Open Regulatory Compliance Working Group Steering Committee Meeting

Steering Committee | Minutes

Deliverable:	2026-03-19
Category:	Meeting Minutes
Owner:	Steering Committee
Status:	Yes Approved
License:	CC-BY-SA 4.0
Date:	2026-03-19

Open Regulatory Compliance Working Group Steering Committee Meeting

###

19 March, 2026

Agenda Topics	Moderator	Minutes
Approval of the minutes of the previous ORC Steering Committee call	Juan	5
ORC Status Update	Juan	10
CRA Expert Group	Juan	15
Cyber Security Act call for feedback ORC role	Juan	5
Attestations joint statement and ORC public positioning	Juan & Shanda	15
AOB	All	5

Quorum - 50% of Representatives / >50% of Quorum Present for simple majority vote Quorum is 4 with 3 votes affirmative for simple majority

ATTENDEES

Steering Committee Members

- No Nokia: Timo Perala (Primary)
- No Huawei: Adrian O'Sullivan (Primary)
- No Red Hat: Roman Zhukov (Primary), Dave Russo (Alternate)
- [ ] Victor Roland, OBEO (Elected Participant)
- No Dirk-Willem van Gulik, Apache Software Foundation (Elected Foundation)
- No Olle E. Johansson, OWASP Foundation (Elected Foundation)

Eclipse Foundation Staff

- [ ] Sharon Corbett
- No Juan Rico
- No Shanda Giacomoni
- [ ] Ciarán O'Riordan

MINUTES

Meeting Chair: Timo Perälä

Quorum:

Quorum reached at 16:02

Notes:

Approval of the minutes of the previous ORC Steering Committee call

Mark them as approved and upload to the public repository.

ORC Status Update

- Membership: we are in 63 members, the first quarter the strategy has been focus on those prospects that will bring revenue to the WG, but we will combine with the participation of other potential members that helps to increase the diversity.
- Operations: The due diligence activity is running and progressing, the attestation work was presented at the CRA Expert Group on March 4th, and we have already started the work on the CRA guidance package released by the European Commission.
- Institutional engagement: good engagement with the EC CRA team. We are also planning a meeting with ENISA SBOM representatives before the end of the month. And we need to progress with the engagement of MSA.
- Events and communication: Good feedback from Embedded world, and now looking forward to Open Community for Compliance at OCX. The training materials will be released and tested in April.

The attestation presentation given to the CRA Expert Group was generally well-received, with no immediate pushback, only minor requests for clarification. This lack of initial challenge, however, presents a risk, as opposition might emerge later in the process when it is harder for us to adapt. A separate point

of discussion was the critical role of transitive dependencies, which the CRA Expert Group currently seems to misunderstand.

We should proactively engage with national member state bodies like Market Surveillance Authorities (MSAs). Building on the 2025 idea of "Friends of ESOs," we propose updating the concept to "Friends of MSAs" for 2026. We already have initial contacts in Sweden and Finland. A strategy combining a global approach with individual contacts is needed to define how we will support these MSAs.

CRA Expert Group meeting

- Slides 5 and 6 include the main points discussed during the Expert Group.
- Important aspect to consider with the presentation and the new guidance is the evolution of the role of stewards.
- The single reporting platform does not fit the reality of decentralised organizations in which hundreds of people can report vulnerabilities.
- The discussion to define the feedback is done in the ORCGithub - there will be a sub-issue per topic reported to the shared document.
- The objective is to have this conversation in the open and leave it accessible so those who want to replicate the feedback, entirely or partially can easily do it.

Cyber Security Act

- It was presented the opportunity to submit feedback to the CSA Call for feedback.
- Starting point will be the feedback submitted to the call for evidence in 2025. It will be compared to the current text and use that as the element for initiating the discussions.
- Deadline is May 11th.
- The work will be presented in the next SIG meeting to enable the whole community to participate.

Joint Statement

- The idea behind creating the joint statement and other public statements is not to explain the details of the work, but to create high level assets, easy to digest and to share to present the work we are doing in different areas.
- In this particular case (attestations), there is only 1 pending to address comment that will be process in the coming days and share the final version with the SC and later with the WG.
- Next item to communicate similarly could be our work on due diligence.

AOB

Code and Compliance

Planning for the Code and Compliance event next fall has begun. During the meeting, the steering committee discussed identified alternatives, ranging from a standalone event in Brussels to a co-located format. Following the discussion, all steering committee members were asked to submit proposals for co-locating the event.

Adjournment

The meeting was closed at 17:03

Resolutions

None

Supporting materials

2026-03-19-orcwg-sc-presentation.pdf (attached below)

Next Meeting

Next meeting will happen on April 16th - 16.00 CEST - 14.00 UTC

Open
Regulatory
Compliance

ORC Steering Committee meeting

2026-03-19

Agenda

Agenda Topics	Moderator	Minutes
Approval of the minutes of the previous ORC Steering Committee call	Juan	5
ORC Status Update	Juan	10
CRA Expert Group	Juan	15
Cyber Security Act call for feedback ORC role	Juan	5
Attestations joint statement and ORC public positioning	Juan & Shanda	15
AOB	All	5

ORC WG Situation as of 2026.02.12

Membership

63 Members

- **No new members, but focused on paying members**

Operations

- **Due diligence workstream running.**
- **Attestation project evolving properly and good feedback from the presentation at the Expert Group meeting.**
- **Guidance released.**

Institutional engagement

- **Engage with the new EC team going well.**
- **Meeting planned on SBOMs before the end of the month.**
- **MSA engagement in progress.**

Events and communication

- **Embedded world**
- **Open Community for Compliance**
- **Training.**

Expert Group Agenda

	Agenda Item	Notes
	Welcome coffee and communications check	
1.	**Welcome and administrative issues**	
1.1	Adoption of the draft agenda	
1.2	Update by the Commission on the implementation of the CRA	
2.	**Commission guidance on the CRA**	
2.1	Presentation by the Commission of the content of the draft Communication & next steps	
2.2	Preliminary exchange of views	
	Coffee break	
3.	**Voluntary attestations for FOSS and due diligence**	
3.1	Presentation by Null Point Studio on the voluntary attestations study	Github of the voluntary attestations study
3.2	Exchange of views	
	Lunch break	
4.	**SBOMs**	
4.1	Presentation by ENISA	Call for Feedback: Advancing Software Supply Chain Security together! | ENISA
5.	**Notification of conformity assessment bodies**	
5.1	Presentation by the Commission	
	Coffee break	
6.	**Support for MSMEs**	
6.1	Presentation by the Commission and ENISA	ENISA CRA SMEs Survey
6.2	Exchange of views	
7.	**Single Reporting Platform**	
7.1	Presentation by ENISA	
8.	**Conclusions**	
8.1	Next steps	
8.2	AOB	

CRA EG main outcomes

1. CRA Implementation Process & Commission Guidance

- An implementing act defining **product categories** was published on December 25.
- **Industry Role:** Commission stressed the need for industry involvement in standards development.
- **Harmonisation:** Confirmed that CRA and NIS2 serious incident reporting are considered equivalent, and they may plan an implementing act on **Software Bills of Materials (SBOMs)**.
- **Scope:** Clarified as "placement on the market of software 'per version'." Source code as educational material is out of scope.
- **FOSS Exemption:** Requires source code to be **publicly available** (“distributed openly”). Mere licensing or paywall access is insufficient.
- **Support:** Discontinuing CRA-mandated support for previous versions is only allowed if the upgrade is available without cost (including dependencies).
- **Substantial Modifications:** Stressed the link between substantial modifications and the need for a new risk assessment.

2. Open Dialogue: Ambiguous Points

- **FOSS Development:** Question on whether FOSS must be “openly developed” (in addition to "openly shared") **remained unanswered**.
- **Steward Status:** Commission stated that being a steward “**is not a choice**.” Clarity is lacking on whether a steward is considered an "economic operator."
- **Monetisation:** More clarity requested on the terms “support,” “technical assistance,” and “support services.”

CRA EG main outcomes

3. SBOMs & Voluntary Attestations

- **SBOM Status:** Survey showed **72% of respondents** already producing SBOMs, mainly using CycloneDX and SPDX.
- **Risk Concern:** Denmark raised concern about the Commission's need to perform a risk assessment on what to include in an SBOM due to potential dangers.
- **Voluntary Attestations:** A proposal for **Tiered Indicators** was introduced, including "Lite" (self-attestation), "Medium" (extra verification with CAB/NB), and "Heavy" (CRA-style risk assessments).

4. Conformity Assessment Bodies (CABs)

- **Capacity Concerns:** Significant waitlist issues noted (similar to MDD/MDR and NIS2/DORA work), despite the Commission's belief in market capacity.
- **Fast-Track:** Commission is exploring a fast-track procedure using existing RED bodies and EUCC CABs, raising concerns about standardisation of judgment levels.
- **Standards:** Harmonised sectoral standards for cybersecurity/CRA do not yet exist, and national standards will need to be complemented.

5. Single Reporting Platform

- **Go-live Date:** Scheduled to **Go-live on September 11, 2026**.
- **Authentication:** Initial manufacturer verification will be handled by CSIRTs via phone/email; long-term plan is eIDAS integration. Reports pending verification will be labelled "unverified."
- **API Focus:** API development is focused on CSIRTs/national bodies, not for end-users.

6. Support for MSMEs

- **ENISA Work:** ENISA is developing a survey, a Cyber Resilience Maturity Assessment Model, and a study on CRA investments.
- **Industry Feedback:** Pushback was noted against making the compliance process easier for SMEs.

CRA Guidance Package

- The new doc is pretty solid.
- Most of our contributions to the previous version are now part of the current document.
- We are coordinating internally feedback to be submitted as ORC.
- We encourage all members to provide their own views.

Commission publishes for feedback draft guidance to assist companies in applying the Cyber Resilience Act

The European Commission has published for feedback draft guidance to assist companies in meeting the obligations of the Cyber Resilience Act (CRA).

The draft guidance clarifies the obligations and the scope of the rules with a particular focus on facilitating compliance by microenterprises and small and medium-sized enterprises.

Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy, said:

> With today's guidelines, the Commission supports the effective application of the Cyber Resilience Act. From baby monitors to smart watches, digital elements are part of our daily lives, and we will make sure all digital products on the EU market are safe from cyber threats.

The draft guidance focuses on remote data processing solutions and free and open-source software, the notion of 'support periods' as well as the interplay between the CRA and other EU legislation.

As part of the broader simplification exercise, the Commission is consulting stakeholders until 31 March to ensure alignment with implementation efforts, practical challenges, and market realities.

The CRA entered into force on 10 December 2024. The main obligations introduced by the Act will apply from 11 December 2027, with reporting obligations to apply as of 11 September 2026.

The Commission is actively working to strengthen the EU's cybersecurity resilience and capabilities. A new cybersecurity package was proposed on 20 January 2026.

AdobeStock © ipopba

See also

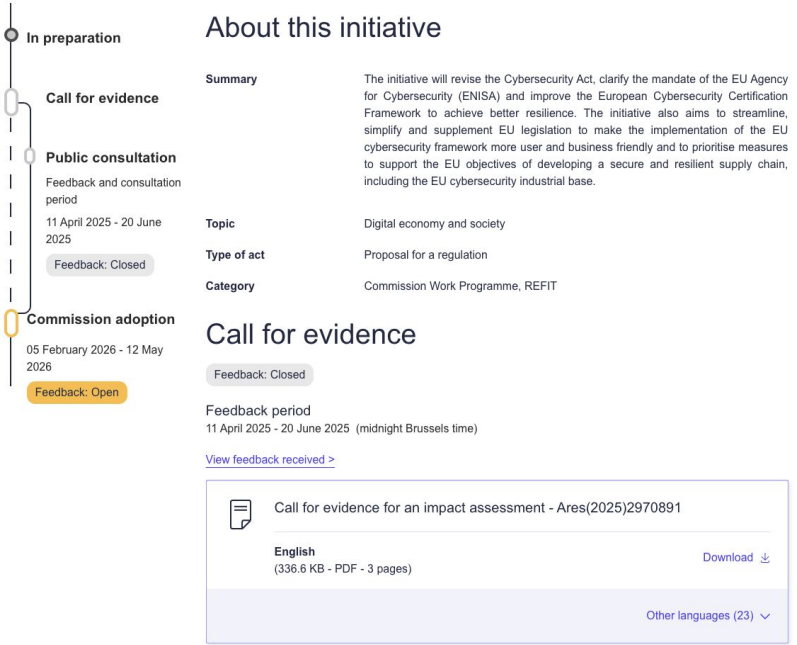
More on the Cyber Resilience Act

Related topics

Cybersecurity

Cyber Security Act

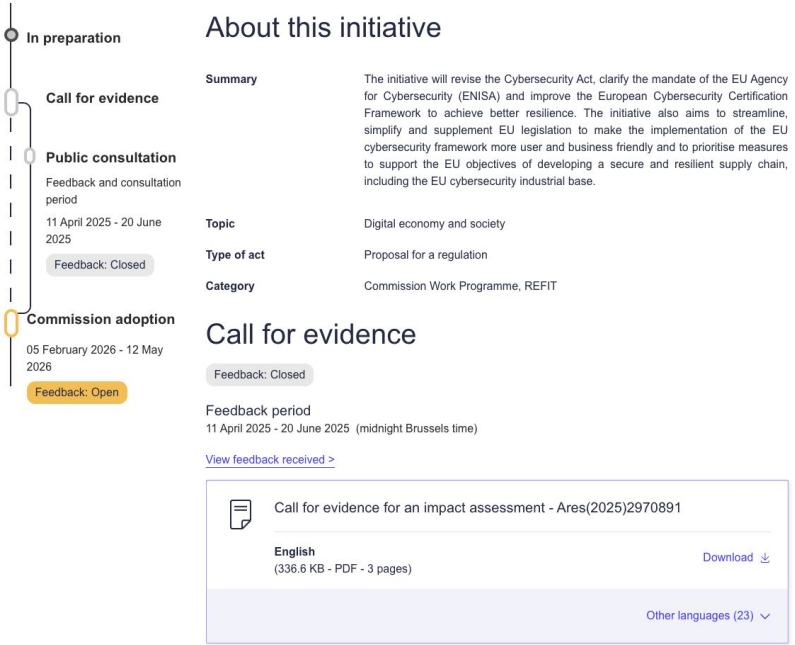
- Cyber Security Act text here
- ENISA’s role
- Cybersecurity scheme.



Cyber Security Act

- Cyber Security Act text here
- ENISA’s role
- Cybersecurity scheme.

Shall we react as ORC to it?



Joint Statement and positioning

- What do we think about the current version?
- Should we do more of this?
- Community development + Steering Committee approval looks reasonable?

Joint Statement: Strengthening Open Source Sustainability via Article 25 of the EU Cyber Resilience Act

Our Core Position

> *We believe the voluntary attestation framework, described in Article 25 of the CRA, offers a transformative opportunity to strengthen open source sustainability. By creating a mechanism to standardise and formally recognise security information provided by open source projects, the overall compliance burden can be reduced and projects can become more attractive to manufacturers by making it easier to carry out their due diligence obligations. We believe Article 25 can enable sustainable long-term funding, and bolster community-led self-governance of open source projects, improving cybersecurity across the European market, and lowering the compliance burden that the CRA would otherwise impose on small and medium enterprises.*

The four pillars of our proposed Article 25 Framework

1. Facilitating efficient Due Diligence via trusted artefacts. The CRA requires manufacturers to perform due diligence on every integrated component, including free and open source components. We support the development of interoperable, open standards for attestation artefacts that can eliminate the "denial-of-service attack" on maintainers caused by duplicative compliance requests and provide manufacturers with consistent, trustworthy information they can integrate into their risk assessments, and that can also be accessible by the Market Surveillance Authorities.

Code & Compliance - Fall 2026

Comply.Land	Community over Code	Standalone	NSSS
Date TBC	October 11-14	Sept or October	November 4-5
Malta	Glasgow	Brussels	Stockholm

Considerations:

- Date - planning timeline, conflicting events, FOSDEM in 2027
- Ease of travel
- Cost of venue and accommodations