided, which states that the product complies with the cybersecurity requirements set out by the CRA[26]. It is drafted in accordance with the model set out in Annex[27]. This model is available in all the languages of the Member States and contains the elements specified in the evaluation procedures. It must be updated throughout the life cycle of the product. In the event of non-compliance, the manufacturer is legally bound by this certificate and is required to retain it for a period of 10 years.

The manufacturer is then required to affix the CE marking to the product in a clearly visible, legible and indelible manner. In the case of software products, the CRA stipulates that the CE marking must be affixed either with the EU declaration of conformity or on the accompanying website[28].

It is the responsibility of distributors and importers to ensure that products meet the requirements of the CRA before being placed on the market (importers) and that other operators have fulfilled their obligations (distributors).

Main contact:

- Manufacturer;

Subsequent managers :

- Authorised representative;

- Distributor;

- Importer (if manufacturer outside the EU).

3.3.3 Technical documentation

The CRA therefore places a significant obligation on the manufacturer to provide the relevant technical documentation for the product in question. As set out in Annex VII of the Regulation, the technical documentation must include a number of elements, as follows:

1. **General description of the product:** intended purpose of the product, software versions relevant to cybersecurity, photos or diagrams showing external and internal features, and instructions for users.

---

26 Article 28(4)
27 6.3 | Model declarations of conformity
28 See appendix 6.2 | CE marking for details of the procedures laid down by the legislator.

2. **Description of the design, development and production:** details of the design and development, including schematics or a description of the architecture, information on the vulnerability management process (list of software used, vulnerability disclosure policy, contact for reporting vulnerabilities, methods for secure distribution of updates), and details of the manufacturing and monitoring processes.

3. **Cybersecurity risk assessment:** document attesting to the proper implementation of a high level of cybersecurity for published products (cybersecurity risk analysis integrated into the design and development of the product, application of the essential cybersecurity requirements).

4. **Information on the support period**: criteria used to determine the duration of product support.

5. **List of the standards and certifications applied,** including any harmonised standards, common specifications and European cybersecurity certifications used, as well as any solutions adopted in the event that certain standards or certifications are not applied in full.

6. **Compliance test reports:** results of any compliance tests with cybersecurity requirements.

7. **EU declaration of conformity**

8. **Software Bill of Materials** (voluntarily or at the regulator's request[29]): detailed list of software components.

Main contact:

- Manufacturer;

Subsequent managers :

- Authorised representative;

- Distributor;

- Importer (if manufacturer outside the EU).

3.3.4 Nomenclature des logiciels (SBOM)

The new European Regulation introduces a significant requirement for the production and regular updating of a Software Bill of Materials[30] [31]. This is designed to enhance transparency, security and resilience in the digital products sector. In accordance with the CRA, manufacturers of digital products are obliged to:

---

29 "*The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements [...]: where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for that authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I*". Annex VII, Content of technical documentation.

30 Article 3 Definitions: " *a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;*"

31 An SBOM is a detailed inventory of the software components, libraries and dependencies that make up a digital product or embedded system. The term SBOM is used in the original version of the CRA.

- **Identify and document vulnerabilities and product components**, in particular by drawing up a nomenclature of software in a commonly used machine-readable format (dual document) covering at least the higher-level dependencies of products[32];

- **Provide this SBOM at the request of the supervisory authorities[33]** for 10 years after the product has been placed on the market. The SBOM is primarily intended for use by manufacturers and the relevant authorities for the purposes of internal safety management. It will be made available to users either as a contractual obligation or at the manufacturer's discretion.

- **Provide the user with information on where they can access the information** when the manufacturer decides to make it available.

This approach will lead to greater software transparency, better management of Open Source components and dependencies, assistance in complying with legal and regulatory obligations, identification of security flaws and possible replacement components, long-term maintenance, and more.

Fortunately, the Open Source and cybersecurity ecosystems have been working together for several years to streamline the generation of SBOMs. This tool is at the nexus of three key areas: cybersecurity, sustainability and compliance. It enables users to check Open Source components and their dependencies, identify who is involved in developing the software they are using and ensure that the product is being used in accordance with the relevant licences. By making the provision of an SBOM compulsory, the CRA **aims to enhance the resilience of the digital ecosystem and disseminate best practice within the Open Source ecosystem.**

This will provide businesses with enhanced visibility of their software supply chains, enabling them to swiftly identify and address obsolete or vulnerable components before they become a threat. End customers, whether business or consumer, will gain a deeper insight into the components that make up the products they purchase. This will enable them to assess the risks and implement suitable security strategies for their own infrastructure. In order to achieve this, SBOMs must:

- it into potentially complex supply chains by standardising formats;

- be as precise and exhaustive as possible in order to cover the widest range of risks. In contrast to existing practices, which aim for relatively fine granularity, the obligation to provide SBOMs established by the CRA currently only covers **first-level dependencies**[34].

There are currently **two main standards** for building SBOMs: SPDX and CycloneDX are the two main standards for building SBOMs. The two standards are based on the PURL specification (URL package) for the designation of third-party components[35].

---

32 Annex 1 Part II. Article 13 §24 of the CRA provides that the Commission may be required to specify the format and elements constituting SBOMs.
33 Article 13 §24
34 Annex 1 Part II: "*Manufacturers of products incorporating digital elements shall: 1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products*".
35 This specification is being developed by NexB, and its community governance is currently being formalised. See
     https://github.com/package-url/purl-spec

SPDX® https://spdx.dev	CycloneDX https://cyclonedx.org/
The first version of SPDX (for System Package Data Exchange) was developed by the legal compliance community under the aegis of the Linux Foundation in 2011. The creation of this standard resulted in the development of a list of identifiers for Open Source licenses, which is now universally used, including in the CycloneDX standard.	A more recent specification has been developed by the security industry under the aegis of the OWASP Foundation (Open Worldwide Application Security Project).
The second iteration of the standard, version 2.2.1, was published as ISO/IEC 5962:2021. The latest version, 3.0.1, introduces the concept of profiles to address specific domains, including security.	It has been refined to more accurately reflect certain licensing considerations and has been standardised at the ECMA for version 1.6.

A priori, compliance with either of these two standards will make it possible to meet the expectations of the CRA. However, a degree of acculturation will be required to ensure that the SBOMs generated are actually usable: in terms of the quality of the information manipulated (SBOM generation or curation is still insufficiently automated) and the relevance of the information shared in this way (it is necessary to limit the SBOM to only those components that are actually distributed in a specific context).

Main contact:

- Manufacturer.

3.3.5 Vulnerability management and notification obligations

All manufacturers and other economic operators are part of a complete system that is designed to monitor, identify and manage vulnerabilities. By combining their respective obligations, the European legislator is ensuring that:

- Reporting any identified vulnerabilities to the relevant authorities and users;

- Product withdrawal or rapid patching (particularly security patches for critical vulnerabilities);

- Pre-market surveillance (by manufacturers and importers) or post-market surveillance (by distributors)

- Possible control by regulators, including access to complete technical documentation for a given period.

In this regard, the manufacturer is required to provide a minimum five-year support period following the last placement of the product on the market, contingent on the specific version of the product in question. During this period, the manufacturer is required to document and update the product's cybersecurity risk assessment on a regular basis and to ensure that the product's vulnerabilities, including those of its components, are managed effectively and in accordance with the requirements of the CRA. These are set out in Part 2 of Annex 1 to the Regulation, which includes documentation via an SBOM, security tests and reviews, security updates, rapid sharing of patches, and so on[36]. To

---

36 6.1.2 Requirements for vulnerability management

reduce the number of supported versions of the software and the associated risk coverage, the manufacturer may encourage users to regularly update the versions of the solution currently on the market and clearly indicate which products are no longer being marketed.

Main contact:

- Manufacturer;

Subsequent managers :

- Distributor;

- Importer (if non-EU manufacturer);

- Open Source software stewards in the case of Open Source software intended for commercial activities.

3.3.6 Summary

Role	Bonds
Manufacturer A 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;	1. It is the responsibility of the manufacturer to **ensure that the conformity procedures established by the CRA are applied, or have been applied, to the products they are marketing.** This entails obtaining a **declaration of conformity and affixing the CE mark.** 2. Furthermore, the manufacturer is required to **prepare and retain comprehensive documentation, including a SBOM.** 3. In **the event of an incident or vulnerability being identified** in one of its products, the manufacturer is obliged to **report it to the relevant authorities, to those responsible for maintenance and to the users concerned** (if possible via the user interface[37]). Furthermore, the manufacturer **is required to implement all necessary measures to address the identified vulnerability and distribute the corresponding patches** for a minimum of five years[38] following the product's market release.
Open Source software 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;	1. It is the responsibility of the Open Source software steward to **implement and document a transparent and verifiable cybersecurity policy.** The objective of this policy is to ensure the security of digital products and to address vulnerabilities in a prompt and effective manner, in accordance with reports from developers. Furthermore, it encourages the voluntary reporting of vulnerabilities, taking into account the specific nature of Open Source software and the legal and organisational particularities associated with it. This policy includes measures for documenting, correcting and sharing vulnerabilities within the Open Source software community. 2. It is the responsibility of the Open Source software software steward to **cooperate with the relevant supervisory authorities in order to reduce the cybersecurity risks** associated with digital products that utilise Open Source software. Upon request from the relevant authorities, he is required to provide documentation pertaining to the cybersecurity policy in a clear and concise manner, in either paper or electronic format. 3. In addition, Open Source software stewards are subject to the **same obligations as manufacturers when participating in the development of digital products.** Furthermore, they are obliged to comply with reporting requirements in the event of serious incidents affecting the security of the products or the information systems they provide for their development.
Authorised representative	The authorised representative is responsible for carrying out the tasks assigned to them by the manufacturer. Upon request from the supervisory authorities, he provides them with a

---

37 See in particular Recital 56: "*Where a product with digital elements has a user interface or similar technical means allowing direct interaction with its users, the manufacturer should make use of such features to inform users that their product with digital elements has reached the end of the support period".*

38 The support period is defined as "*the period during which a manufacturer is required to ensure that vulnerabilities of a product with digital elements are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I;",* i.e. all the requirements relating to vulnerability management.

		copy of his mandate. This mandate entails at least the following responsibilities:
	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;[39]	1. R**etain the declaration of conformity and technical documentation** for a minimum of ten years following product market release or for the duration of the product's warranty, whichever is longer. 2. Upon request, provide the authorities with all information and **documentation necessary to demonstrate product compliance.** 3. **Cooperate with the authorities** on any action to eliminate product-related risks.
	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;	1. It is the responsibility of the importer to ensure that the manufacturer has fulfilled all legal obligations and that any digital components included in the product comply with the relevant cybersecurity requirements. Prior to marketing the product, the importer must verify that the manufacturer has completed the necessary conformity procedures, that the technical documentation is available, that the product bears the CE marking, and that it is accompanied by the declaration of conformity and instructions, which must be written in a clear language. 2. In the event that the importer has reason to believe that a product or the manufacturer's processes do not comply with the aforementioned requirements, it is their responsibility to refrain from placing the product on the market until the necessary rectifications have been made. In the event of a cybersecurity risk, the importer is required to immediately inform the manufacturer and the relevant authorities. Furthermore, the contact details of the importer (name, address, e-mail) must be readily available on the product or packaging or in an accompanying document. This enables users and the authorities to contact the importer if necessary. 3. In the event that a product already on the market is found to be non-compliant, the importer is required to implement corrective measures in a timely manner, which may include withdrawing or recalling the product. In the event of a vulnerability being identified, the manufacturer must be informed without delay. Furthermore, if the risk is significant[40], the relevant authorities must also be alerted. 4. It is the responsibility of the manufacturer to retain a copy of the declaration of conformity and technical documents for a minimum of ten years (or for the duration of the product's warranty period), in order to provide them to the relevant authorities upon request. 5. Ultimately, in the event that the importer becomes aware that the manufacturer has ceased trading and is no longer able to fulfil its obligations, it is required to immediately notify the relevant supervisory authorities and, where feasible, the end users of products already in circulation.
	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;	1. It is the responsibility of distributors to ensure that any product containing digital components placed on the market complies with the relevant cybersecurity requirements. Prior to marketing the product, distributors **must verify that the CE mark has been affixed and that the manufacturer and importer have fulfilled their obligations**, furnishing the requisite documentation[41]. In the event that a distributor has reason to believe that a product or its manufacturing processes do not comply with the relevant requirements, **it is prohibited from selling the product until the identified issues have been rectified**. In the event of a serious risk, the distributor must immediately inform the manufacturer and the relevant authorities. 2. In the event that a product already on the market is found to be non-compliant, the distributor is responsible for **ensuring that appropriate corrective measures are taken**, including the withdrawal or recall of the product in question. In the event of a vulnerability being identified, the manufacturer must be informed without delay. Should the risk be deemed significant, the supervisory authorities must also be alerted. Furthermore, upon request, the distributor must be able to provide documentation proving product compliance and cooperate in resolving cybersecurity risks. 3. Ultimately, in the event that the distributor becomes aware that the manufacturer has ceased trading and is no longer able to fulfil its obligations, **it is required to**

---

39 Article 3.2 of the Blue Guide states that "*Thus, the manufacturer may neither delegate the measures necessary to ensure that the manufacturing process assures compliance of the products nor the drawing up of technical documentation, unless otherwise provided for. Further, an authorised representative cannot modify the product on his own initiative in order to bring it into line with the applicable Union harmonisation legislation.*". https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en

40 Article 7§2 b) :" *the product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.*".

41 The Regulations do not specify the format of these documents, except that they may be "*in paper or electronic form*".

	immediately notify the relevant authorities and, where feasible, the end users affected.

3.4 | Regulation, sanctions and support

3.4.1 The regulatory authorities

The CRA establishes a coordinated approach by designating several regulatory authorities to implement and enforce the Regulation.

It is also recommended that each Member State establish a single national entry point for all safety notifications.

Table 3Definition of the various regulatory authorities and their respective missions.

Authorities	Installation	Missions
Market surveillance authorities	Each Member State is responsible for designating the authority, either by selecting an existing authority or by establishing a new authority.	1. Guarantee that digital products comply with the established cybersecurity standards. They guarantee that products placed on the market comply with security requirements to protect consumers and infrastructure. 2. Inform consumers so that they are aware of how to report any issues. 3. Collaborate with one another, with CSIRTs and with other national and European agencies in order to guarantee a unified approach. 4. Share statistics and data on surveillance and enforcement activities
ENISA European Union Agency for Cybersecurity	Already in place.	1. Set up and manage a single platform for reporting cybersecurity vulnerabilities and incidents in order to simplify and centralise the notification process for manufacturers. 2. Adheres to the highest standards of security and confidentiality. The platform will be integrated with the European vulnerability database[42]. 3. Prepares a biannual report identifying emerging trends in cybersecurity for digital products.
ADCO Administrative Cooperation Group	To be created. The committee will be comprised of representatives from the supervisory authorities.	1. Addresses specific issues related to market surveillance activities in relation to obligations imposed on stewards of Open Source software. 2. Provides a centralised repository of information on software components used in digital products, enabling the monitoring of critical cybersecurity dependencies. 3. Publishes statistics on average support periods and offers indicative support times for each product category, identifying those that require increased monitoring.
CSIRT Security incident response centres	Already in place.	1. Handles the dissemination of vulnerability notifications. 2. Ensures effective coordination and communication between supervisory authorities and ENISA. 3. May delay the dissemination of a notification in exceptional situations where the security of certain Member States is at stake.

3.4.2 Support associated with the CRA

The CRA offers support to these authorities, which is of benefit to:

- **micro-enterprises[43], small[44] enterprises and medium-sized[45] enterprises :** This includes a helpdesk for queries regarding reporting obligations set out in Article 14 (Article 17), as well as the publication of guidelines to assist with the application of the Regulation (Article 26).

- **Open Source projects and players.** This includes voluntary safety certification programmes for free and Open Source software (Article 25), the inclusion of free and Open Source software in the Commission's future guidelines (Article 26) and special relations with free and Open Source software stewards.

---

42 Database provided for in Directive (EU) 2022/2555.
43 Fewer than 10 employees and with an annual turnover or annual balance sheet total not exceeding €2 million. See Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized
44 With fewer than 50 employees and an annual turnover or balance sheet total not exceeding €10 million.
45 With fewer than 250 employees and an annual turnover not exceeding €50 million or an annual balance sheet total not exceeding €43 million.

In addition to the requirement for economic players to contribute to Open Source upstream projects, these programmes aim to address the specific characteristics of free and Open Source software. They will be accessible to any person or entity developing or using this type of software, including third-party manufacturers who integrate products, end users and public administrations in the European Union.

To ensure a beneficial convergence between the dynamics of cybersecurity and Open Source, Open Source projects must work with regulators to ensure that contributions to projects are sustainable over time. If Open Source projects are unable to respond to requests or contributions, or if they are unduly influenced by manufacturers' needs, the Open Source model may not be viable.

3.4.3 Penalties for non-compliance with the CRA

It is the responsibility of each Member State to determine the penalties applicable to breaches of the CRA and to implement them. It is essential that these penalties are **effective, proportionate and dissuasive.** Such penalties are **imposed on a case-by-case basis**. In order to achieve this, the CRA sets out certain criteria that must be taken into account when deciding on the amount of administrative fines.

The following factors will be taken into account when determining the appropriate penalty:

- **the nature, seriousness and duration** of the offence and its consequences;
- **any administrative fines previously imposed on the same economic operator** for a similar infringement;
- **the size and market share** of the economic operator committing the infringement.

To assist Member States in this regard, the CRA sets out different ceilings depending on the type of breach of obligations and the parties involved.

Table 4: Typology of sanctions provided for under the CRA for non-compliant economic operators.

Economic operators concerned	Bonds concerned	Amount of penalty
➔ The manufacturers	All the manufacturer's obligations	Up to €15,000,000 or 2.5% of worldwide annual turnover for companies
➔ The manufacturers ; ➔ Authorised representatives ; ➔ Importers ; ➔ Distributors.	Declarations of conformity, CE marking, technical documentation, conformity assessment procedures, and action following notification.	Up to €10,000,000 or 2% of worldwide annual turnover for companies
➔ The manufacturers ; ➔ Authorised representatives ; ➔ Importers ; ➔ Distributors.	Failing to provide accurate, complete, and truthful information to notified bodies and market surveillance authorities in response to a request.	Up to €5,000,000 or 1% of worldwide annual turnover for companies

It should be noted that the CRA does provide for a number of derogations [46] regarding the application of these penalties.

---

46 Article 64(10). See Recital 120: "*Given that administrative fines do not apply to microenterprises or small enterprises for a failure to meet the 24-hour deadline for the early warning notification of actively exploited vulnerabilities or severe incidents having an impact on the security of the product with digital elements, nor to Open Source software stewards for any infringement of this Regulation, and subject to the principle that penalties should be effective, proportionate and dissuasive, Member States should not impose other kinds of penalties with pecuniary character on those entities*".

- Manufacturers that are considered to be **micro** or **small enterprises**[47] in the case of:

    ○ non-compliance with the deadline for early warning of an actively exploited vulnerability no later than 24 hours after becoming aware of it (Article 14(2)(a)), or

    ○ early warning of a serious incident affecting product safety no later than 24 hours after becoming aware of it (Article 14(4)(a)).

- Any breach of the rules by **stewards of Open Source software.**

It is also worth noting that the sanctions outlined in the CRA are significant, yet the text allows for some flexibility at the Member State level, following the precedent set by the General Data Protection Regulation (GDPR)[48]. Similarly, each Member State establishes the criteria for determining whether, and to what extent, administrative fines may be imposed on public authorities and public bodies established within its territory.

---

47 Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422).

48 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/...
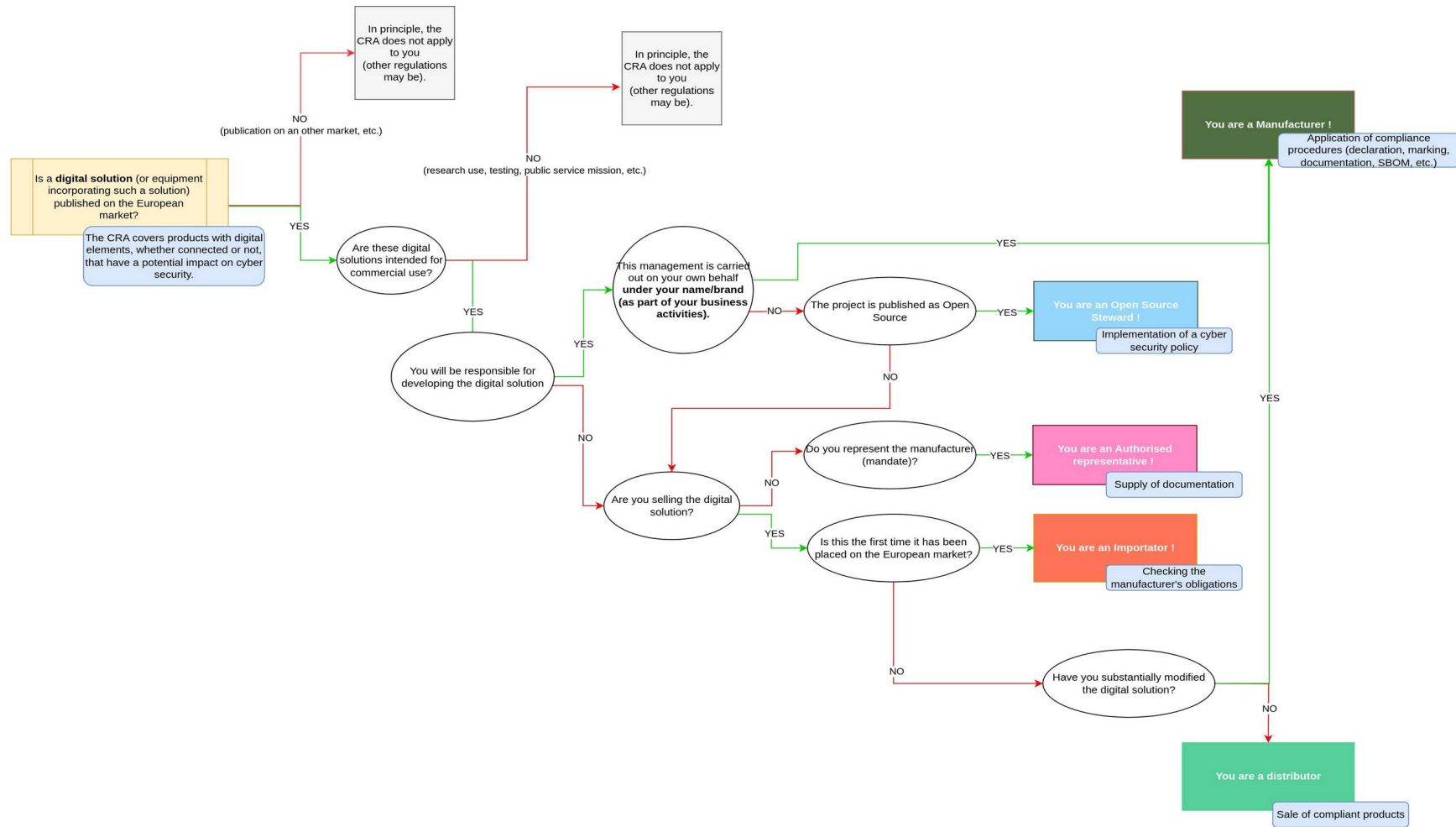
4.1 | Qualification of economic operators

Figure 1: Flow chart for the qualification of economic operators under the CRA

4.2 | Roles and responsibilities of economic operators

Stages in the product launch process	Before placing on the market	Placing on the market	After placing on the market

Coordinator

ENISA
- Set up a single notification platform and ensure its functioning
- Produces a report on cyber security trends every 24 months
- It proposes joint control activities to be carried out by the surveillance authorities

CSIRT
- Provides a support service for SMEs
- Treat the notifications of vulnerability

Market Surveillance Authority
- Facilitate cooperation between organisations and consumers
- Inform the consumers to facilitate the reporting
- Communicates the results of market surveillance activities to the Commission
- Can carry out joint activities to ensure the cybersecurity of consumers
- Can carry out sweep operations

Administrative Cooperation Group (ADCO)
- Processes the monitoring activities of open source stewards
- Controls the definition of the manufacturers' support period
- Publishes statistics on products and support periods

Open Source Actors

OSS Communities

OSS Steward
- Implements a cyber security policy to facilitate the reporting and handling of vulnerabilities

Economic operators

Manufacturers
- Applies or enforces compliance procedures
- Draws up the documentation, declaration of conformity and stamps the CE mark
- Veille à ce que les produits soient accompagnés des instructions nécessaires et que celles-ci soient accessibles et faciles d'utilisation et les tenir à destination des autorités (pendant 10 ans)
- S'informe des changements de normes, certifications, spécifications techniques
- Designs, develops and manufactures products to guarantee a sufficient level of cyber security
- Set the support period and include the information used to set it in the documentation, as well as the exact end date
- Indicates its contact details to users and designates a single point of contact
- Ensures that products can be identified
- Identifies and documents components and vulnerabilities using a specific nomenclature
- Manage vulnerabilities
- Distributes the product with no known vulnerabilities and with a default security configuration
- Obligation to update documentation and declaration of conformity (for 10 years)

Authorised representative (of the manufacturer)

Importers (puts on the EU market)
- Checks CE marking, technical documentation and assessment procedure
- Only puts compliant products on the market
- Indicates contact details
- Provides the authorities with a copy of the declaration of conformity
- Is able to provide documentation

Consumer

Distributors (provides the customer with)
- Doing the necessary due diligence
- Ensures that the manufacturer and importer have provided it with all documents

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

Consumer

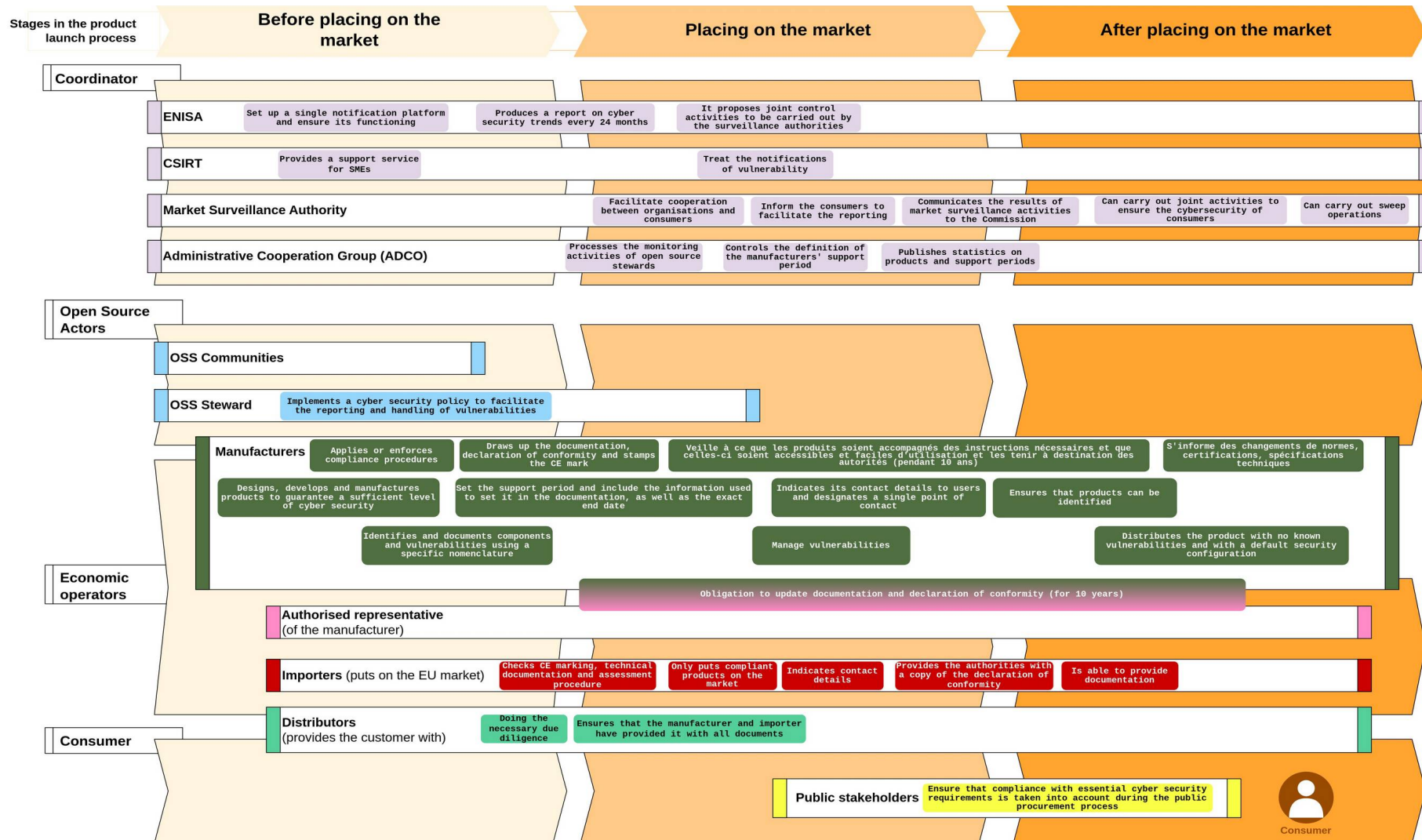*Figure 2: Representation of the different roles and responsibilities of operators, upstream and downstream of the marketing of a digital solution.*
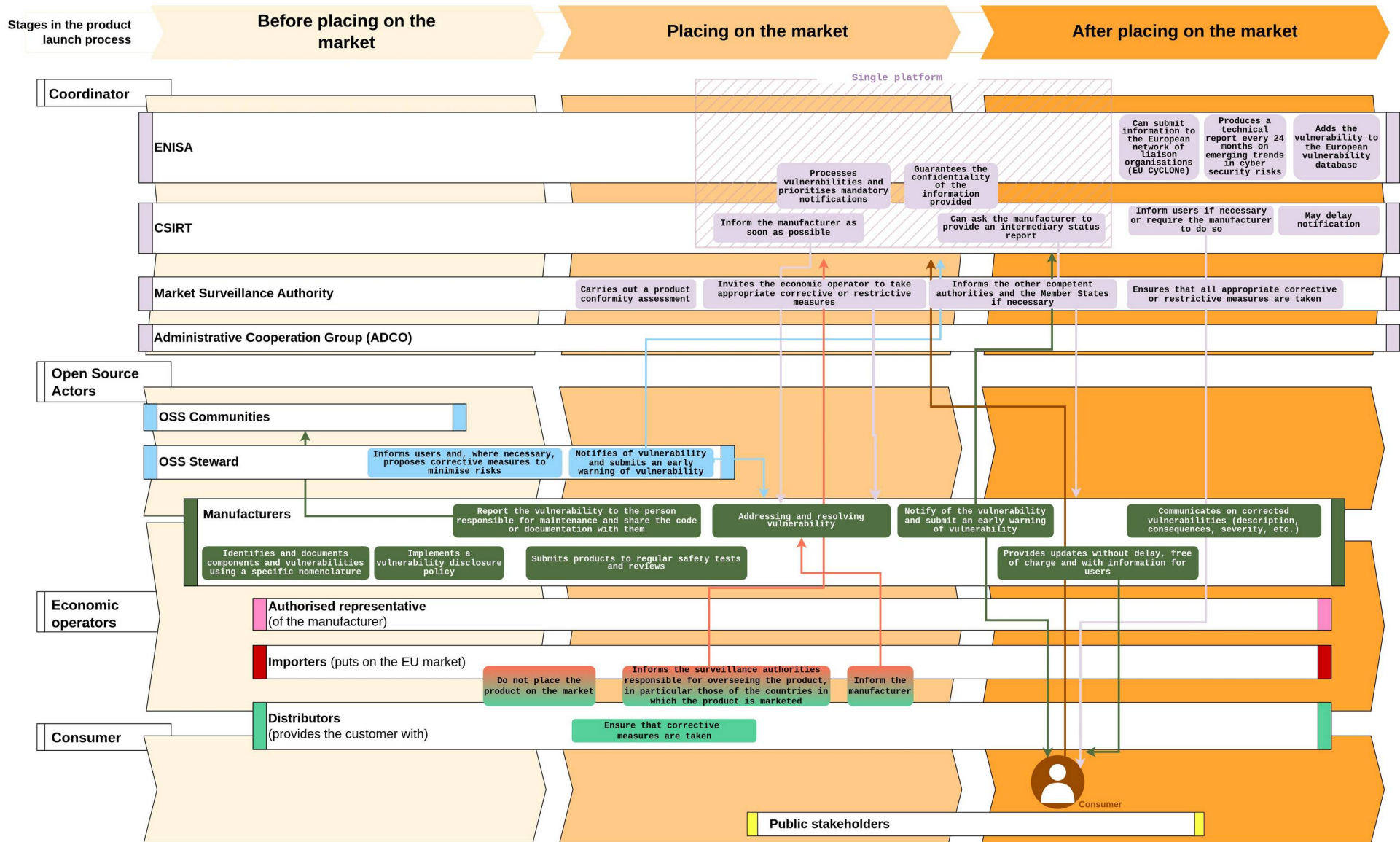
4.3 | Vulnerability management

Stages in the product launch process	Before placing on the market	Placing on the market	After placing on the market

Coordinator

ENISA
- Processes vulnerabilities and prioritises mandatory notifications
- Guarantees the confidentiality of the information provided
- Can submit information to the European network of liaison organisations (EU CyCLONe)
- Produces a technical report every 24 months on emerging trends in cyber security risks
- Adds the vulnerability to the European vulnerability database

CSIRT
- Inform the manufacturer as soon as possible
- Can ask the manufacturer to provide an intermediary status report
- Inform users if necessary or require the manufacturer to do so
- May delay notification

Market Surveillance Authority
- Carries out a product conformity assessment
- Invites the economic operator to take appropriate corrective or restrictive measures
- Informs the other competent authorities and the Member States if necessary
- Ensures that all appropriate corrective or restrictive measures are taken

Administrative Cooperation Group (ADCO)

Open Source Actors

OSS Communities

OSS Steward
- Informs users and, where necessary, proposes corrective measures to minimise risks
- Notifies of vulnerability and submits an early warning of vulnerability

Manufacturers
- Report the vulnerability to the person responsible for maintenance and share the code or documentation with them
- Addressing and resolving vulnerability
- Notify of the vulnerability and submit an early warning of vulnerability
- Communicates on corrected vulnerabilities (description, consequences, severity, etc.)
- Identifies and documents components and vulnerabilities using a specific nomenclature
- Implements a vulnerability disclosure policy
- Submits products to regular safety tests and reviews
- Provides updates without delay, free of charge and with information for users

Economic operators

Authorised representative (of the manufacturer)

Importers (puts on the EU market)
- Do not place the product on the market
- Informs the surveillance authorities responsible for overseeing the product, in particular those of the countries in which the product is marketed
- Inform the manufacturer

Consumer

Distributors (provides the customer with)
- Ensure that corrective measures are taken

Consumer

Public stakeholders

Figure 3: Representation of the various requests between regulatory authorities and economic operators.

4.4 | Query management

Figure 4: Representation of the various requests between the regulatory authorities and economic operators.

5 | Enforcement of the rules for CNLL members' activities

The following pages are intended to illustrate the application of the CRA to a number of economic activities identified by members of the CNLL. The cases are fictitious and deliberately simplified.

5.1 | Summary of the different scenarios

		Operators appointed to the CRA				
		Manufacturer	Open Source software steward	Authorised representative	Importer	Distributor
Distributor of hardware integrating Open Source components	Persona #4.2	(X)				X
Publisher of an Open Source solution	Persona #4.3	X				
Contributor to an Open Source Foundation project marketed in Europe	Persona #4.4				X	
Open Source solutions **integrator** (with modification)	Persona #4.5	X				
Company operating **SaaS services based** on an in-house digital solution.	Persona #4.6	(X)				
Company using **modified Open Source software**	Persona #4.7	(X)				
Independant developer & IT consultant	Persona #4.8					

Table 5: Summary of economic operator qualifications under the CRA.

Caption:

Signs	Meaning
X	Probable CRA qualification
(X)	Qualification may be required in specific contexts defined by the CRA

If you would like more information on operators, please see 3.2.1 Economic operators concerned by the CRA.

5.2 | Digital solutions distributor

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)

Article 2§1 :
Article 3§1

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.

5.3 | Open Source Publisher

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 3§1: 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.

5.4 | Company contributing to an Open Source project

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

Contribution to software ○ → Simply contributing to software does not trigger the CRA

Marketing digital products on the European market ○ → Company subject to the CRA

Recital 18
Article 2

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.

5.5 | Open Source solutions integrator

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.

5.6 | Company operating a Saas service

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.

5.7 | Companies using Open Source solutions

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.

5.8 | Independant developer

John Doe

IT consultant and developer

Description

As part of my work as an IT consultant, I've developed software that I've published as open source on Github. I don't sell the software, but I do occasionally use it as part of my professional activities. In fact, I use the software as part of the services I provide to my clients.

Answer to CRA

Scope

		Article 2 Article 3
Publication of the software on Github ○	➤ No application of the CRA as such	
If no commercial activity associated with the publication of the software ○	➤ Person not subject to the CRA	
Use of the software as part of services provided for customers, but no marketing of the software as such ○	➤ Person not subject to the CRA	

6 | Annexes

6.1 | Essential cybersecurity requirements

6.1.1 Cybersecurity requirements relating to the properties of products with digital elements

1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

(j) be designed, developed and produced to limit attack surfaces, including external interfaces;

(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Annex I - Essential cybersecurity requirements, Part I - Cybersecurity requirements relating to the properties of products with digital elements

6.1.2 Requirements for vulnerability management

Manufacturers of products with digital components:

1) identify and document vulnerabilities and product components, including the establishment of a software nomenclature in a commonly used machine-readable format covering at least the higher-level dependencies of products;

2) manage and correct vulnerabilities in products with digital elements without delay, including through security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

3) regularly subject products with digital components to effective security tests and reviews;

4. immediately upon publication of a security update, communicate on the vulnerabilities fixed, in particular by publishing a description of the vulnerabilities, information enabling users to identify the product incorporating digital elements concerned, the consequences of these vulnerabilities, their seriousness and clear and accessible information helping users to remedy them; in duly justified cases, where manufacturers consider that the security risks associated with publication outweigh the security benefits, they may delay publication of information on a patched vulnerability until users have had the opportunity to apply the appropriate patch;

5) set up and apply a coordinated vulnerability disclosure policy;

6) take steps to facilitate the sharing of information about potential vulnerabilities in their products incorporating digital elements and in third-party components contained in such products, including by providing a contact address for reporting vulnerabilities discovered in the products concerned;

7. provide mechanisms for the secure distribution of updates for products with digital components to ensure that vulnerabilities are corrected or mitigated rapidly and, where appropriate, automate security updates;(8) ensure that, where security patches or updates are available to remedy identified security problems, they are distributed without delay and, unless otherwise agreed between a manufacturer and a professional user in the case of a custom product incorporating digital components, free of charge and accompanied by advisory messages providing users with relevant information, including any action to be taken.

Annex I - Essential cybersecurity Requirements, Part II - Vulnerability handling requirements

6.2 | CE marking

6.2.1 Definition

CE marking: "*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 with the essential cybersecurity requirements set out in Annex I and other applicable Union harmonisation legislation providing for its affixing;*".

<div align="right">Article 3 - Definitions</div>

6.2.2 Installation

1. The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to the packaging and to the EU declaration of conformity referred to in Article 28 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 28 or on the website accompanying the software product. In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.

2. On account of the nature of the product with digital elements, the height of the CE marking affixed to the product with digital elements may be lower than 5 mm, provided that it remains visible and legible.

3. The CE marking shall be affixed before the product with digital elements is placed on the market. It may be followed by a pictogram or any other mark indicating a special cybersecurity risk or use set out in the implementing acts referred to in paragraph 6.

4. The CE marking shall be followed by the identification number of the notified body, where that body is involved in the conformity assessment procedure based on full quality assurance (based on module H) referred to in Article 32. The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the manufacturer or the manufacturer's authorised representative.

5. Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE marking and shall take appropriate action in the event of improper use of that marking. Where the product with digital

elements is subject to Union harmonisation legislation, other than this Regulation, which also provides for the affixing of the CE marking, the CE marking shall indicate that the product also fulfils the requirements set out in such other Union harmonisation legislation.

6. The Commission may, by means of implementing acts, lay down technical specifications for labels, pictograms or any other marks related to the security of the products with digital elements, their support periods and mechanisms to promote their use and to increase public awareness about the security of products with digital elements. When preparing the draft implementing acts, the Commission shall consult relevant stakeholders, and, if it has already been established pursuant to Article 52(15),

ADCO. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).."

Article 30 - Rules and conditions for affixing the CE marking

6.3 | Model declarations of conformity

6.3.1 Declaration of conformity (ANNEX V)

The EU declaration of conformity referred to in Article 28, shall contain all of the following information:

1. Name and type and any additional information enabling the unique identification of the product with digital elements

2. Name and address of the manufacturer or its authorised representative

3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider

4. Object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate)

5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation

6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared

7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued

8. Additional information:

Signed for and on behalf of:

(place and date of issue):

(name, function) (signature):

6.3.2 Simplified declaration of conformity (ANNEX VI)

The simplified EU declaration of conformity referred to in Article 13(20) shall be provided as follows:

Hereby, … [name of manufacturer] declares that the product with digital elements type … [designation of type of product

with digital element] is in compliance with Regulation (EU) 2024/2847 (1).

The full text of the EU declaration of conformity is available at the following internet address: …

6.4 | Useful links

- Cyber Resilience Act link: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

- Blue Guide link: https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en

- To monitor the status: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act

- Contact: https://www.europarl.europa.eu/portal/en/contact