



Open Regulatory Compliance

**Navigating Regulatory Complexity Through Open Source
Collaboration**

Francisco Carneiro

About me

Francisco Carneiro

Ecosystem Development at the Eclipse
Foundation

Let's Connect on LinkedIn:



One vehicle. Multiple regulatory layers.



UN R155 / R156

Cybersecurity & OTA
Vehicle level

Fully active since July 2024
for all newly registered
vehicles.

Cyber Resilience Act

Product cybersecurity
Connected ecosystem

Vulnerability reporting begins
Sept 2026; full application by
Dec 2027.

EU AI Act

AI safety & risk
AI systems

High-risk automotive
provisions become fully
applicable in August 2027.

GDPR & DATA ACT

Data & privacy
Vehicle data.

Active

Cybersecurity is no longer a one-time approval



THEN

Vehicle-Level Type Approval

- Point-in-time approval
- Vehicle boundary
- Checklist-driven

NOW

Systemic & AI Resilience

- Continuous lifecycle
- Software & AI supply chain
- Evidence-driven compliance

Compliance risk comes in four forms

Pillar 1

Substantive Obligations

(Safety & Security)

Meet the Requirements

Cyber Security Management System ·
Secure-by-default
· AI risk mitigation

Pillar 2

Evidentiary Obligations

(Transparency)

Prove you did it

SBOMs · Logs ·
Technical documentation

Pillar 3

Governance Obligations

(Accountability)

Know who is responsible

OEM · Tier 1 ·
Provider · Deployer

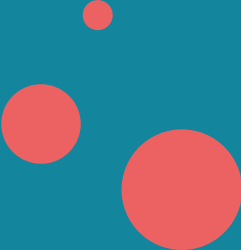
Pillar 4

Enforcement & Remediation

(Liability)

If you fail?

Fines · Withdrawal ·
Claims



**Regulation tells us -*what*-
The challenge is -*how*-**

"Open Source" does not mean the same thing everywhere

Cyber Resilience Act (CRA)

Ecosystem + Governance

- Open development model
- Collaborative distribution
- Recognises **Open Source Stewards**

EU AI Act

Artifact + License

- Licensing conditions
- Rights to use, modify & distribute
- More artifact-centric approach

Same open source software. Different regulatory treatment: Your existing quotes, recital references and explanation become what **you say**, not what they read. The current slide already makes this distinction, but buries it under legal text.

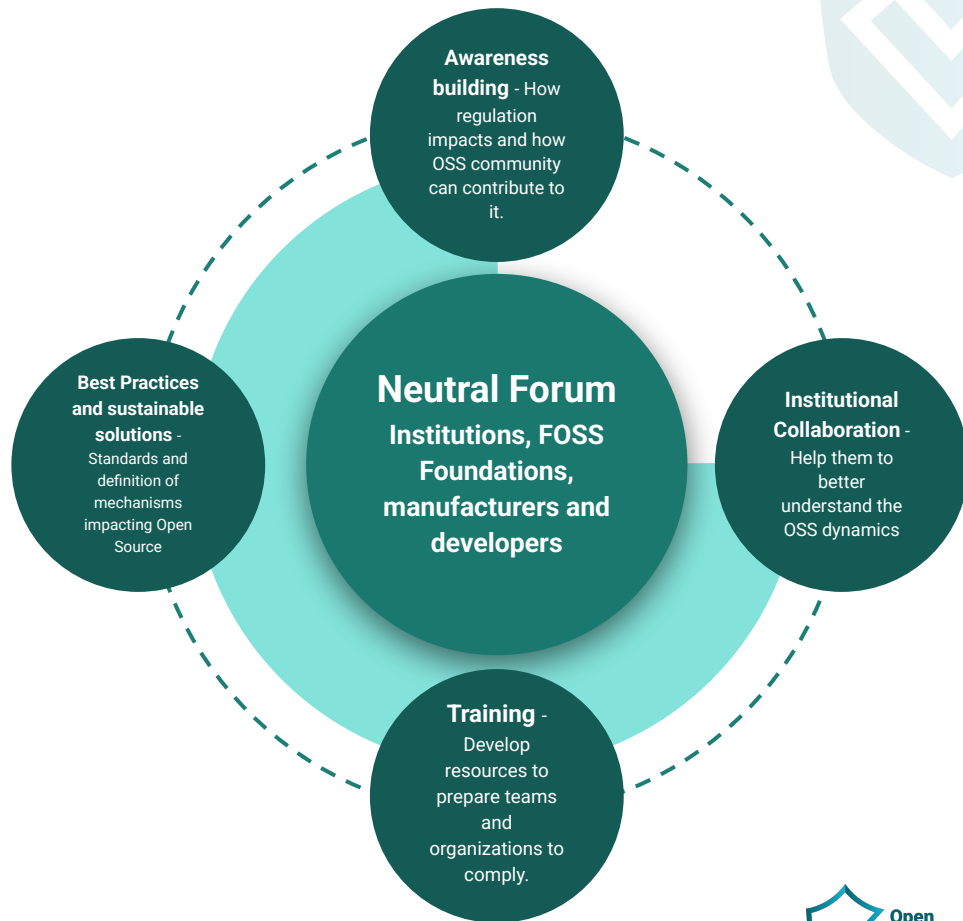


**Open
Regulatory
Compliance**

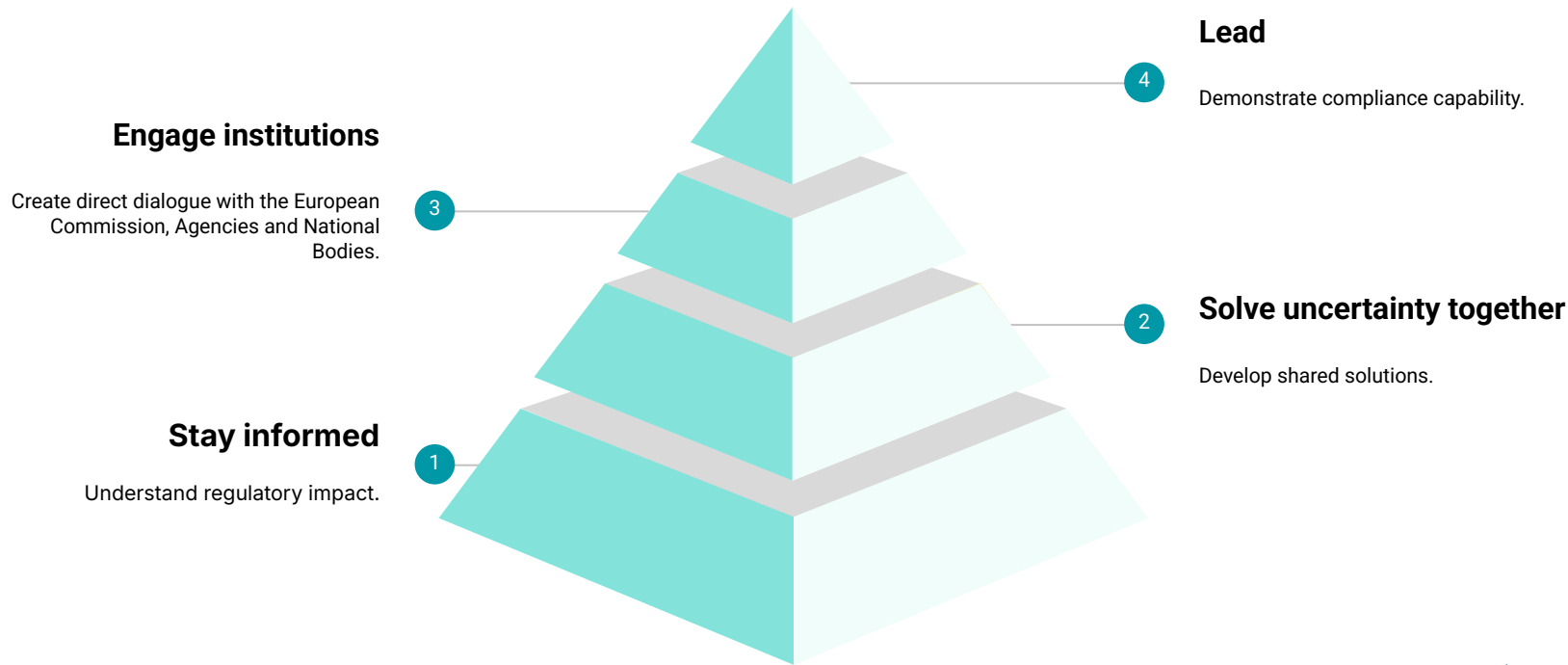
Software is regulated

Non-Compliance is costly

*We turn regulation into practical,
shared compliance.*



How ORC helps its members



Current activities and success cases

Cyber resilience Act

- Over 50 text comments included and 10+ examples to the current guidance process.
- Definition of attestations according to the article 25 as a community effort.
- Product definition, including a proposal to properly address open hardware.
- Training materials for understanding the CRA.

AI Act

- Contribution to the interplay between the CRA and AI Act, focusing mainly on how the different approaches to open source doesn't help to its implementation.

Other activities

- Consultations - from 1025 reflecting our standardisation concerns to CSAv2.

ORC Members

Strategic Members



Participant Members



Foundation Members



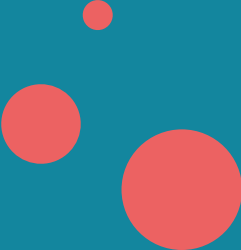
Guest Members



{code & compliance}

Bridging the Regulatory Gap

27 October 2026 | Maison de la Poste | Brussels, Belgium



Thank you!

Questions?



Join our GitHub
www.github.com/orcwg



Follow us on LinkedIn
@Open Regulatory Compliance



orcwg.org/resources/videos/



[@orcwg.org](https://twitter.com/orcwg.org)



@orcwg@fosstodon.org