

**The CRA has landed. Now what?**

# Agenda

1. CRA Fundamentals
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”*

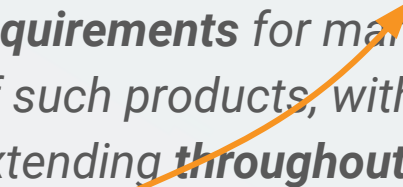
\*Source: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

# 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**.”*



*The “What”*

\*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

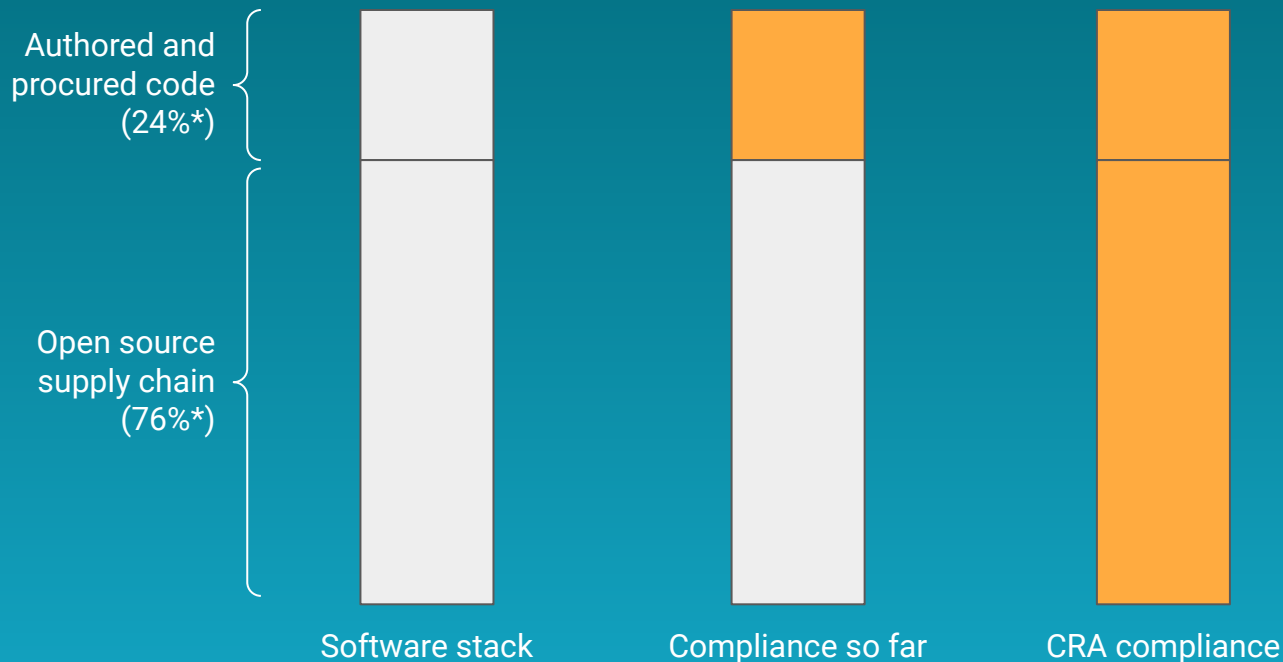
Horizontal (type B): October 30, 2027





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

# CRA innovation: full supply chain compliance



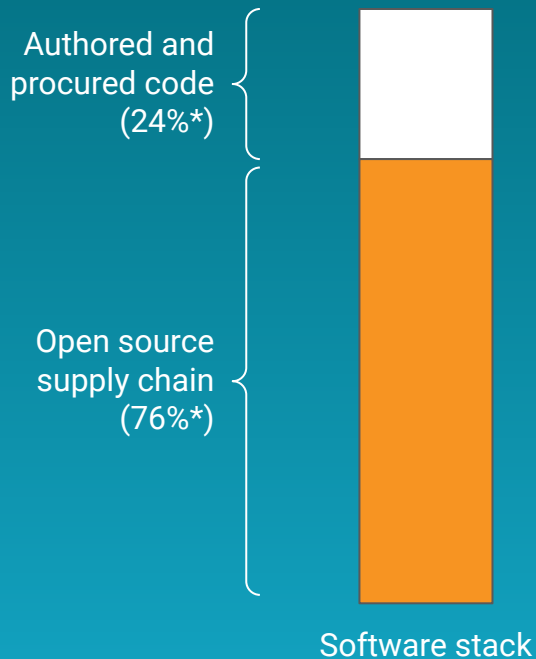
\* Source: Synopsis OSSRA Report 2023

# Impact of full supply chain compliance



\* Source: Synopsis OSSRA Report 2023

# Impact of full supply chain compliance



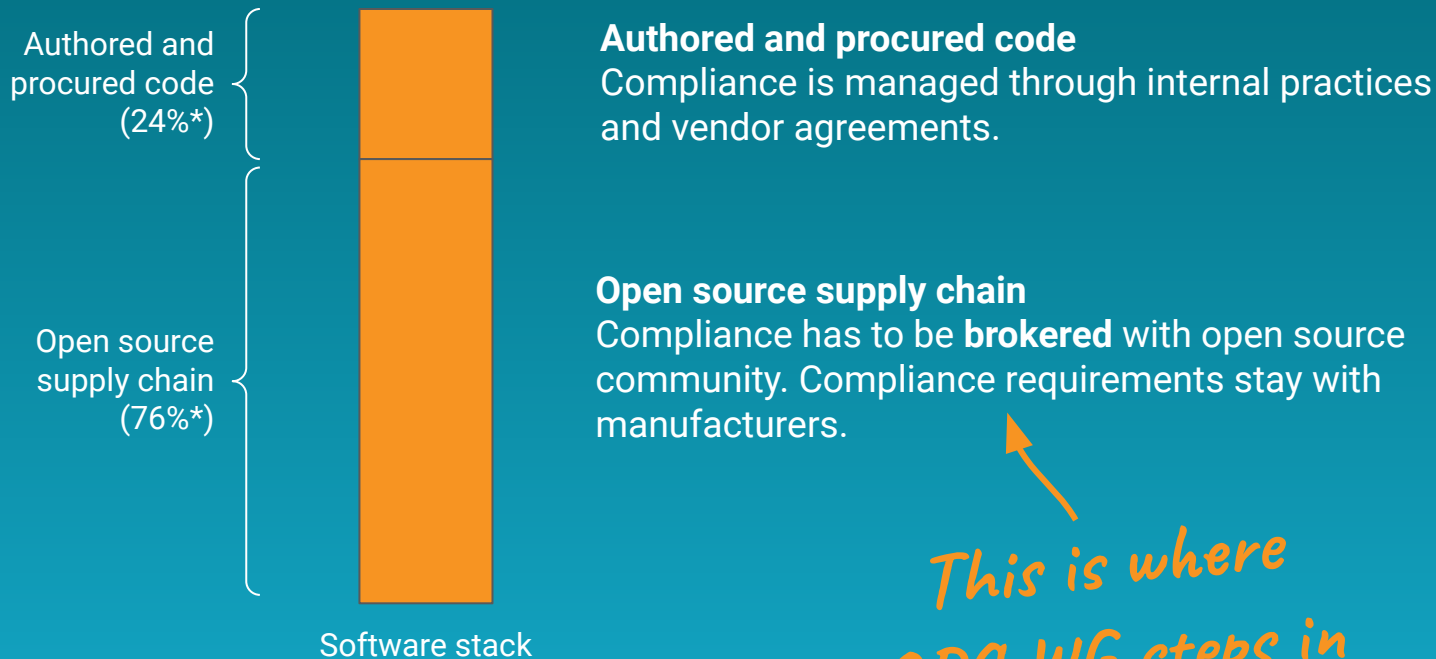
## Open source supply chain

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



\* Source: Synopsis OSSRA Report 2023





**Open  
Regulatory  
Compliance**

## **ORC WG**

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

# ORC WG (draft) Mission

*The mission of the ORC WG is to serve as a neutral forum for the open source community, maintainers, industry, small and medium enterprise (SME), research, open source foundations and related nonprofits to come together to understand and develop a point of view on emerging regulation, inform the broader ecosystem of its impact and collect its feedback, propose solutions leading to a sustainable and thriving open source ecosystem, develop educational material to inform and help with the implementation of regulation, develop specifications that formalize best practices, and collaborate with institutions by providing inputs to regulatory processes and participating in formal standardization efforts.*

# 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!

# ORC WG Members

AboutCode



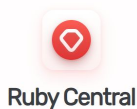
CYBERISMO!



Mercedes-Benz  
Tech Innovation



NOKIA



SIEMENS





**Open  
Regulatory  
Compliance**

***Join us!***



**<https://orcwg.org/>**



# Thank you!