Open Regulatory Compliance

Contribution to the call for feedback of the CRA Guidance Package

2.11 | Submissions

Deliverable:	2.11
Category:	Submissions
Owner:	Cyber Resilience SIG
Status:	Shipped
License:	CC-BY-SA 4.0
Date:	June 2026

SIG: Cyber Resilience SIG Document type: Submission Number: "2.11" Status: Shipped Editors: Juan Rico Group: European Commission Date: 2026-02-03 Deadline: 2026-04-13 The discussion about the feedback that the ORC WG provided can be found here

The comments to the text can be found in .xlsx and .ods formats.

The introductory text provided in our response is presented below

On behalf of the Open Regulatory Compliance Working Group, we would like to express our gratitude for the opportunity to provide feedback on the draft guidance for the Cyber Resilience Act (CRA). We appreciate the significant effort and work the Commission has put into building this comprehensive document.

The following points summarise our group's primary areas of interest and proposed clarifications based on the draft guidance:

1. Definitions and clarifications for the FOSS ecosystem

- **Open Development:** The concept of "openly developed" requires more precise criteria, such as public issue trackers, open communication channels, and accessible version control histories for peer review.
- **Commercial Status and Donations:** We recommend interpreting "actual costs" to include fair remuneration for developers to prevent individual maintainers who rely on sponsorships from being inadvertently classified as commercial entities.

2. The role and obligations of open source software stewards

- **Defining Stewardship:** Stewardship should be recognised as a voluntary, fact-based role that begins when an entity undertakes systematic support (e.g., providing infrastructure or security staff) and ends when that support ceases.
- **Decentralised Governance:** If a foundation provides infrastructure but volunteers manage releases, the foundation should still be considered the steward, while the volunteer maintainers should remain exempt from personal CRA obligations.
- **Cumulative vs. Tiered Obligations:** When multiple entities support a single project, they should only be responsible for the specific "layer" of support they provide (e.g., infrastructure vs. engineering).

3. Vulnerability handling and reporting

- **Becoming Aware:** For stewards, the 24-hour reporting clock should only trigger upon confirmation of technical applicability and actual exploitation, allowing for a reasonable initial assessment period.
- **Coordinated Vulnerability Disclosure (CVD):** Reporting to regulators should follow CVD practices to allow a "silent period" for developing fixes, thereby avoiding the creation of zero-day risks.
- **Upstream coordination:** Manufacturers should verify if a vulnerability is already known upstream

before filing reports to avoid overwhelming maintainers with duplicate notifications.

4. Maintenance and Substantial Modification

- **Agile security models:** Minor patches, bug fixes, and performance optimisations should not be considered "substantial modifications" provided the product's intended purpose and risk profile remain unchanged.
- **Security vs. Functional updates:** Guidance should explicitly clarify that manufacturers can charge for new features but must provide security updates free of charge for the duration of the support period.

5. Operational and technical clarifications

- **Remote Data Processing Solutions (RDPS):** We request a clear statement that services falling under the scope of NIS2 are not subject to the CRA and that public package repositories (e.g., PyPI, Maven) are excluded from the definition of RDPS.
- **Risk Assessments:** To ensure scalability, manufacturers should be permitted to fulfil risk assessment obligations for product families by documenting the security-by-design processes of a common codebase.

We remain at your disposal for any further clarifications or discussions regarding these points.

Sincerely,

The Open Regulatory Compliance Working Group