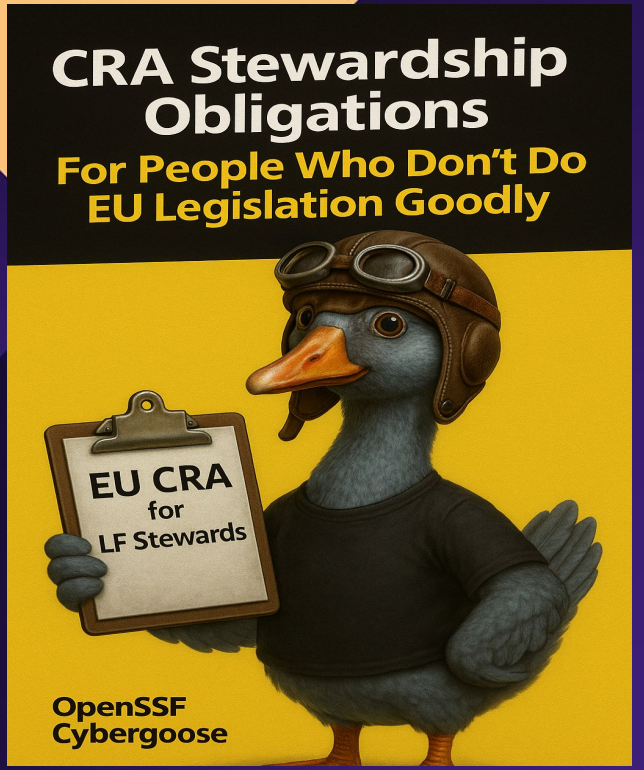
LF CRA Stewards Plan

The Cliff Notes Edition

November 2026



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Copyright © 2024 The Linux Foundation®. All rights reserved. The Linux Foundation has registered trademarks and uses trademarks.

Agenda

- Introduction
- CRA Stewards Obligations
- How the LF will act as a Steward
- Beyond Legal Obligations
- Next steps



TL/DR - CRA WAT

So… you “get to” do some CRA, eh?

Regulation (EU) 2024/2847 (Cyber Resilience Act, CRA)

The Cyber Resilience Act is a piece of European legislation that will go into full effect December of 2027 that puts new cybersecurity requirements on any “product with digital elements” “put onto” or “made available” on the common market.

Predominantly focused on commercial vendors (“Manufacturers”), it will require proof of due diligence and software development/design activities as well as vulnerability reporting/coordination.

While not directly impacted by or beholden to the upcoming law, open source developers WILL be affected by their downstream consumers attempting to meet THEIR legal obligations.

A new legal category “Open Source Software Steward” (“Steward” going forward) has been created that broadly defines a handful of obligations for entities such as the Linux Foundation and our numerous sub-projects/foundations.

Stewards have three legal obligations under the CRA.



LF CRA Steward “One-Pager”

LF CRA Steward Playbook

- **Oct 2026** Vulnerability Reporting for Manufacturers in force
- **Dec 2027** All CRA requirements fully enforced for all stakeholders

Why Steward Something?

Look for the Helpers - OSS Stewards are legal entities that support a project, community, or ecosystem that is used downstream commercially. Being a Steward is a visible, public demonstration of support and sends a positive signal of the health and utility of a project.

Not every project needs a Steward (docs-only, specs, archived projects, etc.). Consider taking the Steward role for graduated projects that are used downstream in commercial products sold within the EU*.

Certain capabilities are offered at the LF top-level that may be sufficient for your community's needs. You community may already have some of these capabilities (such as a security policy, vuln. management team).

**Internationally other jurisdictions are considering similar requirements, so "no presence in the EU" does not necessarily exclude us from doing anything.*

Requirement 1

Citation	Requirement
Article 24.1	Open-source software stewards shall **put in place and document … a cybersecurity policy** to … <manage the>... **effective handling of vulnerabilities** … as laid down in **Article 15** … 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.

***Req 1 TL/DR** - Projects must have a publicly accessible security and vulnerability handling policy.*

Solution 1

If your foundation and projects do not already have a security policy or vulnerability disclosure policy consider:

- Deferring to/using the LF top-level security/reporting policy
- Fork and update one of these templates
  - security.md (Vulnerability Disclosure OSS Maintainer CVD Guide)
  - https://github.com/ossf/oss-vulnerability-guide/tree/main/templates/security_policies
- Consider developing a security team-like capability for your projects to assist in these efforts.

Requirement 2

Citation	Requirement
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.

***Req 2 TL/DR** - If your Projects are contacted by EU-authorities, assist them as able.*

Solution 2

- Know which of your subprojects could be included in downstream commercial products and understand how you will react to requests for documentation or assistance in Coordinated Vulnerability Disclosure (CVD).
- Establish communication paths to security contacts for projects (vulnerability intake, triage, and reporting processes; playbooks; trusted external partners, etc.)

Requirement 3

Citation	Requirement
Article 24	…**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**.

Req 3 TL/DR *- Projects must report known exploited vulnerabilities related to any cyber security breaches that impact infrastructure supporting those projects to ENISA + National CSIRTs.*

Solution 3

- Establish processes to monitor and alert on core infrastructure supporting projects (e.g. CI/CD and other shared services).
- Determine an EU National CSIRT to also report these breaches to along with ENISA via the Single Reporting Platform.
- Develop the capability to quickly assess and provide information around vulnerabilities reported with your projects.

How the LF is approaching Stewardship



8

A Top-level solution for most....

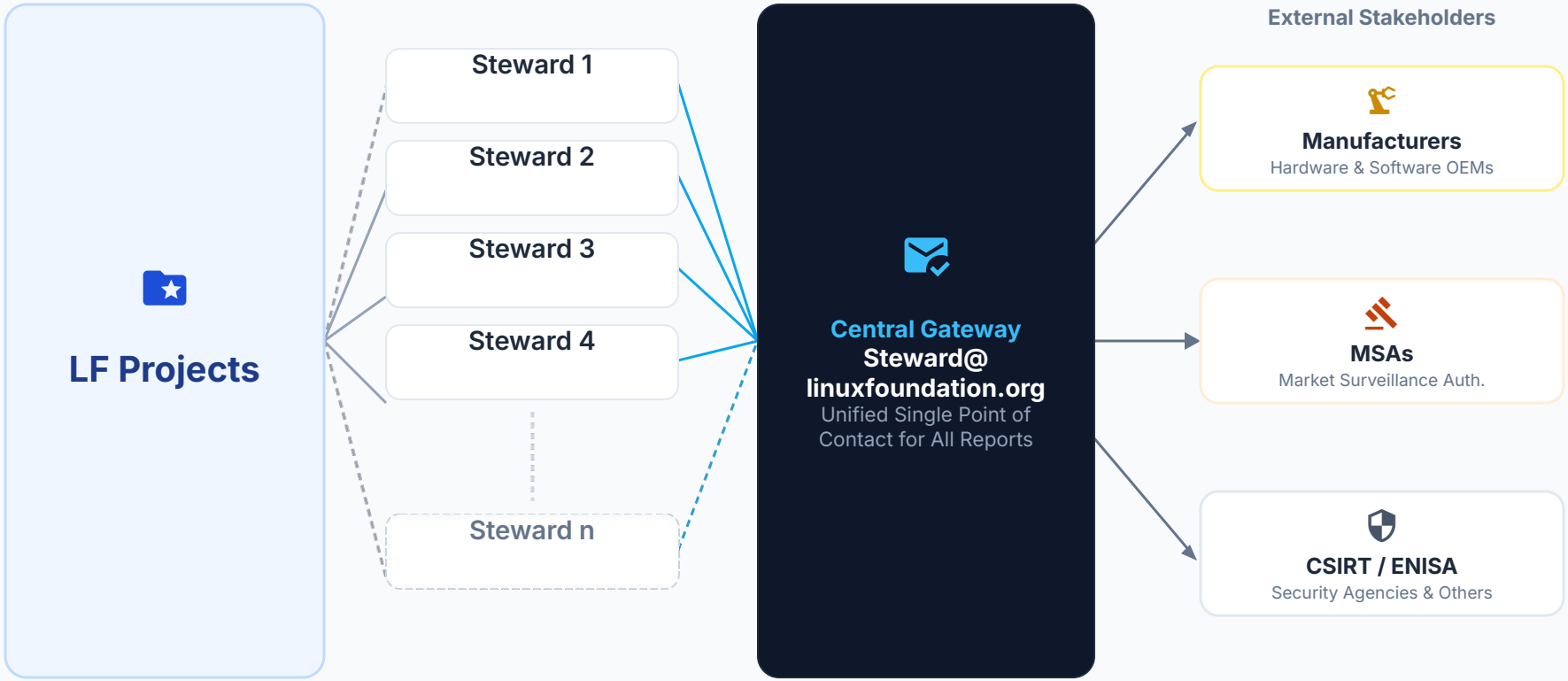
...flexibility for self-control for those that choses it.

Leadership for all.



Stewardship Communication Architecture

Centralized reporting and coordination model between Linux Foundation projects and external entities



Steward

What is FOSS in CRA terminology?

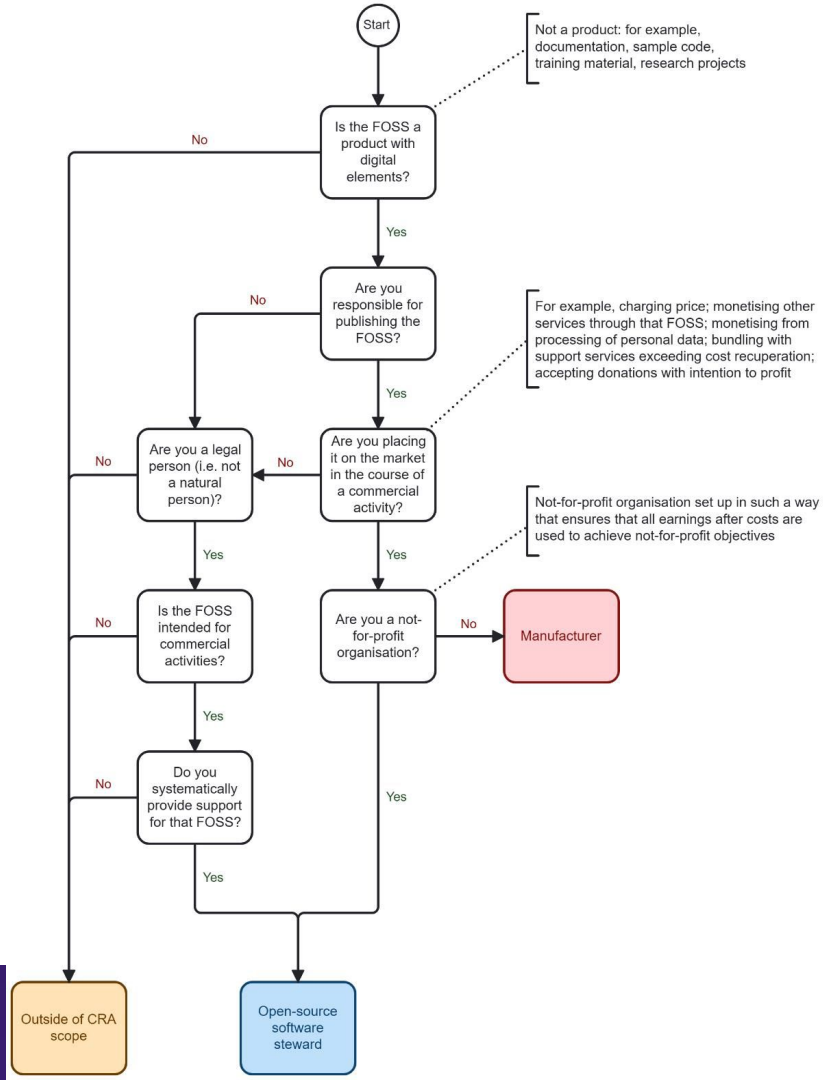
- "software the source code of which is **openly shared** and which is **made available under a free and open-source licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable**" (CRA Guidance, 44: Article 3(48))

Concept of steward

- "**legal person** that supplies a FOSS intended for commercial activities, but does not place it on the market within the meaning of the CRA."
- "applies to **specific instances of FOSS that 'are ultimately intended for commercial activities, such as for integration into commercial services or into monetised products with digital elements**" (CRA Guidance, 47&71, *recital 19*)

Sustained support

- "*the provision of sustained support to the development of a product with digital elements may include (but is not limited to):* ***(i) the hosting and managing of software development collaboration platforms; (ii) hosting source code or software; (iii) governing or managing products with digital elements q*****ualifying as FOSS; and (iv) steering the development of such products with digital elements.**" (CRA Guidance, 75; *Recital 19*)



- https://ec.europa.eu/newsroom/dae/redirection/document/131456
- https://openssf.org/wp-content/uploads/2026/09/LF-Supported-Projects-and-CRA-Readiness-2026-09-10.pdf

Be ready to report

- What to report?
  - **Actively Exploited Vulnerabilities:** Vulnerabilities in products with digital elements that are known to be currently exploited by a malicious actor, in accordance with Article 3(42) of the CRA.
  - **Severe Incidents:** Incidents that have a severe impact on the security of the product with digital elements (e.g., compromising availability, authenticity, integrity, or confidentiality) in accordance with Article 3(44); the criteria for severity are defined in Article 14(5).

- When?



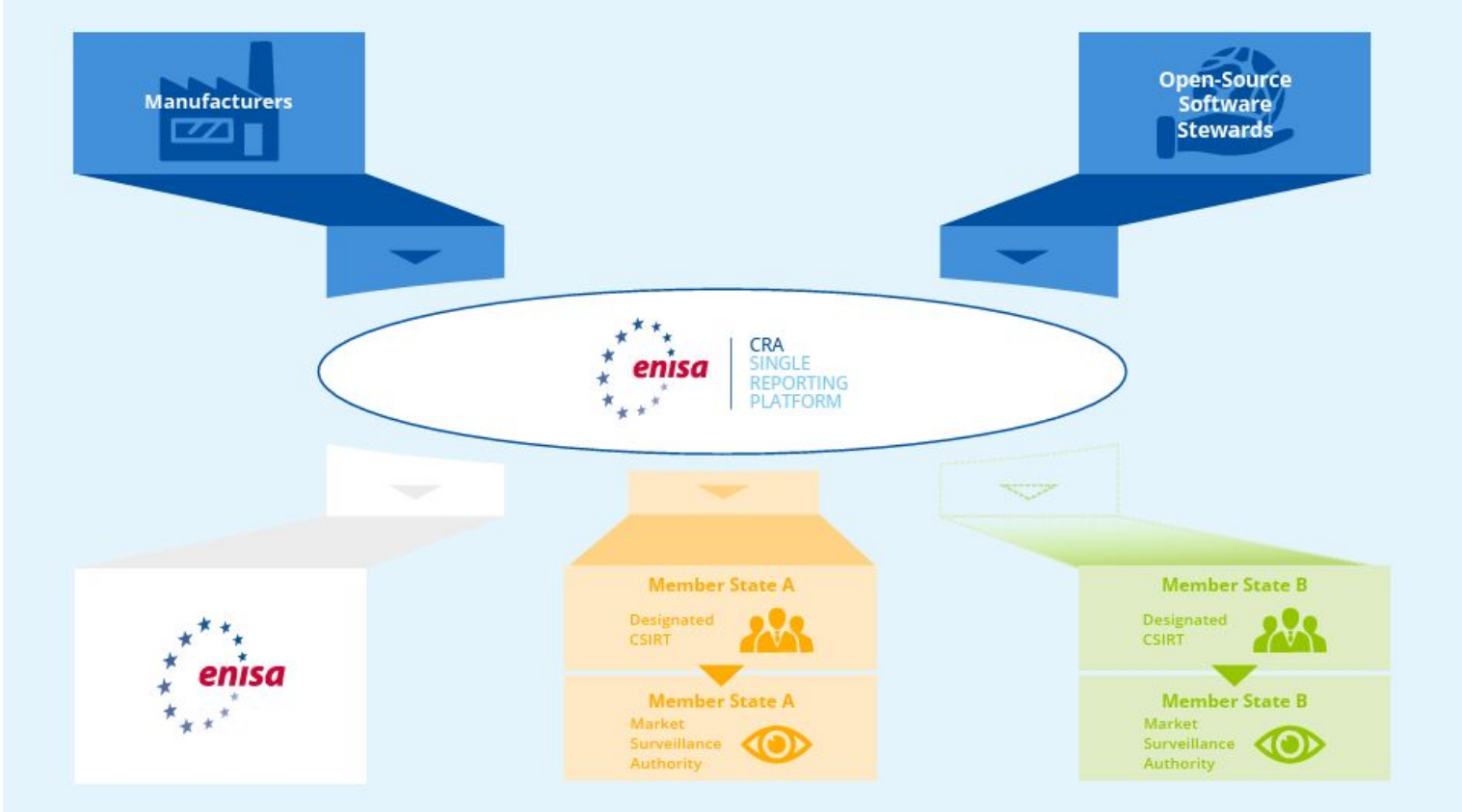
internal procedures to ensure timely identification, triage, and escalation of vulnerabilities and incidents that may trigger CRA reporting obligations;

a process capable of meeting the 24-hour, 72-hour and final-report deadlines

https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA_CRA_SRP_Factsheet_v1.0_0.pdf

EU SRP

- Article 16



https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA_CRA_SRP_Factsheet_v1.0_0.pdf

LF CRA Journey



CVE

OSV | Open Source Vulnerabilities

CVE CNA-LR

enisa | EUROPEAN UNION VULNERABILITY DATABASE

NVD



Sept 11, 2026 | Nov 2026 | Q1 2027 | Dec 11, 2027





CENTRE FOR CYBERSECURITY BELGIUM

AKRITES



OpenVEX

enisa | CRA SINGLE REPORTING PLATFORM

- Sept 11, 2026 - *Steward@LF.org* online & accepting incoming requests from projects and external entities; AEVs & SIs published via *SIREN* mailing list; Belgium's CCB selected as LF's National CSIRT
- Nov 2026 Akrites SIRT becomes CVE CNA for LF projects
- Q4 2026 Akrites publishes VDRs via GitHub repository; explore publication to OSV
- Q1 2027 Akrites becomes CNA-LR for "open source"
- Q2 2027 Akrites publishes reports to CVE List/NVD and EUVD, Akrites LF Project API for reporting
- Q3 2027 Akrites publishes VEX statements
- Q4 2027 EU SRP API online?
- Dec 11, 2027 Akrites sends AEVs & SIs to EU SRP

LF CRA Stewardship and responsibilities

Some of our Stewards

- The Linux Foundation
- Linux Foundation Europe
- LF Projects, LLC
- Joint Development Foundation Projects, LLC
- LF Charities, Inc.
- The Linux Kernel Organization
- LF Open Source, LLC

EU reporting capability

Primary AR + the Secondary ARs registered with a personal EU Login account and able to file reports through the SRP

Deadline-capable processes

Internal triage and escalation procedures built to meet the CRA's 24-hour early warning, 72-hour notification, and final-report deadlines.

CSIRT relationship

Identification of and collaboration with the relevant national coordinating CSIRT (e.g. Belgium's Center for Cybersecurity, based on Linux Foundation Europe's establishment in Brussels)

Authority interface

Acting as the CRA point of contact for market surveillance authorities and coordinating responses, so authorities deal with the steward, not with individual maintainers.

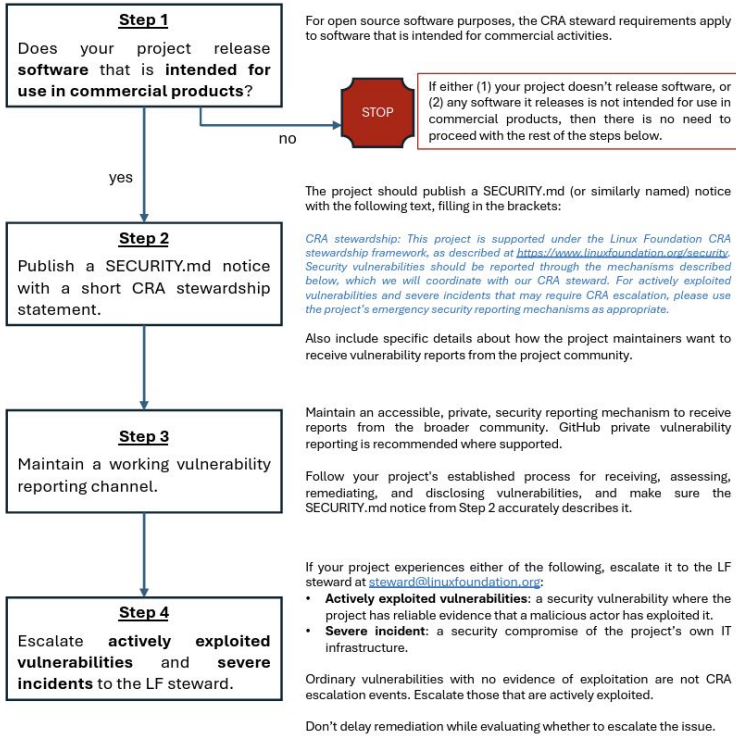
Cybersecurity policy

A cohesive cybersecurity policy fostering secure development across covered foundations and projects, as CRA Article 24 requires of stewards.

Records and review

Documentation of stewardship arrangements, covered foundations/projects, communications with market surveillance authorities, and evidence of fulfilment of responsibilities. Periodic review when circumstances change.

LF-Supported Projects and CRA Readiness



complement it with

Add to your repository and/or to your webpage:

This project voluntarily documents its security practices.

This information is provided "as is", without warranties or guarantees. See the project's license for more details.

The maintainers and contributors:

- have no obligations under the EU CRA,
- are not Manufacturers, Importers, or Economic Operators,
- assume no financial, contractual, or legal liability,
- and do not provide CRA compliance assurances.

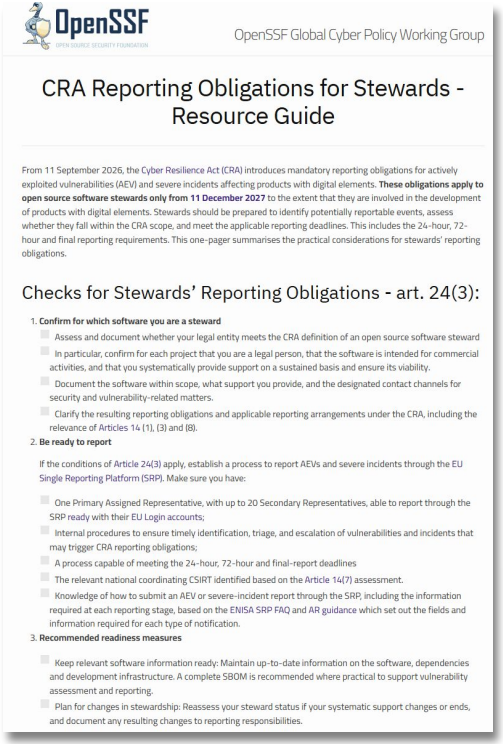
Anyone incorporating this software into commercial products remains solely responsible for such products, including regulatory compliance, risk assessment, and vulnerability management.

Supporting the LF around the globe

- OpenSSF/Akrites holds regular meeting with ENISA, CCB, and other EU Authorities
- German BSI periodically reaches out to both for consultations on guidance (SBOM, Vuln Management, etc.)
- We are in ongoing talks with METI from Japan and KISA from South Korea as both of those nations consider CRA-like legislation.
- Greg KH & Madalin Neag are members of the CRA Expert group, and the kernel was involved in the EU SRP testing.
- OpenSSF has held AMA sessions for LF projects and community meetings for our members to prepare for the deadlines.
- We've worked with LF Research on two reports (1)(2) and plan a 3rd report for 2027 that speaks to ecosystem readiness.

1.) 2025 -Unaware and Uncertain The Stark Realities of Cyber Resilience Act Readiness in Open Source
2.) 2026 CRA Awareness and Readiness

Supporting LF Projects, Maintainers, Members, and the Community



OpenSSF Global Cyber Policy Working Group

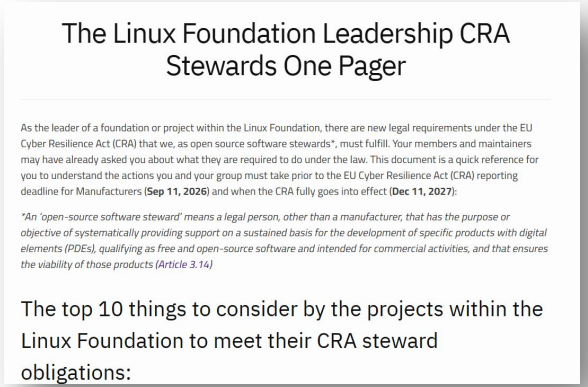
CRA Reporting Obligations for Stewards - Resource Guide

From 11 September 2026, the Cyber Resilience Act (CRA) introduces mandatory reporting obligations for actively exploited vulnerabilities (AEV) and severe incidents affecting products with digital elements. **These obligations apply to open source software stewards only from 11 December 2027** to the extent that they are involved in the development of products with digital elements. Stewards should be prepared to identify potentially reportable events, assess whether they fall within the CRA scope, and meet the applicable reporting deadlines. This includes the 24-hour, 72-hour and final reporting requirements. This one-pager summarises the practical considerations for stewards' reporting obligations.

Checks for Stewards' Reporting Obligations - art. 24(3):

1. **Confirm for which software you are a steward**
   - Assess and document whether your legal entity meets the CRA definition of an open source software steward
   - In particular, confirm for each project that you are a legal person, that the software is intended for commercial activities, and that you systematically provide support on a sustained basis and ensure its viability.
   - Document the software within scope, what support you provide, and the designated contact channels for security and vulnerability-related matters.
   - Clarify the resulting reporting obligations and applicable reporting arrangements under the CRA, including the relevance of Articles 14 (1), (3) and (8).
2. **Be ready to report**

   If the conditions of Article 24(3) apply, establish a process to report AEVs and severe incidents through the EU Single Reporting Platform (SRP). Make sure you have:
   - One Primary Assigned Representative, with up to 20 Secondary Representatives, able to report through the SRP ready with their EU Login accounts;
   - Internal procedures to ensure timely identification, triage, and escalation of vulnerabilities and incidents that may trigger CRA reporting obligations;
   - A process capable of meeting the 24-hour, 72-hour and final-report deadlines
   - The relevant national coordinating CSIRT identified based on the Article 14(7) assessment.
   - Knowledge of how to submit an AEV or severe-incident report through the SRP, including the information required at each reporting stage, based on the ENISA SRP FAQ and AR guidance which set out the fields and information required for each type of notification.
3. **Recommended readiness measures**
   - Keep relevant software information ready: Maintain up-to-date information on the software, dependencies and development infrastructure. A complete SBOM is recommended where practical to support vulnerability assessment and reporting.
   - Plan for changes in stewardship: Reassess your steward status if your systematic support changes or ends, and document any resulting changes to reporting responsibilities.



The Linux Foundation Leadership CRA Stewards One Pager

As the leader of a foundation or project within the Linux Foundation, there are new legal requirements under the EU Cyber Resilience Act (CRA) that we, as open source software stewards*, must fulfill. Your members and maintainers may have already asked you about what they are required to do under the law. This document is a quick reference for you to understand the actions you and your group must take prior to the EU Cyber Resilience Act (CRA) reporting deadline for Manufacturers (**Sep 11, 2026**) and when the CRA fully goes into effect (**Dec 11, 2027**):

**An 'open-source software steward' means 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 (PDEs), qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products (Article 3.14)*

The top 10 things to consider by the projects within the Linux Foundation to meet their CRA steward obligations:

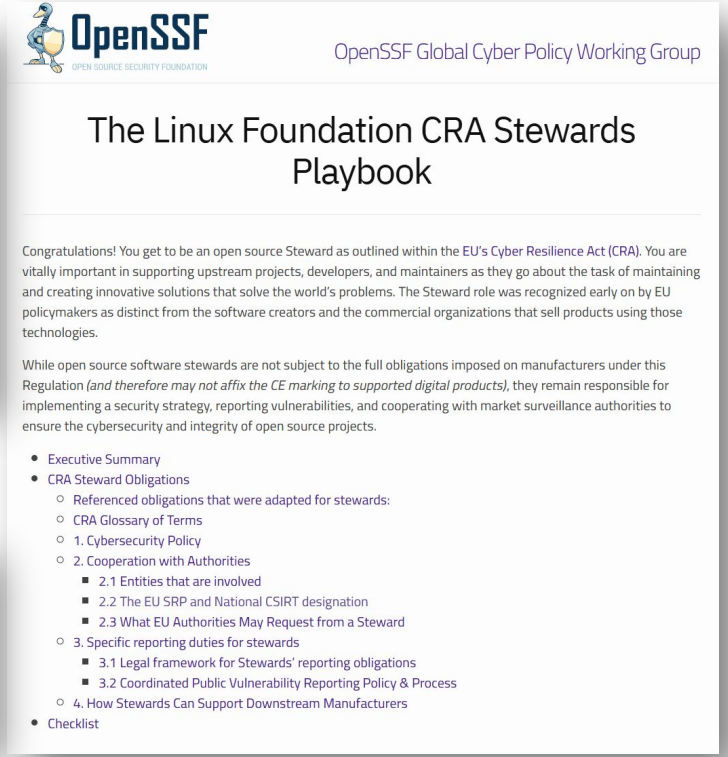


OSS Stewards Obligations Checklist

This is a checklist of the requirements Open Source Stewards must fulfill to meet the requirements laid out in the CRA

An Open Source Steward is defined in Article 3.14 as:

> *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*



OpenSSF Global Cyber Policy Working Group

The Linux Foundation CRA Stewards Playbook

Congratulations! You get to be an open source Steward as outlined within the EU's Cyber Resilience Act (CRA). You are vitally important in supporting upstream projects, developers, and maintainers as they go about the task of maintaining and creating innovative solutions that solve the world's problems. The Steward role was recognized early on by EU policymakers as distinct from the software creators and the commercial organizations that sell products using those technologies.

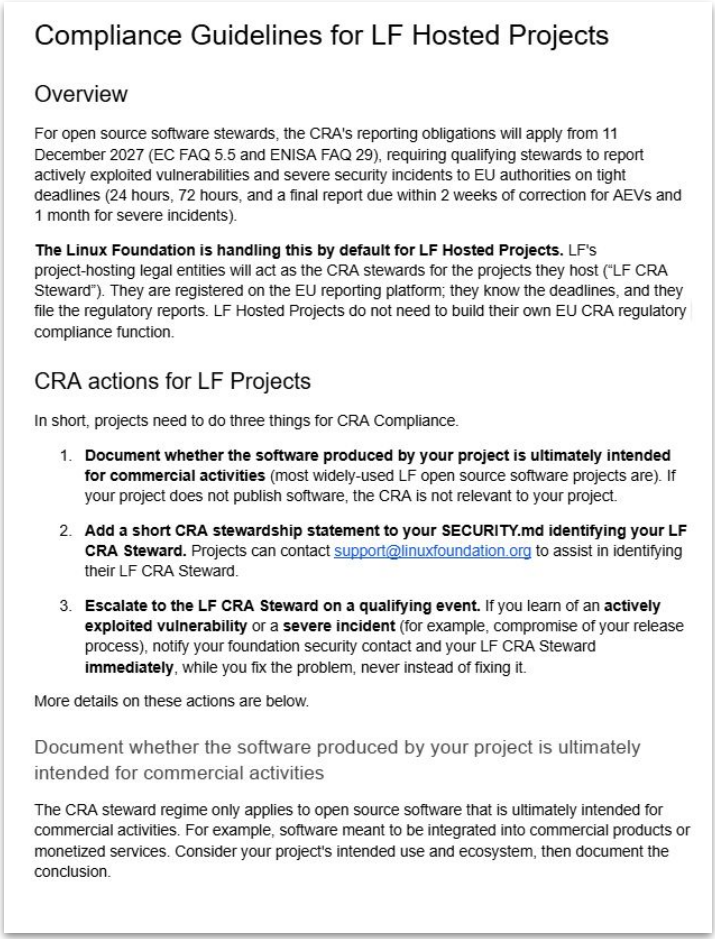
While open source software stewards are not subject to the full obligations imposed on manufacturers under this Regulation *(and therefore may not affix the CE marking to supported digital products)*, they remain responsible for implementing a security strategy, reporting vulnerabilities, and cooperating with market surveillance authorities to ensure the cybersecurity and integrity of open source projects.

- Executive Summary
- CRA Steward Obligations
  - Referenced obligations that were adapted for stewards:
  - CRA Glossary of Terms
  - 1. Cybersecurity Policy
  - 2. Cooperation with Authorities
    - 2.1 Entities that are involved
    - 2.2 The EU SRP and National CSIRT designation
    - 2.3 What EU Authorities May Request from a Steward
  - 3. Specific reporting duties for stewards
    - 3.1 Legal framework for Stewards' reporting obligations
    - 3.2 Coordinated Public Vulnerability Reporting Policy & Process
  - 4. How Stewards Can Support Downstream Manufacturers
- Checklist

- https://policy.openssf.org/CRA/stewards-one-pager.html
- https://policy.openssf.org/CRA/checklists/Stewards_December_Checklist.html
- https://policy.openssf.org/CRA/stewards-playbook.html

To learn more....

This guide encompasses our other output into a more comprehensive document for those eager to learn more about the specifics “beyond the checklist”



Compliance Guidelines for LF Hosted Projects

Overview

For open source software stewards, the CRA's reporting obligations will apply from 11 December 2027 (EC FAQ 5.5 and ENISA FAQ 29), requiring qualifying stewards to report actively exploited vulnerabilities and severe security incidents to EU authorities on tight deadlines (24 hours, 72 hours, and a final report due within 2 weeks of correction for AEVs and 1 month for severe incidents).

The Linux Foundation is handling this by default for LF Hosted Projects. LF's project-hosting legal entities will act as the CRA stewards for the projects they host (“LF CRA Steward”). They are registered on the EU reporting platform; they know the deadlines, and they file the regulatory reports. LF Hosted Projects do not need to build their own EU CRA regulatory compliance function.

CRA actions for LF Projects

In short, projects need to do three things for CRA Compliance.

1. **Document whether the software produced by your project is ultimately intended for commercial activities** (most widely-used LF open source software projects are). If your project does not publish software, the CRA is not relevant to your project.
2. **Add a short CRA stewardship statement to your SECURITY.md identifying your LF CRA Steward.** Projects can contact support@linuxfoundation.org to assist in identifying their LF CRA Steward.
3. **Escalate to the LF CRA Steward on a qualifying event.** If you learn of an **actively exploited vulnerability** or a **severe incident** (for example, compromise of your release process), notify your foundation security contact and your LF CRA Steward **immediately**, while you fix the problem, never instead of fixing it.

More details on these actions are below.

Document whether the software produced by your project is ultimately intended for commercial activities

The CRA steward regime only applies to open source software that is ultimately intended for commercial activities. For example, software meant to be integrated into commercial products or monetized services. Consider your project's intended use and ecosystem, then document the conclusion.

Thank You



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Full text of Applicable Articles

CRA Stewards Obligations

Emphasis added

Area	Citation	Requirement	*TL/DR*
Cyber Policy	Article 24	1. Open-source software stewards shall **put in place and document i**n 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.	*security.md +vuln reporting process/link*
	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.	*cooperate with M.S.A. to mitigate risks*
		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.	*policy posted electronically, translated*
Vuln Reporting	Article 24	3. 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**.	*Report vulns and known exploits to the Union*

CRA Stewards Obligations, continued

Area	Citation	Requirement	*TL/DR*
Vuln Reporting	Article 14.1	For the purposes of the notification referred to in paragraph 1, the **manufacturer** shall submit: **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.	*establish an EU National CSIRT contact, report known actively exploited vulns to EU National CSIRT contact and ENISA*
	Article 14.3	**A manufacturer shall notify any severe incident having an impact on the security of 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 incident via the single reporting platform established pursuant to Article 16.	*establish an EU National CSIRT contact, report "severe" vulns to EU National CSIRT contact and ENISA*
	Article 14.8	**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.	*notify end-consumers of "severe" vulnerabilities*

Legal Notice

Copyright © Akrites®, Open Source Security Foundation®, The Linux Foundation®, & their contributors. The Linux Foundation has registered trademarks and uses trademarks. All other trademarks are those of their respective owners.

Per the OpenSSF Charter, this presentation is released under the Creative Commons Attribution 4.0 International License (CC-BY-4.0), available at <https://creativecommons.org/licenses/by/4.0/>. You are free to:

- Share — copy and redistribute the material in any medium or format for any purpose, even commercially.
- Adapt — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms:

- Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.