Open Regulatory Compliance

Contribution to Vulnerability Handling Standard Clause 4.4

2.2 | Inputs & contributions

Deliverable:	2.2
Category:	Inputs & contributions
Owner:	Cyber Resilience SIG
Status:	Shipped
License:	CC-BY-SA 4.0
Date:	December 2025

Contribution to CEN/CENELEC Vulnerability Handling Standard Clause 4.4

Request

Provide the content for the informative section on open source software stewards (Clause 4.4).

Context

- This is the standard for vulnerability handling covering the requirements defined in Annex I, Part II of the CRA.
- The standard only focuses on whats in this annex, not any other obligations.
- The standard is aimed at manufacturers, not stewards.
- The section were asked to contribute too is informative (not normative), which means it doesnt create any requirements for anybody; its just there to provide context.

Goals for the submission

Remind the reader that:

- There are such a thing as stewards.
- This standard doesnt place requirements on stewards.
- Manufacturers might be considered as stewards for some of their open source projects.
- Manufacturers need to interface with stewards for reporting vulnerabilities.
- Stewards dont have to fix vulnerabilities that are reported to them, nor do they have to accept fixes for it. In particular they wont if those fixes dont meet the projects IP requirements.
- Not all open source projects have stewards and manufacturers might still need to interface with them.
- The existence of a steward isnt a guarantee that the project meets manufacturer security requirements, manufacturers will need to exercise due diligence regardless. Free and open source security attestations might help facilitate due diligence in the future.

Rationale for these goals:

- Stewards are a new class of actors that manufacturers might not be familiar with, its useful to give them additional context.

• Theres a common misconception that all open source projects will have stewards, it is useful to remind manufacturers that this isnt the case.

• As this standard will be behind a paywall, we want to avoid placing any requirements on open source in it.

Contribution submitted on May 20, 2025

The CRA introduces a new class of market actors: Open-Source Software Stewards (Stewards). This standard does not place any requirements on Stewards. However, the CRA does impose a number of obligations on Stewards, particularly to facilitate vulnerability handling.

Manufacturers are expected to interface with Stewards when reporting vulnerabilities they have discovered in open-source products that the Steward supports. Manufacturers are encouraged to contribute fixes they might have developed for those vulnerabilities under a license compatible with the open-source product.

To facilitate the reporting of vulnerabilities, Stewards shall create, implement, make publicly available, and ensure adherence to a policy on vulnerability handling for the products for which they are Stewards.

Not all open-source projects that a manufacturer depends on should be expected to be supported by a Steward. The obligations of the manufacturers towards those projects remain the same regardless.

Stewards are not responsible for developing remedies for the vulnerabilities reported in the software for which they are Stewards. However, a Steward must report severe incidents of which they are aware that impact the tools and services they provide to support open-source software development. Additionally, a Steward has a limited reporting obligation if they are involved in developing the open-source software for which they are Stewards.

Acknowledgments

The following people have contributed to this document either directly or indirectly (e.g. by raising questions):

Arnout Engelen,
Juan Rico,
Lars Francke,
Marta Rybczynska,
Mikael Barbero,
Timo Perala,
and Tobie Langel.

If you have contributed to this document and arent properly acknowledged or if you want to edit or remove your name, please let us know by opening an issue and we will fix this right away.