29 January

2026

{code & compliance}

FOSDEM EDITION

Open Source Software Stewards

The Current Understanding, Opportunities, and Challenges

Mikael Barbero

Head of Security — Eclipse Foundation

https://linktr.ee/mbarbero

I Am Not A Lawyer

Do not take business decisions based on this presentation

What changed with the CRA?

New “Steward” Category

Lighter-touch regulation introduced for open-source software stewards.

Differential Regulation

Stewards face reduced burden and risk compared to Manufacturers.

Required Core Processes

Must establish policy, cooperation, and limited reporting mechanisms.

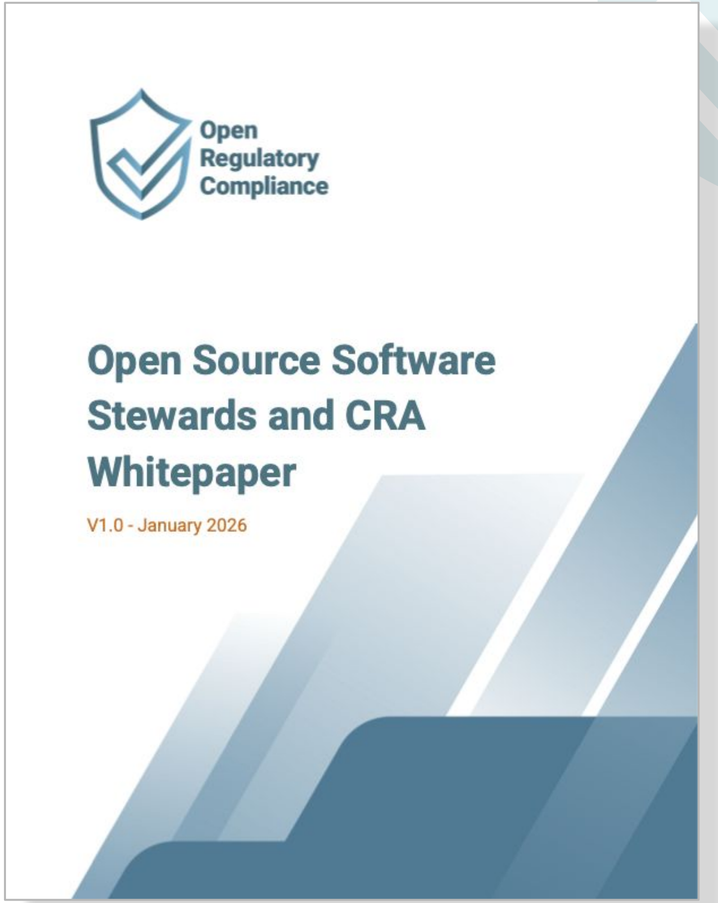
Whitepaper Available Today

Interpretation of the obligations and what they translate to in day-to-day OSS operations

https://orcwg.org

Note

Open Source Software Steward
= the “Steward”, hereafter

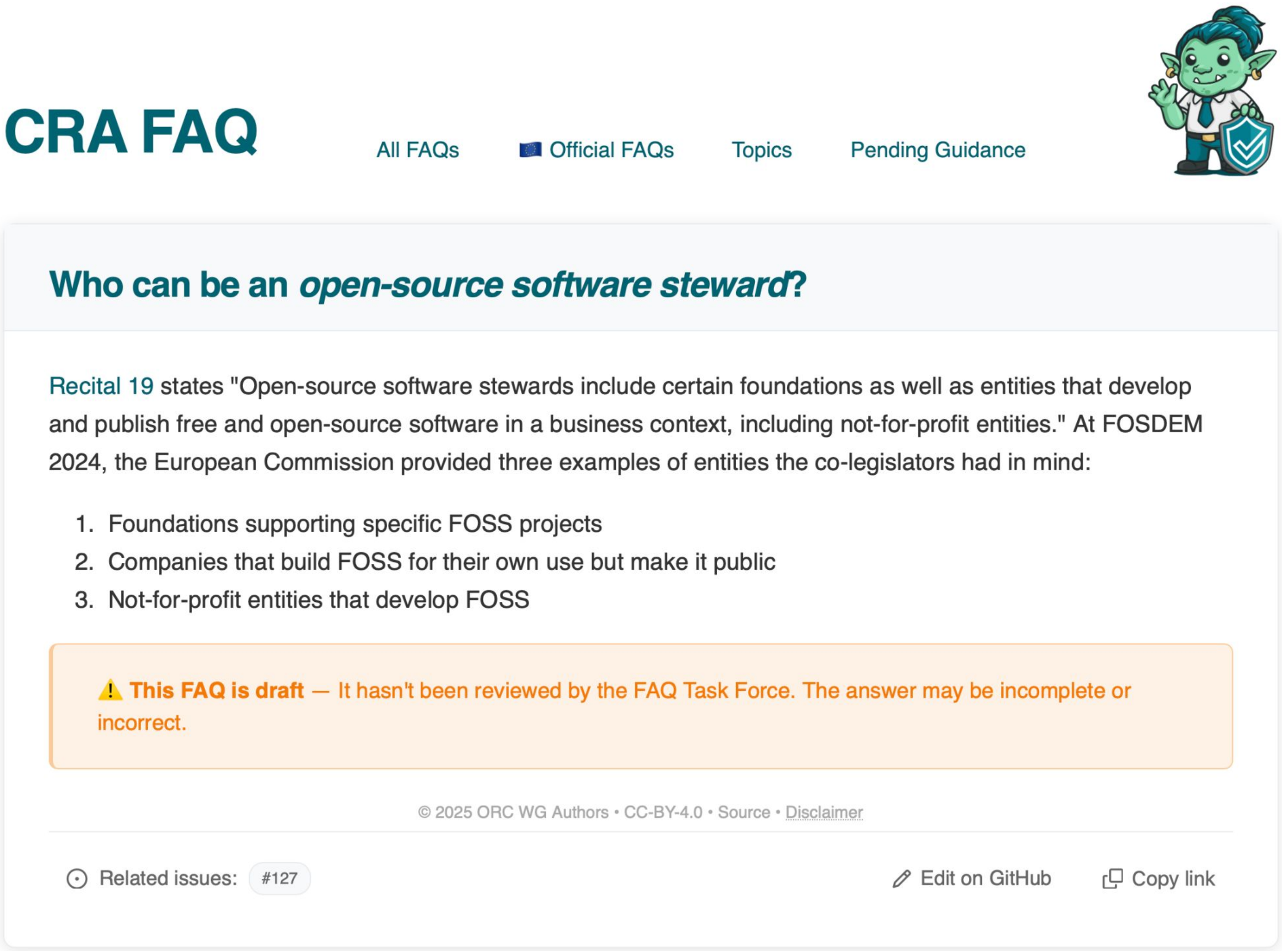


Open Regulatory Compliance

Open Source Software Stewards and CRA Whitepaper

V1.0 - January 2026

The whitepaper does not address who does or does not qualify as a Steward under Recital 19 or the definition set out in Article 3(14)



CRA FAQ

Who can be an *open-source software steward*?

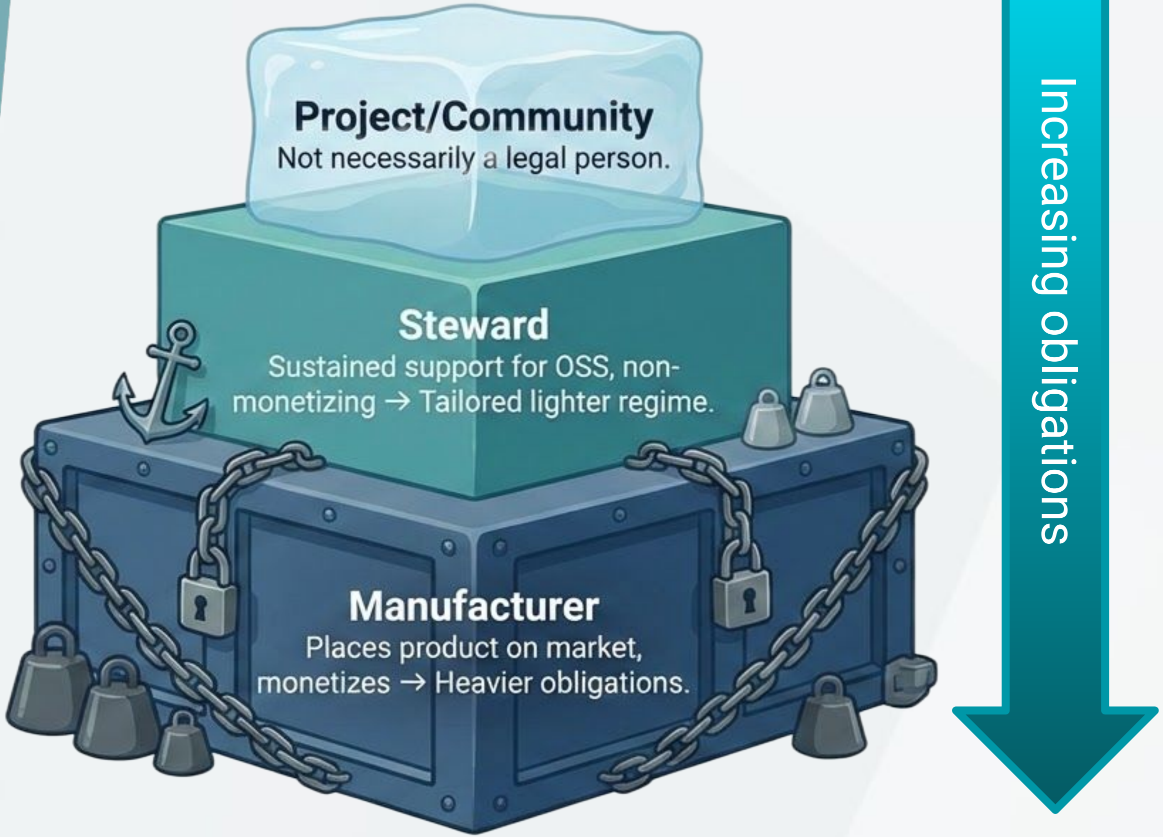
Recital 19 states "Open-source software stewards include certain foundations as well as entities that develop and publish free and open-source software in a business context, including not-for-profit entities." At FOSDEM 2024, the European Commission provided three examples of entities the co-legislators had in mind:

1. Foundations supporting specific FOSS projects
2. Companies that build FOSS for their own use but make it public
3. Not-for-profit entities that develop FOSS

⚠ **This FAQ is draft** — It hasn't been reviewed by the FAQ Task Force. The answer may be incomplete or incorrect.

https://cra.orcwg.org/faq/stewards/who-can-be-steward/

Project *vs* Steward *vs* Manufacturer



Project/Community
Not necessarily a legal person.
Steward
Sustained support for OSS, non-monetizing → Tailored lighter regime.
Manufacturer
Places product on market, monetizes → Heavier obligations.
Increasing obligations

Reality Check

Many projects have no Steward

→ these obligations don’t apply to them

Steward obligations

1. Have a verifiable security policy (and follow it).

2. Cooperate with market surveillance authorities when asked.

3. Report exploited vulnerabilities / severe incidents, but only in certain cases.

4. Inform users when something is actively exploited or there’s a severe incident.

Security policy: what it means

Documented & Verifiable: Write down how the project handles security and vulnerabilities in a verifiable manner (paper/electronic, must be provable).

Comprehensive Coverage: Covers reporting, triage, fixes/mitigations, and public documentation.

Goals:

- Foster development of secure products
- Ensure effective vulnerability handling: document, address, remediate.
- Promote sharing information about discovered vulnerabilities within OSS community.
- Foster voluntary reporting to/coordination with a national CSIRT.

Security policy: what it looks like

- ❑ Reporting intake: how to report vulnerabilities (contact points, expectations).
- ❑ Triage & prioritization: how issues are evaluated.
- ❑ Remediation: fixes/mitigations, timelines, backports.
- ❑ Documentation of fixed/mitigated vulnerabilities: advisories, CVE/EUVD entries.
- ❑ Community information sharing: upstream/downstream notifications, peer projects in similar risk space.
- ❑ Handling abusive/low-quality reports and dispute resolution

Cooperation with authorities: what it means

Policy & Proof

If asked, provide the policy and proof it's applied.

Corrective Actions

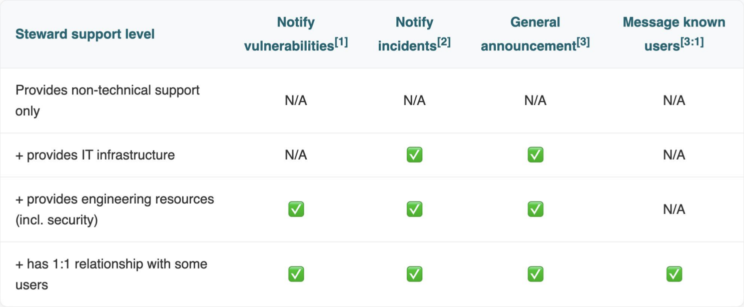
Corrective actions may be required if obligations aren't met.

Language Barrier

Language requirement is a practical issue (OSS is often English-first).

Reporting obligations: “it depends”

- Are you involved in development? If yes → exploited vulnerabilities reporting applies.
- Do you run project infrastructure? If yes → severe incident reporting applies.
- Do you have direct user lists? If yes → direct user notifications apply.



Steward support level	Notify vulnerabilities[1]	Notify incidents[2]	General announcement[3]	Message known users[3:1]
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	✅	✅	✅	✅

Full decision matrix: https://cra.orcwg.org/faq/stewards/notification-obligations/

Informing users: what good looks like

Public Channels

Public advisory page + mailing list/RSS

Comprehensive Content

What to include: impact, affected versions, mitigations, fix status

Machine-Readable Formats

Machine-readable recommended (e.g., CSAF)

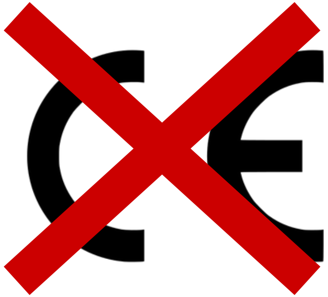
Voluntary reporting + CSIRT coordinator

Voluntary reporting is encouraged and shouldn't create extra obligations.

Identify your CSIRT coordinator (usually HQ country as a practical default).

Open questions for non-EU / language barriers.

Restriction: no CE marking for stewards

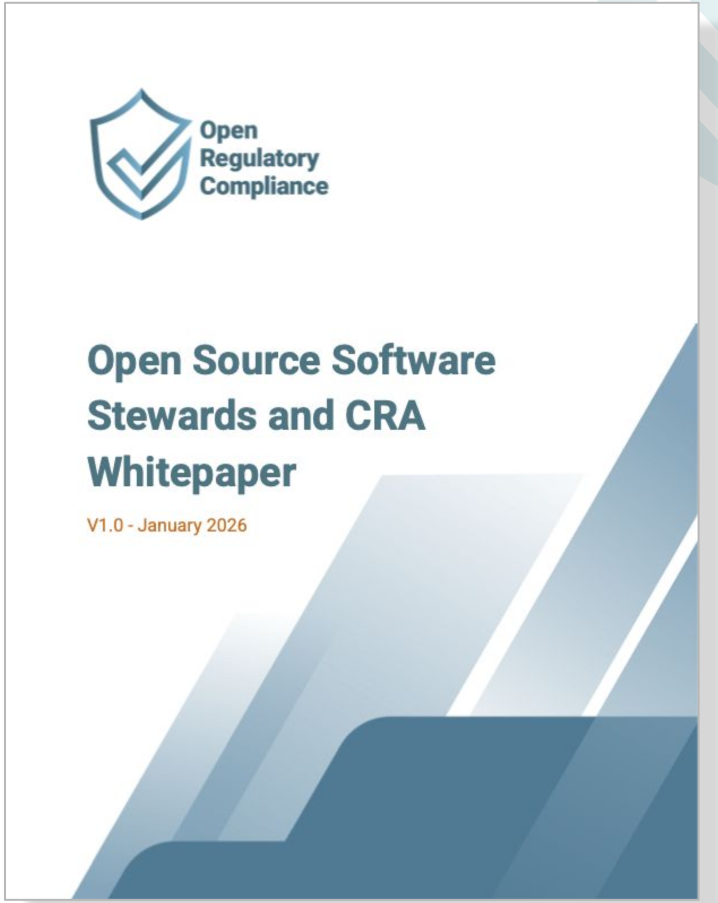


- Stewards cannot affix CE marking to the OSS they steward (lighter regime ≠ manufacturer regime).
- They don’t provide the full CRA manufacturer documentation.
- Stewards *may* run an attestation program to provide equivalent documentation for manufacturers’ use.

Whitepaper Available Today

Interpretation of the obligations and what they translate to in day-to-day OSS operations

https://orcwg.org



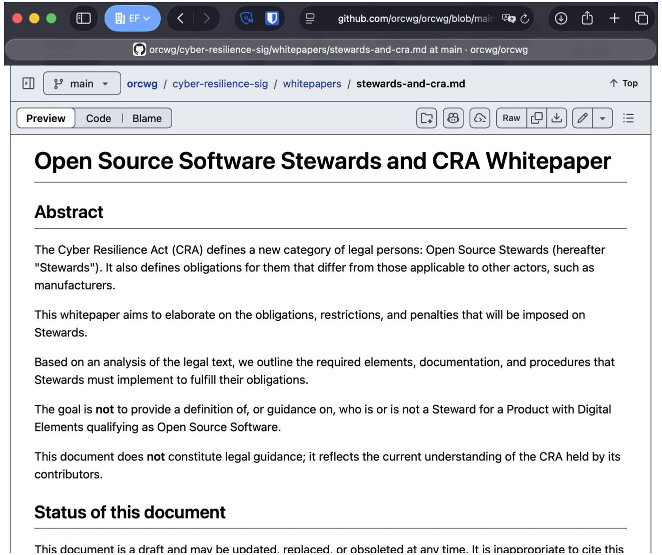
Open Regulatory Compliance

Open Source Software Stewards and CRA Whitepaper

V1.0 - January 2026

Publication of v1 is not the End

Issues, comments, and pull requests are welcome!


EF
github.com/orcwg/orcwg/blob/main
orcwg/cyber-resilience-sig/whitepapers/stewards-and-cra.md at main · orcwg/orcwg
main
orcwg / cyber-resilience-sig / whitepapers / stewards-and-cra.md
Top
Preview
Code
Blame
Raw

Open Source Software Stewards and CRA Whitepaper

Abstract

The Cyber Resilience Act (CRA) defines a new category of legal persons: Open Source Stewards (hereafter "Stewards"). It also defines obligations for them that differ from those applicable to other actors, such as manufacturers.

This whitepaper aims to elaborate on the obligations, restrictions, and penalties that will be imposed on Stewards.

Based on an analysis of the legal text, we outline the required elements, documentation, and procedures that Stewards must implement to fulfill their obligations.

The goal is **not** to provide a definition of, or guidance on, who is or is not a Steward for a Product with Digital Elements qualifying as Open Source Software.

This document does **not** constitute legal guidance; it reflects the current understanding of the CRA held by its contributors.

Status of this document

This document is a draft and may be updated, replaced, or obsoleted at any time. It is inappropriate to cite this

https://github.com/orcwg/orcwg/blob/main/cyber-resilience-sig/whitepapers/stewards-and-cra.md

Takeaways

If you are (or might be) a Steward, do these 5 things:

❏ Establish **steward↔project relationship** and governance leverage (policy adoption + enforcement).

❏ Publish a CRA-aligned, **verifiable security policy**; define evidence artifacts.

❏ Implement **vulnerability handling** + documentation workflows (advisories/CVE links discoverable).

❏ Define **reporting playbooks**: exploited vulnerabilities vs infra incident, and user notification channels.

❏ Identify your **CSIRT coordinator** and Market Surveillance Authority; decide language strategy.

Most gaps aren’t tooling
They’re governance and evidence

Thank you!

Mikael Barbero
Head of Security — Eclipse Foundation
https://linktr.ee/mbarbero