Open Regulatory Compliance

Comments on CEN/CENELEC PT 1 Standard

2.5 | Inputs & contributions

Deliverable:	2.5
Category:	Inputs & contributions
Owner:	CEN/CENELEC WG 9 PT 1 liaisons
Status:	Shipped
License:	CC-BY-SA 4.0
Date:	December 2025

Comments to CEN/CENELEC PT 1 Standard

Request

As part of its process, CEN/CENELEC WG 9 PT 1 requested comments on its Horizontal standard on General principles for cyber resilience (JT013089) from its working group participants (note this was not a public call for comments).

Goals

1. Prevent the open source ecosystem from having to purchase standards to comply to the CRA
Prevent requirements placed on stewards, open source projects, and maintainers in CEN/CENELEC standards as these standards arent freely available.

2. Avoid placing unnecessary demands on the open source ecosystem
Prevent requirements placed on manufacturers that rely on stewards, open source projects, or maintainers performing certain actions they have no obligations to perform.Prevent requirements that might lead manufacturers to expect the same interactions with stewards, open source projects, or maintainers as they have with their suppliers.

3. Maintain a leveled playing field
Prevent requirements placed on manufacturers which unfairly favor proprietary software (such as mandating security by obscurity, for example).

4. Maintain Europes ability to leverage open source
Prevent requirements that unreasonably burden manufacturers integrating open source components.

Comments

We identified two sections of the Horizontal standard on General principles for cyber resilience (JT013089) that were concerning given the goals stated above and submitted comments for them:

Clause 5.5 describes a required consultation process when integrating third-party components, including open source software, that would require manufacturers to build a 1:1 relationship with open source maintainers in order to integrate open source components.

Clause 6.12 essentially describes due diligence requirements for third-party components and includes a number of requirements that are concerning given the above-mentioned goals.

We submitted our comments on June 12, 2025 using the requested docx template.

Copyright © Eclipse Foundation AISBL and contributors. Made available under CC-BY-SA 4.0 International

At a high-level, our comments centered around the folllowing four concerns:

1. Incorrect assumption that manufacturers should expect similar relationships with open source maintainers and stewards as they have with commercial suppliers

The standard operates from the perspective that every component has a supplier that manufacturers are expected to have a direct contractual relationship with. Thats particularly obvious in clause 5.5 which requires a consultation to happen between manufacturer and supplier notably leading to documentation containing agreement to responsibility distribution (5.5.4).

Open source maintainers and stewards are not suppliers for the software they provide for free.

As the CRA recognizes, there are no requirements on open source maintainers nor on open source software stewards to engage in consultations with users of their software, nor to provide documentation beyond what is required of stewards in Article 24(1). Manufacturers shouldnt be led to believe that this is the case, as it will cause already overburdened open source maintainers to have to field consultation requests from well-meaning manufacturers or deal with demands for responsibility distribution instead of focusing on securing their software. Open source projects might make freely available information that helps manufacturers exercise due diligence, and a future security attestation program might facilitate this further (possibly for a fee), but that is the extent of the relationship manufacturers should expect. The standards need to reflect this reality and should not expect open source maintainers or stewards to enter into a direct relation with the manufacturers that chose to integrate their software.

2. Incorrect assumption that open source maintainers and stewards exercise due diligence of their own dependencies

Because of the incorrect assumption that open source maintainers and stewards are suppliers, the standard implicitly assumes that open source maintainers and stewards are required to exercise due diligence for their own dependencies as if they were themselves manufacturers. Of course, this isnt the case as neither open source maintainers nor stewards are subject to due diligence obligations. Manufacturers will need to exercise their due diligence requirements for both their open source components, and the dependencies of those components, recursively. In particular, the second part of Clause 6.12.3, is focused on the requirements of manufacturers to the components themselves, and doesnt seem to consider that manufacturers are responsible for the dependencies of those components and the dependencies of those dependencies, recursively. Concretely, dependencies of open source components might require different treatment of associated risks, different controls, dedicated monitoring and review procedures, etc. than the components themselves. The standards need to reflect the reality of the recursive component structure of open source software and acknowledge that the responsibility of manufactures extends across that whole supply chain and not just to the layer that is directly visible to them.

Copyright © Eclipse Foundation AISBL and contributors. Made available under CC-BY-SA 4.0 International

3. Requirements for third-party components doesnt account for the security benefits of open source transparency

Contrary to industry best practices, section 6.12.3 treats all components the same regardless of whether or not they are open source. As open source components can be easily audited by manufacturers or third parties due to the transparency of their codebases, manufacturers can independently assess their fitness for purpose, the presence of appropriate controls, the security of the code base, etc. regardless of how they were developed or what documentation is provided. The transparency of open source provides security guarantees that the industry understands and knows how to leverage. By failing to account for this, the standard is making it unreasonably difficult for manufacturers to leverage open source. The standards should acknowledge the security benefits provided by open source transparency and account for industry best practices for consuming open source software in the requirements it specifies.

4. Pass/fail structure of requirements risk dis-incentivising investments in open source security

The pass/fail structure of the first section of 6.12.3, means that the vast majority of open source projects will fall to the second part of the section regardless of any improvements they might be able to make to their security posture. If improving the security of open source projects doesnt lighten the compliance burden of manufacturers integrating them (or only does so marginally), this risks dis-incentivising investments from said manufacturers to improve the security of the open source projects they rely on. The standards should consider open source components specifically and take care not to dis-incentivize investments to improve their security postures, as more cyber resilient open source components directly benefit EU citizens and businesses.

Acknowledgments

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

Juan Rico,
Lars Francke,
Timo Perälä,
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.

Copyright © Eclipse Foundation AISBL and contributors. Made available under CC-BY-SA 4.0 International