Open
Regulatory
Compliance

# ORC WG Workshop

## January 30, 2025 - Brussels

# Agenda

| Rooms | Lobby | Room 8 | Room 3 | Room 7 |
|---|---|---|---|---|
| Room capacity | | 80 people (50 in the afternoon) | 20 people | 28 people |
| 9:00 | Registration | | | |
| 10:00 | | Introductory presentations | | |
| 10:45 | | Workshop: FAQ | Workshop: FAQ / Inventory | Workshop: Deliverables Plan |
| 12:00 | | Fireside chat with Filipe Jones Mourão, EU Commission | | |
| 13:15 | Lunch | | | |
| 14:15 | | Workshop: FAQ | Workshop: FAQ / Inventory | Workshop: Deliverables Plan |
| 16:10 | | CRA Compliance Guide for Open Source Industry Players | Vulnerability Handling Specification | |
| 16:45 | | Wrap up & next steps | | |
| 16:50 | | Closing Comments | | |


The CRA is here! Now what?

# The CRA is here! Now what?

1. **CRA Fundamentals:** *Why? Who? What? How? When?*
2. **CRA innovation: *full* supply chain compliance**
3. **How ORC WG steps in**

# CRA fundamentals

# The “*Why*”

**In the European Commission’s own words***

*“Hardware and software products are increasingly subject to successful **cyberattacks**, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.”*

*Source: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

# CRA fundamentals

# The "*Why*"

**In the European Commission's own words***

*"From baby-monitors to smart-watches, products and software that contain a digital component are **omnipresent in our daily lives**. Less apparent to many users is the **security risk** such products and software may present."*

*Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

## CRA fundamentals

# The “*Why*”

**In the European Commission’s own words***

*“The Cyber Resilience Act (CRA) aims to **safeguard consumers and businesses** buying or using products or software with a digital component.”*

*Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

## CRA fundamentals

# The “*Why*”

**In the European Commission’s own words***

*“The Act would see **inadequate security features become a thing of the past** with the introduction of mandatory cybersecurity requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle.”*

*Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

# CRA fundamentals

# The "*Why*"

**In the European Commission's own words***

*"The Act would see inadequate security features become a thing of the past with the introduction of mandatory cybersecurity requirements for **manufacturers and retailers** of such products, with this protection extending throughout the product lifecycle."*

The "Who"

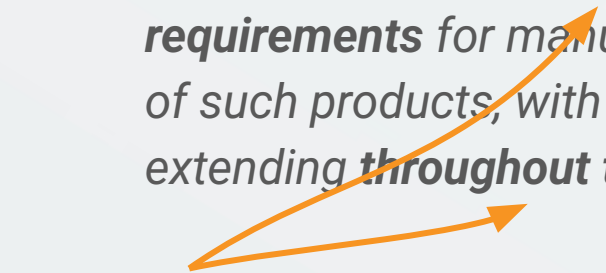
*Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

## CRA fundamentals

# The "*Why*"

**In the European Commission's own words***

*"The Act would see inadequate security features become a thing of the past with the introduction of **mandatory cybersecurity requirements** for manufacturers and retailers of such products, with this protection extending **throughout the product lifecycle**."*




*Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

## CRA fundamentals

# The “*Who*”

**“Manufacturers”**
Anyone “placing a product” on the European market.

**“Open Source Stewards”**
Essentially code-hosting foundations.
For-profits can be stewards too if they’re *not monetizing* the project.

**Open Source maintainers**
“Hobbyist” projects aren’t in scope, but any widely adopted project will be *indirectly* impacted.

# CRA fundamentals

# The “*What*”

**Manufacturers**

Cybersecurity risk assessment.

Cybersecurity requirements governing planning, design, development and maintenance **across supply chain** and **throughout product lifecycle**.

Vulnerability management, reporting, and upstreaming of fixes.

Etc.

*Perform due diligence of open source dependencies!*

## CRA fundamentals

# The “*What*”

**Open Source Stewards** *(light-touch regime)*
Cybersecurity policy.
Vulnerability handling.

**Both**
Additional requirements for *important* and *critical* products.

Cooperation with market surveillance authorities.

## CRA fundamentals

# The “*How*”

**“Harmonized standards”**

44(!) standards requested to the European Standards Organisations (ESOs). Provide *presumption of conformity*.

**Additional “Implementing Acts”**

E.g. to set up an attestation program

**Best practices**

Formalized best practices help manufacturers perform due diligence

## CRA fundamentals

# The “*When*”

**CRA**

Entry into force: November 11, 2024

Vulnerability reporting: September 11, 2026

All other obligations: December 11, 2027

**Harmonized standards**

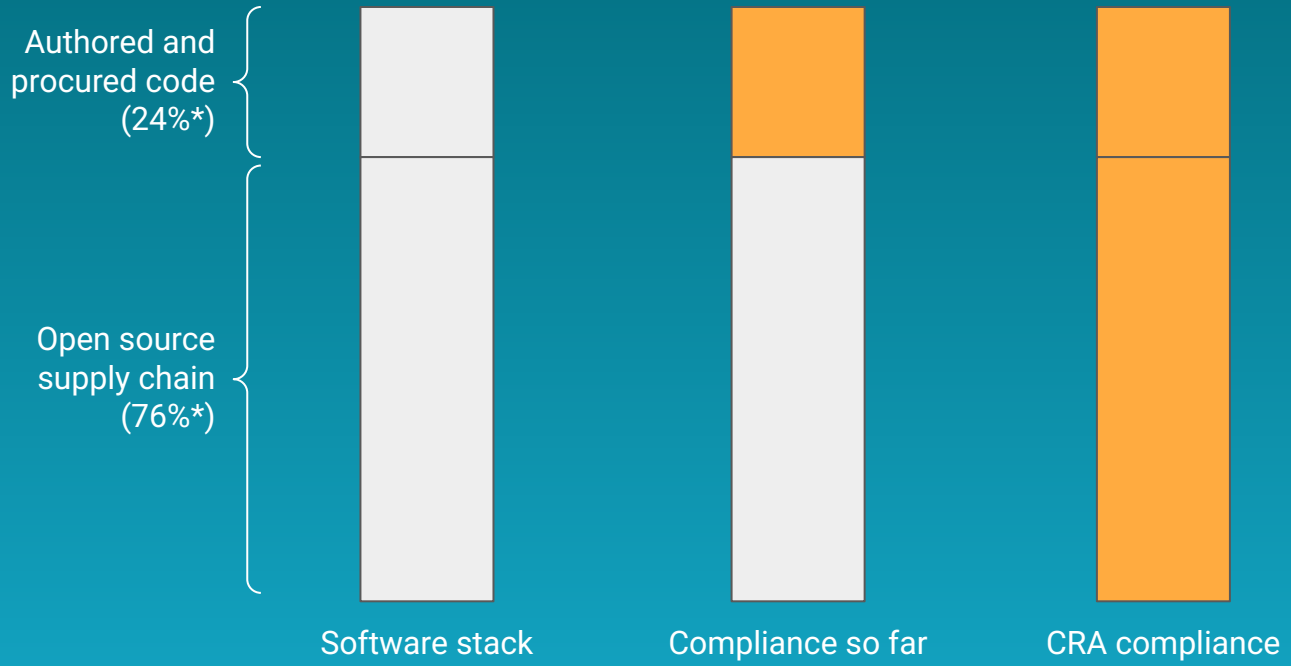
Horizontal (type A): August 30, 2026

Vertical (type C): October 30, 2026

Horizontal (type B): October 30, 2027

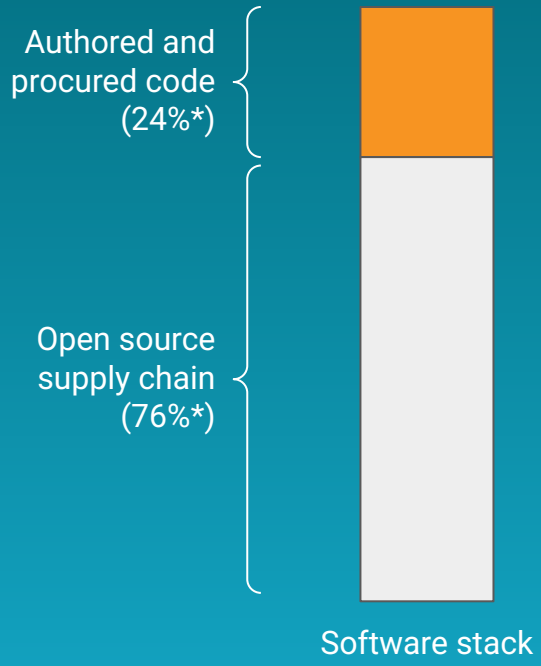
*“We know how to do compliance already. How is this different?”*

# CRA innovation: full supply chain compliance




* Source: Synopsis OSSRA Report 2023

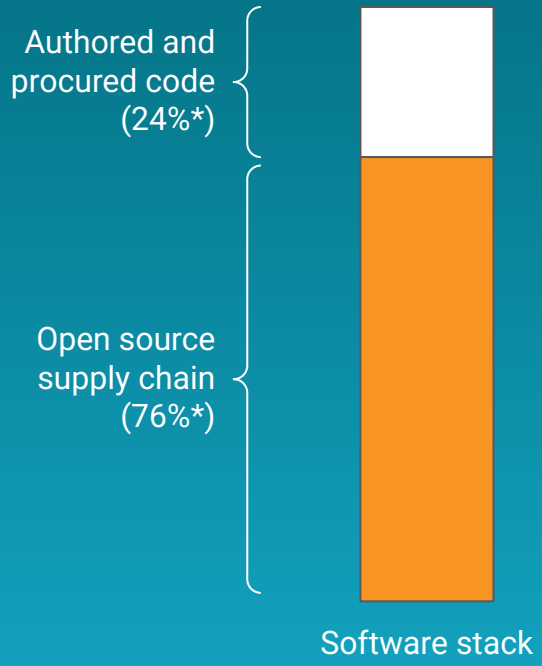
# Impact of full supply chain compliance




**Authored and procured code**
Compliance is managed through internal practices and vendor agreements.

* Source: Synopsis OSSRA Report 2023

# Impact of full supply chain compliance

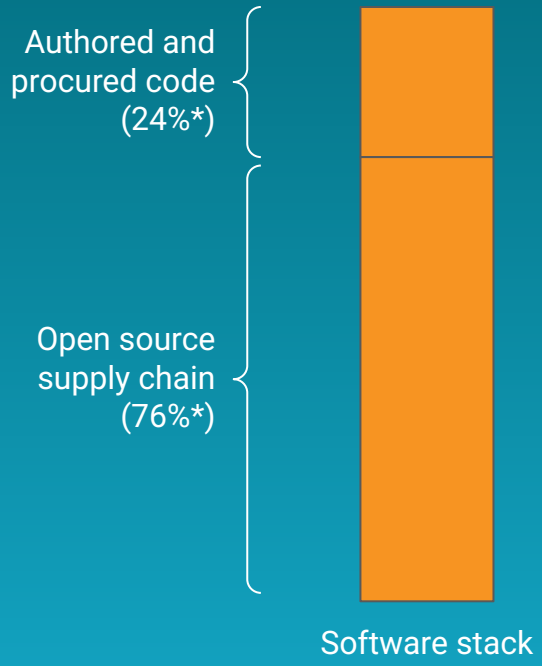



**Open source supply chain**
Compliance has to be **brokered** with open source community. Compliance requirements stay with manufacturers.

This is new!

* Source: Synopsis OSSRA Report 2023

# Impact of full supply chain compliance




**Authored and procured code**
Compliance is managed through internal practices and vendor agreements.

**Open source supply chain**
Compliance has to be **brokered** with open source community. Compliance requirements stay with manufacturers.

This is where ORC WG steps in

* Source: Synopsis OSSRA Report 2023

Open
Regulatory
Compliance

# ORC WG

**Neutral forum where community and industry can work out supply chain compliance together**

# ORG WG focus

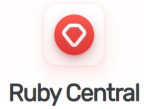
**Education & Thought Leadership**
Close the knowledge gap!

**Technical Development**
Formalize best practices into specifications.
Channel community and industry input to formal standardization bodies.

**Institutional Engagement**
Coordinate community and industry collaboration with the institutions.

**Representation**
The more we are, the stronger our voice is!

# Open Regulatory Compliance Working Group Members



# WORKSHOPS

FAQs

Inventory of relevant resources

Deliverables Plan

# Agenda

| Rooms | Lobby | Room 8 | Room 3 | Room 7 |
|---|---|---|---|---|
| Room capacity | | 80 people (50 in the afternoon) | 20 people | 28 people |
| 9:00 | Registration | | | |
| 10:00 | | Introductory presentations | | |
| 10:45 | | Workshop: FAQ | Workshop: FAQ / Inventory | Workshop: Deliverables Plan |
| 12:00 | | Fireside chat with Filipe Jones Mourão, EU Commission | | |
| 13:15 | Lunch | | | |
| 14:15 | | Workshop: FAQ | Workshop: FAQ / Inventory | Workshop: Deliverables Plan |
| 16:10 | | CRA Compliance Guide for Open Source Industry Players | Vulnerability Handling Specification | |
| 16:45 | | Wrap up & next steps | | |
| 16:50 | | Closing Comments | | |

# Fireside Chat

# Fireside Chat

**Tobie Langel**
Technical Lead ORC WG
Eclipse Foundation

**Lucía Lanfri**
Project Manager
CEN and CENELEC

**Filipe Jones Mourão**
Policy Officer
DG CNECT, European Commission

# Closing Comments

**Dirk-Willem van Gulik**
VP of Public Policy
Apache Software Foundation

**Timo Perala**
Head of Software & Internet Standardisation
Nokia Networks

# Open Regulatory Compliance

# *Join us!*

**https://orcwg.org/**

Open
Regulatory
Compliance

# The CRA is Here! Now What?

## January 29, 2025 - Brussels

# Thank you!