standICT.2026.eu

ICT Standardisation Observatory and Support Facility in Europe

Case Study 2

The EU Cyber Resilience Act and Software Standards

Álvaro Vilas Gomez (OFE)

Funded by the European Union

February 2026

1. Introduction

This case study examines the relationship between the European Union's Cyber Resilience Act (CRA) and the evolving landscape of software standards, focusing particularly on the critical role of open source software (OSS) in driving innovation and digital transformation. Introduced as part of the EU's digital legislation during the 2019-2025 mandate, the CRA aims to strengthen cybersecurity standards for software and hardware products within the EU market. Central to this initiative is the collaboration between European Standardisation Organisations (ESOs) and the open source community to develop harmonised standards that address cybersecurity requirements across the software lifecycle and supply chain. This collaboration highlights the importance of integrating open source considerations into broader policies to ensure a balanced and inclusive approach to standardisation.

The case study looks into the experiences of the software ecosystem as it engages with the European Standardisation System, highlighting the steps taken by ESOs to include open source stakeholders in response to the CRA's standardisation request. A key focus is the Eclipse Foundation's Open Regulatory Compliance Working Group (ORC), launched in September 2024. The ORC aims to support the open source ecosystem in creating open specifications to meet the CRA's regulatory requirements, fostering collaboration with ESOs and European institutions.

Through this exploration, the case study underscores the importance of adapting standardisation processes to accommodate a diverse group of experts and contributors from the software community, ensuring the timely implementation of the CRA by the August 2026 deadline.

2. Analysis

The Collaboration Challenge of the ESOs and the OSS Community

For software manufacturers, the CRA represents the first horizontal EU legislation that sets specific obligations to enhance cybersecurity in their products. This legislation underscores the need for ESOs to adapt their processes to accommodate diverse stakeholders, including those from the open source community, who may not fit the traditional multi-stakeholder model. Additionally, the CRA requires manufacturers to maintain mandatory documentation to prove their compliance, including Software Bills of Materials and EU Declarations of Conformity. This documentation should be accessible to users under certain conditions and include relevant information regarding the product's compliance with the CRA. The inclusion of open source stakeholders in this process is crucial for ensuring that standards remain relevant and effective in the face of rapid technological advancements.

To help market actors meet these obligations, harmonised standards will play an important role. The European Commission has requested ESOs to develop 41 harmonised standards for the CRA, as set out in Annex I and the standardisation request.

The standardisation request outlines specific obligations for ESOs to ensure effective participation of relevant stakeholders, including those typically involved in these processes in accordance with Article 5 of Regulation (EU) No 1025/2012, such as small and medium-sized enterprises (SMEs) and civil society organisations. Notably, the CRA's standardisation request includes direct references to the inclusion of the open source community.

- **Recital 8** of the standardisation request emphasises that ESOs are tasked with ensuring effective coordination among various technical committees involved in developing vertical harmonised standards, with a particular focus on addressing the needs of the open source software community.

- **Article 3(2)** mandates that the draft work programme must outline actions to ensure the effective participation of the open source community where relevant.
- **Article 5(5b)** requires that reports include evidence demonstrating how ESOs have facilitated the representation and participation of the open source community, ensuring their involvement in the standardisation process.

This aligns with Regulation 1025/2012 but introduces a novel element by explicitly referencing the open source community. This is significant for both ESOs and the open source community, which by its nature does not fit the traditional multi-stakeholder model typically seen in EU legislation and standardisation. The open source community is not an industry or interest group.

The standardisation request explicitly obliges ESOs to ensure this process, but in practice, it also puts expectations on the open source community to organise itself effectively to participate in the standardisation process. Two culturally and structurally different communities that engage in collaborative innovation need to work together.

The Experience of the First Phases of Collaborating

The CRA and the standardisation request have sparked numerous activities within the open source community, highlighting the need for agility and speed in the standardisation process. New institutions are being built, and the need for financial support and strategic guidance from policymakers has been identified by active participants. Balancing speed with quality and inclusivity is essential for ensuring that the open source community can effectively participate in the standardisation process and contribute to the development of harmonised standards.

At a fundamental level, the driver of these activities is the new obligations introduced by the CRA. Before the CRA, software products, and by extension open source projects, their stewards, and developers, were not subject to horizontal cybersecurity requirements from EU legislation. This demands that the OSS ecosystem adapt, and part of this adaptation involves constructive engagement in standardisation. Some notable examples of OSS ecosystem actions include:

- The Eclipse Foundation has applied for liaison status with CEN-CENELEC to ensure the open source ecosystem's contribution to the European standardisation process.
- The Eclipse Foundation is also an ETSI member, strengthening links between open source communities and European standardisation.
- ETSI has signed a Memorandum of Understanding (MoU) with Linux Foundation Europe, supporting collaboration on software-related standardisation.
- Several national open source organisations have applied for memberships in NSOs (for example the OSBA joining DIN[1])
- OpenSSF and Linux Foundation Europe hosted a workshop titled "The Open Source Software Stewards and Manufacturers."[2]
- The Linux Foundation has created and launched a new free course called "Understanding the EU Cyber Resilience Act"[3]

1 Open Source Business Alliance. *Neues vom Cyber Resilience Act*. OSB Alliance, accessed 4 May 2025. Available at: https://osb-alliance.de/featured/neues-vom-cyber-resilience-act

2 Linux Foundation. *OpenSSF and LF Europe Launch Initiative to Help Open Source Projects Comply with EU Cyber Resilience Act*. Linux Foundation, published 17 October 2023. Available at: https://www.linuxfoundation.org/press/openssf-and-lf-europe-launch-cra-initiative

3 Linux Foundation. *Understanding the EU Cyber Resilience Act*. Linux Foundation Training, accessed 8 May 2025. Available at: https://training.linuxfoundation.org/express-learning/understanding-the-eu-cyber-resilience-act-cra-lfel1001/

- The Open Source Initiative (OSI)[4], Github[5], and OpenSSF[6] have published their considerations and compliance guidance.

Moreover, ETSI operates "software development groups" (SDGs), which provide dedicated structures for collaborative software development within a standards framework.[7]

In response to these new obligations and expectations, the Eclipse Foundation launched the Open Regulatory Compliance Working Group (ORC WG)[8]. The ORC aims to do something new within the open source community: it provides a platform for community members to collaborate, share best practices, and develop specifications that can be recognised by legislators through standardisation organisations. The initiative initially focuses on the European Cyber Resilience Act (CRA) but plans to expand to other global regulations. The ultimate deliverables include process specifications under liberal licences, aiming to create cohesive cybersecurity processes for regulatory compliance and provide a neutral space for technical discussions involving both industry and the open source community. Notably, the ORC WG is designed for a broad range of participants, including foundations, maintainers, vendors, users, and package managers. Participation aligns more closely with the terms and norms of open source rather than traditional standardisation.

Regarding the challenges for the OSS ecosystem in standardisation, the OSS ecosystem has historically not participated intensively in standardisation processes. There are several reasons for this lack of participation, with IPR policies and collaboration norms and processes playing important roles. A separate case study will look into these barriers, but for the CRA standardisation process, the Commission demands collaboration and facilitated participation.

The overarching concern from the OSS community is that unintended, negative consequences for the OSS innovation model may occur if ESOs and OSS communities do not collaborate successfully in the standardisation process. Since software regulation like the CRA will chiefly impact open source software (as the vast majority of software in existence is under open source licences), it is also hoped that the open source model can complement the standards development process initiated by the CRA. The goal is to offer different, more representative channels without compromising the speed and quality of the standards being developed.

The CRA impacts the full supply chain of software development. In the case of the open source supply chain, compliance will need to be brokered with the open source community, as the main requirements remain on the side of manufacturers who place the software on the market as part of a commercial activity. Thus, when assessing if an open source project is subject to all CRA requirements, developers will need to consider if such a project is made available on the market, i.e., if the project is intended 'for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge'.

The CRA demands that the Commission publish guidance to address the scope with a particular focus on remote data processing solutions and open source software. In their absence, legal uncertainty may prevent OSS communities from investing in and maintaining open source projects. Another unintended consequence may occur if ESOs and OSS communities do not collaborate in the standardisation process.

4 Open Source Initiative. (2024, December 10). *Standards and the Presumption of Conformity*. Open Source Initiative. Available at: https://opensource.org/blog/standards-and-the-presumption-of-conformity

5 GitHub. (2024, December 10). *What the EU's New Software Legislation Means for Developers*. GitHub Blog. Available at: https://github.blog/open-source/maintainers/what-the-eus-new-software-legislation-means-for-developers/

6 Open Source Security Foundation (OpenSSF). (2025). *EU Cyber Resilience Act (CRA)*. OpenSSF. Available at: https://openssf.org/public-policy/eu-cyber-resilience-act/

7 ETSI. (2023, February 2). *ETSI to Transform the Standards Development Landscape with Software Development Groups*. ETSI Newsroom. Available at: https://www.etsi.org/newsroom/press-releases/2184-etsi-to-transform-the-standards-development-landscape-with-software-development-groups

8 See Open Regulatory Compliance Working Group (ORCWG). *Open Regulatory Compliance Working Group*. Accessed 8 May 2025. Available at: https://orcwg.org/

In parallel, the ORC contributes to aligning open source activities with EU standardisation goals and identifying opportunities for collaboration between standardisation bodies and open source initiatives. However, it is the view within the OSS ecosystem that it needs more strategic support in terms of funding and guidance from policymakers at the EU and national levels. The CRA made a step in the right direction by including open source, but this needs to be accompanied by bolstering open source collaboration, governance, and integration with the EU's broader standardisation landscape. As it is not a traditional industry, this support needs to be designed differently.

Concretely, the CRA explicitly mentions the role of open source software stewards, who have lighter obligations than software manufacturers. These obligations include elaborating a cybersecurity policy, notifying cybersecurity authorities of any known exploited vulnerabilities, and promoting the sharing of information on discovered vulnerabilities with the open source community. Harmonised standards drafted by ESOs shall clarify from the technical perspective how to comply with these obligations.

3. Conclusion

This case study underscores the critical importance of successful collaboration between ESOs and the OSS ecosystem, emphasising the potential for collaboration and innovation between these stakeholders. As the CRA introduces new obligations and expectations, it is essential for the European Commission to remain vigilant to the experiences and challenges faced by the OSS community. The insights gained from these experiences should inform broader policy considerations, particularly as the Commission contemplates the redrafting of Regulation 1025/2012. Ensuring that the evolving regulatory framework supports both innovation and compliance, while providing financial support and strategic guidance to the open source community, will be key to fostering a resilient and inclusive digital market in Europe.

standICT.2026.eu

ICT Standardisation Observatory and Support Facility in Europe

Disclaimer

This case study has been developed for informational purposes only and does not represent any official position of the European Commission. It is part of a broader series of case studies launched under StandICT.eu to explore emerging challenges and developments in the ICT standardisation landscape. The series aims to stimulate critical reflection and discussion among stakeholders on topics of strategic relevance to the European and global standardisation ecosystem. The views expressed are those of the authors and interviewees and do not necessarily reflect the views of the European Commission, any SDOs or any affiliated organisation.

Funded by
the European Union