Open
Regulatory
Compliance

Open Source Software Stewards and CRA Whitepaper

V1.0 - January 2026

Table of Contents

Abstract

This whitepaper addresses the new legal category of Open Source Software Stewards ("Stewards") introduced by the European Union's Cyber Resilience Act (CRA). It serves as an analysis and elaboration of the specific obligations, restrictions, and penalties that will be imposed on Stewards, who are defined as legal persons (e.g., foundations, companies) distinct from the Open Source Projects they support and separate from commercial Manufacturers. The paper clarifies that this role imposes a lighter regulatory burden on Open Source actors who do not monetise their software, though many projects currently lack a Steward.

The core of a Steward's responsibility centers on implementing a verifiable Cybersecurity Policy in cooperation with their projects. This policy must aim to; foster the development of secure products; ensure the effective handling of vulnerabilities, including documentation, addressing, and remediation; promote information sharing within the open source community; and, describe the project’s vulnerability reporting and handling processes, including voluntary reporting to a national CSIRT.

Additionally, Stewards have obligations related to mandatory reporting and regulatory cooperation:

- Mandatory Reporting: Stewards must report actively exploited vulnerabilities only if they are involved in the development of the product. They must also report severe incidents affecting the IT infrastructure they provide to the projects (e.g., version control systems, build systems). All mandatory reporting is done via the single reporting platform.
- User Notification: When an exploited vulnerability or severe incident occurs, Stewards must inform affected users and provide necessary mitigation or corrective measures, preferably in a machine-readable format.
- Market Surveillance Cooperation: Stewards are required to cooperate with Market Surveillance Authorities (MSAs) to mitigate security risks and provide the required security documentation.

Crucially, the CRA explicitly excludes Stewards from the administrative fines/penalties that apply to Manufacturers for non-compliance, reflecting the reduced risks and lighter burden intended for this non-monetising role. This document is not legal guidance but a reflection of the contributors' current understanding of the CRA requirements, outlining practical steps and resources needed by Stewards and their Projects to fulfill these new legal obligations.

Introduction

Open Source Software Stewards are defined in the Cyber Resilience Act (CRA) as a distinct category of legal persons, separate from Manufacturers. A Steward must be a registered legal entity, such as a for-profit or non-profit organisation or a foundation, and is legally distinct from the Open Source Project itself.

The CRA introduces this category to reflect the specific role played by organisations that support the development and sustainability of open source software without placing products with digital elements on the market for commercial purposes. As a result, Open Source Stewards are subject to a tailored and lighter regulatory regime compared to Manufacturers, reflecting their different responsibilities and risk profile.

This document focuses on the obligations, expectations, and practical implications of the CRA as they apply to Open Source Stewards, with the objective of supporting a consistent and pragmatic understanding of their role within the regulatory framework.

Obligations of Open Source Stewards

Under the CRA, Stewards have specific obligations with respect to the Open Source projects for which they act as Stewards.

Establishing a formal relationship between a given Open Source Project and its Steward is something the two parties may need to define themselves. For example, a Steward organisation may already be performing a supporting role for the project due to ownership of intellectual property, historical reasons, an explicit agreement entered into by the project leadership with a Steward organisation, or because the project was originally founded as such.

Security Policy

Stewards shall, with the cooperation of their Projects, develop, document, and implement a cybersecurity policy that these Projects adopt. The goals of this policy are to:

- encourage the development of secure 'products with digital elements[1];
- ensure the effective handling of vulnerabilities by developers of those products, including the documentation, addressing, and remediation of vulnerabilities, as well as the sharing of information on discovered vulnerabilities within the Open Source community;
- describe the Project’s vulnerability reporting and handling processes, including policies for voluntary reporting to, and coordination with, a national CSIRT (see below).

The Steward may maintain the policy in paper or electronic form, but it must be "verifiable". As the relationships between Stewards and their Projects vary, the Policy should take into account their shared modes of operation.

Market Surveillance Authorities may request access to this Security Policy.

[1] The legal text states: Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. There are different possible interpretations: the "fostering" described in the Policy applies to the FOSS project, to the integration of the FOSS project into Products by Manufacturers, or to both. We trace the resolution of this question in a dedicated FAQ entry

References: Article 24(1)

> *Cyber Resilience Act, Article 24(1):*
>
> *Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. That policy shall also foster the voluntary reporting of vulnerabilities as laid down in Article 15 by the developers of that product and take into account the specific nature of the open-source software steward and the legal and organisational arrangements to which it is subject. That policy shall, in particular, include aspects related to documenting, addressing and remediating vulnerabilities and promote the sharing of information concerning discovered vulnerabilities within the open-source community.*

In Open Source Projects, Security Policies are typically public (thereby fulfilling the publication requirement) and are published on the Project site and/or included in the source code repository.

In practice, multiple patterns exist with respect to security policies, for example:

- The supporting organisation (the Steward) creates and publishes a policy; Projects agree to that policy and link to it in their documentation. A Project may make minor clarifications, such as adding a project-specific link or email address for reporting vulnerabilities.
- The supporting organisation provides a template, and Projects publish their own policies based on that template. In this case, the number of changes to the Policy template may be more significant.
- The Project has a long-established public policy, which is adapted by the Steward to serve as its policy in CRA terms.
- The Project already has an established policy that meets CRA requirements and therefore continues to use it; however, this Policy may differ substantially from the Steward's (default) policy.

In all cases, both the Steward and the Project must verify that the Policy they provide includes all required elements and that it is effectively followed. If the Project does not follow the policy, the Steward needs to define an action plan; see the related FAQ entry. For example, accepting a generic Policy from a Foundation acting as Steward may be a prerequisite for creating a Project or for that Project to be admitted to the Foundation.

The Project and the Steward also need to agree on how changes to the Policy are introduced, in order to align legal requirements with the Project's current practices (for example: bug tracking tools, communication methods).

A policy to develop secure products

The legal text says *Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements* without further clarifications. This section will need to be updated once the meaning of this clause is clarified, see a dedicated FAQ entry.

A policy to effectively handle vulnerabilities

The policy for effective vulnerability handling should form part of the overall security policy, in accordance with Article 24(1), and should include processes for:

- documenting vulnerabilities - understood here as documenting fixed or otherwise mitigated vulnerabilities once they become public. Projects may use techniques such CVE/EUVD entries or security advisories (in textual and/or machine-readable formats). All such vulnerabilities should be documented, with the documentation made available in a location that is easy for users to find, e.g., via a link in `SECURITY.md` or on the Project's Security web page.
- addressing vulnerabilities - the policy should define how the Project handles vulnerabilities, including triage and prioritisation. This is a part of the typical security processes of Open Source Projects.
- remediating vulnerabilities - the policy should define how the Project remediates vulnerabilities, whether through fixes or mitigations. This is a part of the typical security processes of Open Source Projects.
- promoting information sharing in the open source community - this is a new, and currently often implicit, requirement. Under the CRA, this aspect of the policy must be explicitly documented. Best practices include sharing information about discovered vulnerabilities with upstream projects; notifying the maintainers of dependencies when a reported vulnerability originates there; and, where there is a likelihood of similar issues in related projects (for example, across different HTTP implementations), informing potentially affected peers.
- enable reporting vulnerabilities to the project (or to the Steward) by Manufacturers that include the Project in their product, in line with Manufacturers' obligations. Each Project must provide a mechanism for reporting vulnerabilities. This is part of the typical security processes of Open Source projects.

Resources

What Stewards and Projects will need:

- The published Policy (which includes more elements than a typical Project security policy today).

- Evidence that the policy is being followed.

What resources could be created to help fulfil these requirements:

- A description of how to demonstrate that the policy is put in place - how to record and store it so that an independent party can verify its existence (for example, version-controlled documents, maintaining a change log, etc.). For instance, the Policy may be stored in Project's `SECURITY.md` file, and versioned in Git.
- A description of how to prove that the Policy is actually being followed, by linking policy statements to concrete evidence. For example, the Policy may state that the security decisions are documented in the `CHANGELOG` file that is versioned next to the `SECURITY.md`.
- A specification and/or template for the Policy, illustrating what it means for a policy to foster the development of secure Products with Digital Elements. For example, this could include a list of methodologies for risk assessment, secure-by-design and secure-by-default principles, a secure SDLC, a process for effective handling of vulnerabilities by the developers of that product, and a description of the coordinated vulnerability disclosure (CVD) process.

Collaboration with Market Surveillance Authorities

When Market Surveillance Authorities request assistance from a Steward in relation to one of its projects, the Steward shall cooperate with the aim of mitigating the security risks posed by the Project for which it acts as Steward.

In particular, the Market Surveillance Authority may request a copy of the Security Policy.

When an Open Source Project makes its Security Policy public (for example, by publishing it on the Project website and/or including in the source code repository), then the publication requirement is fulfilled.

However, the regulation also requires that the policy be provided "in a language which can be easily understood by that authority", which may imply the language(s) of the country in which the Market Surveillance Authority is located. As most Projects and supporting organisations publish their policies in English, it would be beneficial if authorities accepted documents in that language. The language of the country in which the Steward is established may differ from the language spoken or understood by the contributors to the Project.

The Market Surveillance Authority may also request documentation related to the Security Policy, given the requirement to "put in place and document in a verifiable manner a cybersecurity policy". In addition to the Policy itself, this includes any documents demonstrating that the Policy has been applied. Examples include published security advisories (or, more generally, a list of published advisories) and documentation of an ongoing CVD process (for instance, in case of a widely exploited vulnerability for which no fix has yet been published).

If a Market Surveillance Authority finds that a Steward does not comply with its obligations (which likely means not having a Policy and/or not promoting the best practices), it may require the Steward to ensure that all appropriate corrective actions are taken. As a result, Stewards "shall ensure" (wording from the regulation) that appropriate corrective action is taken in respect to their obligations. This implies that the Steward must have a means to influence the Project to follow defined policies. Possible situations include, for example, a Project not responding to vulnerability reports at all, or not documenting fixed vulnerabilities.

In a vulnerability management process, it is common for reporters and developers to disagree on whether a reported issue constitutes a vulnerability. In addition, many Projects face AI-generated reports and low quality reports of minor issues[2]. It is best practice to document in the Policy how such conflicts are resolved and to always respond to reports, even if only to state that the Project does not consider the issue a vulnerability. It may be helpful to specify in the policy that reports which do not relate to an undisclosed vulnerability may be ignored by the Project.

Another best practice is to document the Project's security model and define which components are in scope for vulnerability reporting. For example, a Project may be developing a new, experimental module, that has not yet been released. In this case, it may state that the module is out of scope for vulnerability reporting, while still accepting regular bug reports. Another example is support for a legacy protocol maintained for compatibility reasons and known to have security weaknesses. In this case, the Project may document that it does not accept vulnerability reports for those known weaknesses.

The regulation requires the Steward to take action, but explicitly excludes any fees in the event of non-compliance.

References: Article 24(2), Article 64(10b), Article 52(3)

[2] This is a serious issue for the Open Source community, as each investigation requires developer time. Low quality reports are caused, amongst other factors, by the potential reward (e.g., a CVE number or a bounty - which open source projects typically do not offer). It is therefore reasonable for the Policy to include a process for handling abusive reports. In such cases, Projects and Stewards should keep a minimum of trace of their decison (for example, emails records) and may rely on additional guidelines defining what constitutes a vulnerability, such as the CVE Program rules.

> *Cyber Resilience Act, Article 24(2):*
>
> *Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software.*
>
> *Further to a reasoned request from a market surveillance authority, open-source software stewards shall provide that authority, in a language which can be easily understood by that authority, with the documentation referred to in paragraph 1, in paper or electronic form.*
>
> *Cyber Resilience Act, Article 64(10) "Penalties":*
>
> *By way of derogation from paragraphs 3 to 9, the administrative fines referred to in those paragraphs shall not apply to the following:*
>
> *[...] (b) any infringement of this Regulation by open-source software stewards.*
>
> *Cyber Resilience Act, Article 52 (3) "Market surveillance and control of products with digital elements in the Union market":*
>
> *The market surveillance authorities designated under paragraph 2 of this Article shall also be responsible for carrying out market surveillance activities in relation to the obligations for open-source software stewards laid down in Article 24. Where a market surveillance authority finds that an open-source software steward does not comply with the obligations set out in that Article, it shall require the open-source software steward to ensure that all appropriate corrective actions are taken. Open-source software stewards shall ensure that all appropriate corrective action is taken in respect of their obligations under this Regulation.*

What Stewards and Project will need:

- Know which organisation is their Market Surveillance Authority.

What resources could be created to help fulfil that requirement:

- A guide on how to identify the appropriate Market Surveillance Authority for each Steward.
- Guidance on verifying with the Market Surveillance Authority whether it accepts policies and communications in a language acceptable to both the Project and the Steward.

Mandatory reporting of exploited vulnerabilities and security incidents

Stewards have an obligation to mandatorily report actively exploited vulnerabilities and severe incidents. However, this obligation is more limited in scope than that of Manufacturers.

The table below, taken from the FAQ entry on Steward obligation, summarises Steward obligations depending on the services they provide to the Project:

Steward support level	**Notify vulnerabilities**[3]	**Notify incidents**[4]	**General announcement**[5]	**Message known users**[6]
Provides non-technical support only	N/A	N/A	N/A	N/A
+ provides IT infrastructure	N/A	✅	✅	N/A
+ provides engineering resources (incl. security)	✅	✅	✅	N/A
+ has 1:1 relationship with some users	✅	✅	✅	✅

First, Stewards are expected to report actively exploited vulnerabilities, only if they are involved in the development of the product. This means that if the Steward handles elements other than

[3] Art. 14(1)

[4] Art. 14(3)

[5] Art. 14(8)

[6] Art. 14(8)

development (for example, finances only) and the Project is taking development decisions independently, the Steward is not required to report.

This matches the typical relationship between Stewards and Projects when Stewards are not directly involved in the development, which is frequently the case for foundations. In such situations, the Steward also has no practical means of becoming aware of an exploited vulnerability unless it is informed by the Project.

Information about an actively exploited vulnerability may also come from external sources, such as security researchers. If the Steward is not involved in development, it has no legal obligation to report the vulnerability. However, it should pass the information on to the Project. Whether the Project itself must report is an open question, but doing so would be considered best practice.

Conversely, if the Steward is involved in development and operations (which may often be the case for companies stewarding Projects they do not monetise) its staff are likely to handle vulnerability reports. In that situation, the Steward may receive information about exploitation or detect it directly, and is therefore required to report the exploited vulnerability.

Second, the Steward is obliged to report serious incidents affecting the information systems it provides for the Open Source Projects it hosts. This applies when the Steward organisation manages that infrastructure through its IT team. Examples include intrusions into the IT infrastructure leading to unauthorised modification of the version control system, account takeovers, leakage of signing keys, or prolonged unavailability of the infrastructure that makes development impossible.

Stewards who do not manage the IT infrastructure are not required to report such incidents.

When reporting exploited vulnerabilities or serious incidents, Stewards are required to inform affected users (see below).

The Steward must report, without delay and via the single reporting platform for any actively exploited vulnerabilities or severe incidents.

Stewards may also receive information about exploited vulnerabilities or incidents from a CSIRT, where the CSIRT has obtained such information through voluntary reporting. In that case, the Steward must inform the affected Project.

References: 16, 14(1), 14(3), 14(8), 24(3), 15

> *Cyber Resilience Act, Article 24(3) "Obligations of open-source software stewards":*
>
> *The obligations laid down in Article 14(1) shall apply to open-source software stewards to the extent that they are involved in the development of the products with digital elements. The obligations laid down in Article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products.*
>
> *Cyber Resilience Act, Article 14(1) "Reporting obligations of manufacturers":*
>
> *A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.*

What Stewards and Projects will need:

- Define a process specifying who, within the Steward and/or Project, is responsible for submitting notifications via the single reporting platform, and how to credentials (if needed) are handled. This may be documented in the Steward's Security Policy or in a separate document describing implementation details, as agreed between the Steward and the Project.

What resources could be created to help fulfil this requirement:

- A guide to submitting reports through the common reporting platform.

Informing users about exploited vulnerabilities and security incidents

When a Steward becomes aware of an actively-exploited vulnerability related to one of its Projects, or of a security incident affecting the Steward or the Project's infrastructure, it is required to inform affected users. In the context of Open Source Project, most such notifications will likely be public. They might initially be private and targeted at a specific group of affected individuals, e.g., in case of an IT compromise requiring password resets or verification of recent suspicious activity. Best practice is to publicly disclose the issue once the Steward and the Project have taken immediate mitigation measures.

A typical notification includes information about the vulnerability or incident, as well as any mitigations or measures users can take (for example, disabling a feature or resetting passwords). The regulation recommends providing this information in a machine-readable format. This may take the form of a machine-readable security advisory, such as CSAF. Stewards may also choose to update the relevant CVE entry (and, in the future, the EUVD entry) for an exploited vulnerability. In practice, most Stewards will also publish the information in a human-readable format, such as on a web page or via email.

The legal text suggests that notification does not need to be immediate, allowing time for analysis, verification, and the deployment of fixes. It also indicates that user notification may occur in parallel with reporting through the common reporting platform.

If a Steward does not notify users within a reasonable timeframe, the CSIRT may do so, if it considers this appropriate.

References: 16, 14(1), 14(3), 14(8), 24(3)

> *Cyber Resilience Act, Article 14(8) "Reporting obligations of manufacturers":*
>
> *After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.*

What Stewards and Projects will need:

- Define a method by which a Steward notifies users of exploited vulnerabilities and severe incidents. This may involve a dedicated web page, a mailing list, or a combination of communication channels.

What resources could be created to help fulfil this requirement:

- Best practices for notifying users about exploited vulnerabilities and severe incidents.

Voluntary vulnerability reporting

Stewards may voluntarily report vulnerabilities and incidents to a CSIRT or ENISA, as well as "near misses" (situations in which exploitation or an incident was possible but ultimately avoided). They may also receive reports via a CSIRT and/or ENISA that originate from voluntary reporting.

> *Cyber Resilience Act, Article 24(1) "Obligations of open-source software stewards"*
>
> *Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. That policy shall also foster the voluntary reporting of vulnerabilities as laid down in Article 15 by the developers of that product and take into account the specific nature of the open-source software steward and the legal and organisational arrangements to which it is subject.[..]*
>
> *Article (15)*
>
> 1. *Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA.*
>
> 2. *Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA.*
>
> 3. *The CSIRT designated as coordinator or ENISA shall process the notifications referred to in paragraphs 1 and 2 of this Article in accordance with the procedure laid down in Article 16.*
>
> *The CSIRT designated as coordinator may prioritise the processing of mandatory notifications over voluntary notifications.*
>
> 4. *Where a natural or legal person other than the manufacturer notifies an actively exploited vulnerability or a severe incident having an impact on the security of a product with digital elements in accordance with paragraph 1 or 2, the CSIRT designated as coordinator shall without undue delay inform the manufacturer.*
>
> 5. *The CSIRTs designated as coordinators as well as ENISA shall ensure the confidentiality and appropriate protection of the information provided by a notifying natural or legal person. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon a notifying natural or legal person to which it would not have been subject had it not submitted the notification.*

CSIRT designated as coordinator

The regulation states that Stewards should report to the CSIRT designated as coordinator. However, all reporting is performed via the single reporting platform. Interaction with CSIRTs is two-way: the Steward or Project reports to CSIRT, and the CSIRT may in turn, inform the Steward of potential vulnerabilities and incidents that have been reported to it.

Stewards must identify which CSIRT is designated as their coordinator. The relevant CSIRT is that of the Member State in which (in order of priority):

- the Steward has their main establishment. The main establishment is where decisions related to the cybersecurity of its Products with Digital Elements are predominantly taken;
- the Steward has the establishment with the highest number of employees in the Union;
- the highest number of instances of the Steward's software are located.

If the Steward has no main establishment in the Union, the appropriate CSIRT is that of the Member State in which:

- the authorised representative acting on behalf of the Steward for the highest number of the Steward's products is established;
- the highest number of users of the Steward's products are located.

In practice, it can be assumed that, by default, the Steward or Project reports to the CSIRT of the country in which the Steward has its headquarters.

If the Steward has no official representation in the European Union, reporting may be made to the CSIRTs of a large Member State (such as Germany, France, Spain, or Italy), unless a specific Project has a strong user base in another country. This topic requires clarification, especially for Stewards and Projects without any EU representation and in cases where there may be a language barrier between the CSIRT and the Project. ENISA could also serve as a "CSIRT of last resort" for Stewards without a clear national alignment.

If the Steward or Project cannot determine the appropriate CSIRT using these rules, it is currently assumed that they may choose the CSIRT they consider most appropriate. As the legislation appears to assume a single CSIRT per Steward, multiple Projects under the same Steward will need to share the decision regarding the choice of CSIRT

It is also good practice to explicitly name the designated CSIRT for each Project in its standard security documentation, making it easy to find for anyone wishing to report a vulnerability, as well as for Project contributors.

Open Source usage being global in nature, different CSIRTs will likely receive reports about vulnerabilities for the same Project. Moreover, two parties may interpret conditions differently, and as such report to different CSIRTS for the same Project. It will be necessary to define rules of how those reports will be routed. ENISA may play a coordinator role in this scenario.

Related ORC FAQ entries: on CSIRTs and on choice of CSIRT.

References: 24(3), Directive 2022/2555

> *Directive 2022/2555, Article 12(1) "Coordinated vulnerability disclosure and a European vulnerability database":*
>
> *Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include:*
>
> *(a) identifying and contacting the entities concerned;*
>
> *(b) assisting the natural or legal persons reporting a vulnerability; and*
>
> *(c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.*
>
> *Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.*

What Stewards and Projects will need:

- Documentation identifying the main CSIRT for each Project. This information may, for example, be included in the Project's source code files, such as `SECURITY.md`.

What resources could be created to help fulfil this requirement:

- Clarification of the rules for deciding on the main CSIRT for Stewards based outside the EU, pending guidance.
- Clarification of the rules for deciding on the main CSIRT where there is a language barrier between the Project and the CSIRT, pending guidance.

Market surveillance authorities

Market surveillance authorities might request information from the Steward regarding their policies.

Stewards must know which Market Surveillance Authority is responsible for them. The same rules and open questions apply as for the choice of the designated CSIRT.

What Stewards and Projects will need:

- Documentation identifying the Market Surveillance Authority for the Project and the Steward. This information may, for example, be included in the Project's source code files, such as `SECURITY.md`.

What resources could be created to help fulfil this requirement:

- Clarification of the rules for determining the appropriate Market Surveillance Authority for Stewards based outside the EU.
- Clarification of the rules for determining the appropriate Market Surveillance Authority where there is a language barrier between the Project and the authority.

Restrictions

As Stewards (and Open Source Projects) are subject to less stringent requirements than Products with Digital Elements placed on the market by Manufacturers, Stewards cannot affix the CE marking to the products they publish. This also means that they do not provide the full set of CRA documentation for their Projects.

However, Stewards may operate an attestation program that provides equivalent documentation for use by Manufacturers.

References: the Cyber Resilience Act, recital 19:

> *[..] legal persons who provide support on a sustained basis for the development of such products which are intended for commercial activities, and who play a main role in ensuring the viability of those products (open-source software stewards), should be subject to a light-touch and tailor-made regulatory regime. [..] Given that the light-touch and tailor-made regulatory regime does not subject those acting as open-source software stewards to the same obligations as those acting as manufacturers under this Regulation, they should not be permitted to affix the CE marking to the products with digital elements whose development they support.*

Conclusions

The Cyber Resilience Act (CRA) establishes the "Open Source Software Steward" as a distinct legal category, acknowledging the non-commercial and supportive role of organisations that sustain open source projects. This whitepaper has served to clarify the tailored, lighter regulatory regime applied to Stewards compared to commercial Manufacturers.

The core of a Steward's obligation centres on the collaborative development and implementation of a verifiable Cybersecurity Policy with their Projects, that must address:

- Fostering the development of secure products.
- Ensuring the effective documentation, addressing, and remediation of vulnerabilities.
- Promoting information sharing within the open source community.
- Outlining the process for voluntary vulnerability reporting to a national CSIRT.

Additionally, Stewards have specific responsibilities for mandatory reporting and regulatory cooperation, though their scope is limited:

- Mandatory Reporting: Stewards must report actively exploited vulnerabilities only if they are involved in the development of the product. They must also report severe incidents affecting the IT infrastructure they provide to projects (e.g., build systems, version control). All mandatory reporting is done via the single reporting platform.
- User Notification: Stewards are required to inform affected users of exploited vulnerabilities or severe incidents, providing necessary mitigation measures, ideally in a machine-readable format like CSAF.
- Market Surveillance Cooperation: Stewards must cooperate with Market Surveillance Authorities (MSAs) and provide the Security Policy and evidence of its application upon request. Crucially, they must ensure corrective actions are taken if non-compliant, but they are explicitly excluded from the administrative fines that apply to Manufacturers.

This distinction in penalties is a significant aspect of the CRA, reflecting the reduced risk profile of non-monetising entities. The whitepaper highlights that successfully fulfilling these new obligations requires stewards and their projects to formalise existing security practices, define clear internal processes for reporting and compliance, and develop new resources such as policy templates and guides for verifying policy adherence. While the CRA imposes a necessary framework, its effective adoption depends on a consistent, pragmatic understanding and collaborative implementation within the open source ecosystem.

Scope Clarifications

While this document addresses the obligations of Open Source Stewards under the CRA, it intentionally does not cover certain related topics that are acknowledged as important and complex.

In particular:

- Many Open Source projects, especially smaller or community-led projects, do not currently have an associated steward. The CRA obligations discussed in this document do not apply to such projects.
- This document does not define the criteria for determining whether an organisation qualifies as a Steward for a given Project, nor does it assess whether a specific organisation should be considered a Steward or a Manufacturer.
- Questions related to role qualification, boundary cases, and classification are addressed separately in the ORC Working Group FAQ and may evolve as regulatory interpretation and practice mature.

Glossary

- ENISA - European Union Agency for Cybersecurity
- CRA - Cyber Resilience Act
- CSAF - Common Security Advisory Framework
- CSIRT - Computer Security Incident Response Team
- CVD - Coordinated Vulnerability Disclosure
- EUVD - European Vulnerability Database
- PwDE or PWD - Product with Digital Elements (as defined by the CRA)
- SDLC - Secure Development Life Cycle

References

1. The choice of CSIRT
2. ORC FAQ entries on Open Source Software Stewards
3. FOSDEM 2025 session: CRA Q&A on Open Source Stewards under the Cyber Resilience Act
4. CVE Numbering Authority (CNA) Operational Rules version 4.1.0
5. European Vulnerability Database

Acknowledgments

The following individuals have contributed to this document, either directly or indirectly (for example, by raising questions):

- Mikaël Barbero
- Æva Black
- Arnout Engelen
- Marta Garcia
- Tobie Langel
- Faidon Liambotis
- Jordan Maris
- Salve J. Nilsen
- Juan Rico
- Marta Rybczynska
- Jeremy Stanley
- Mark Thomas
- Daniel Thompson-Yvetot
- Martin von Willebrand

If you have contributed to this document and are not properly acknowledged, or if you want to edit or remove your name, please let us know by opening an issue, and we will address it promptly.