
The CRA is here.
Let’s build bridges!


The CRA is here. Now what!?


The CRA is here.
Let’s build bridges!

Agenda

1. **CRA Fundamentals:** *Why? Who? What? How? When?*
2. **CRA innovation: *full* supply chain compliance**
3. **The Steward as bridge builder…**
4. **…security attestations as bridge**
5. **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"

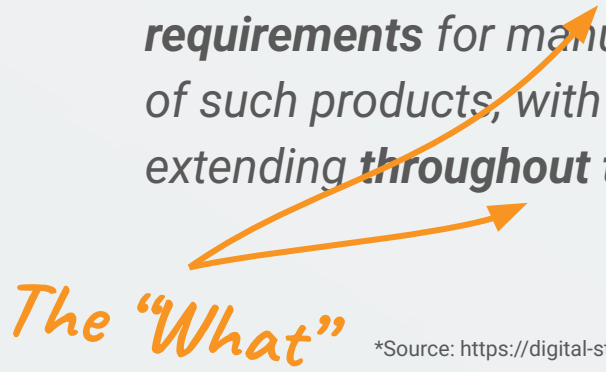
*Source: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

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 software 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 software 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

41(!) 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: December 11, 2024

Vulnerability reporting: September 11, 2026

All other obligations: December 11, 2027

Harmonized standards

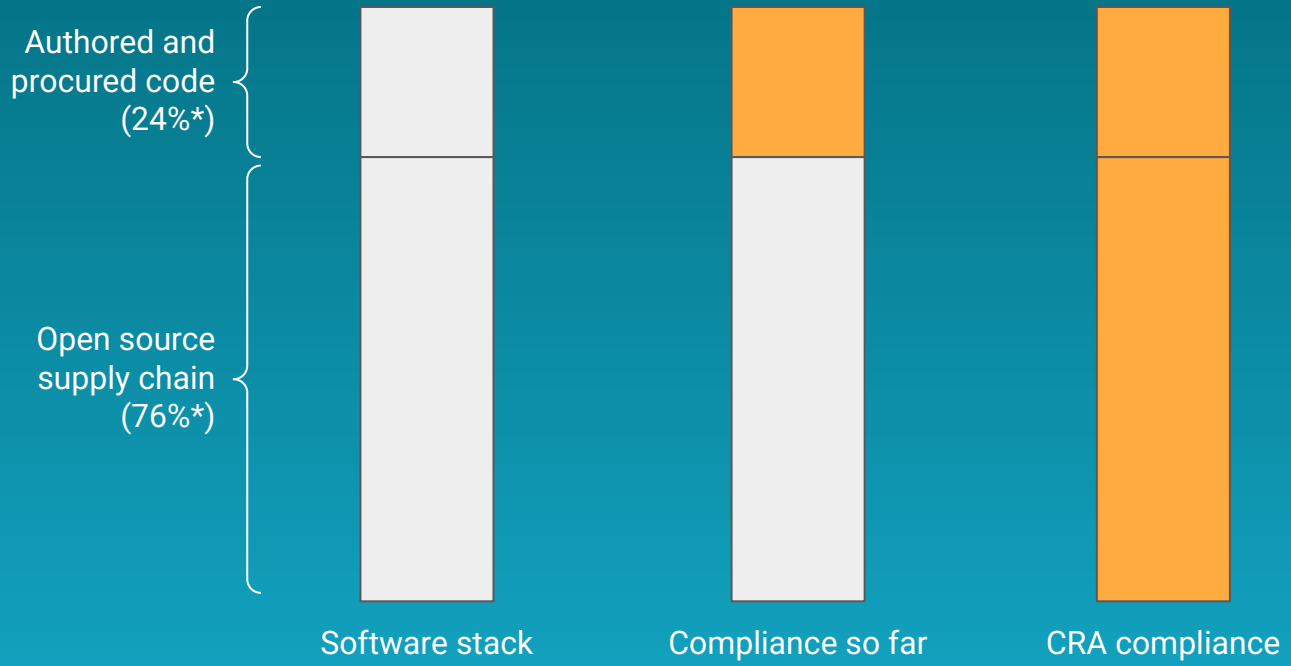
Horizontal (type A): August 30, 2026

Vertical (type C): October 30, 2026

Horizontal (type B): October 30, 2027

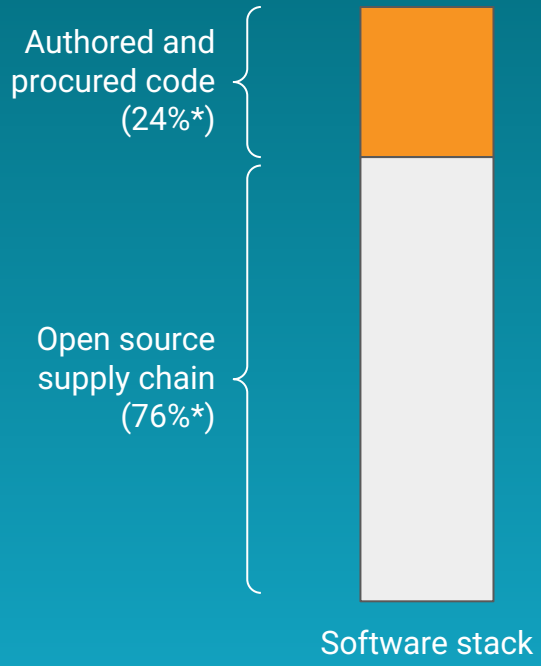
“We know how to do compliance already. How is this different?”

CRA innovation: full supply chain compliance



* Source: Synopsis OSSRA Report 2023

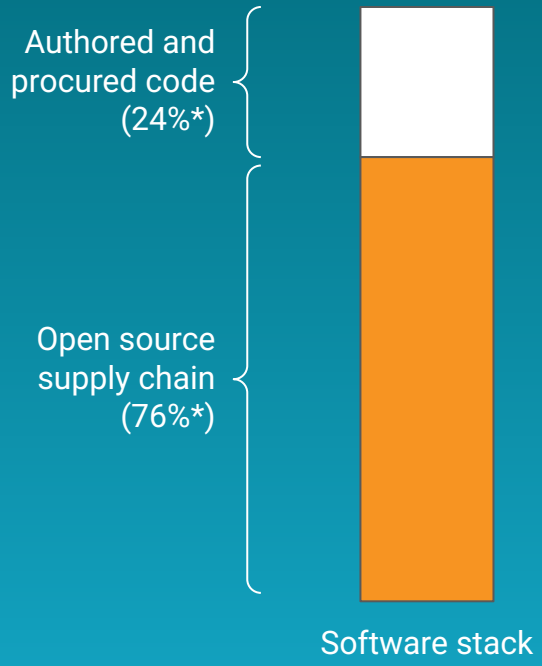
Impact of full supply chain compliance



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

* Source: Synopsis OSSRA Report 2023

Impact of full supply chain compliance

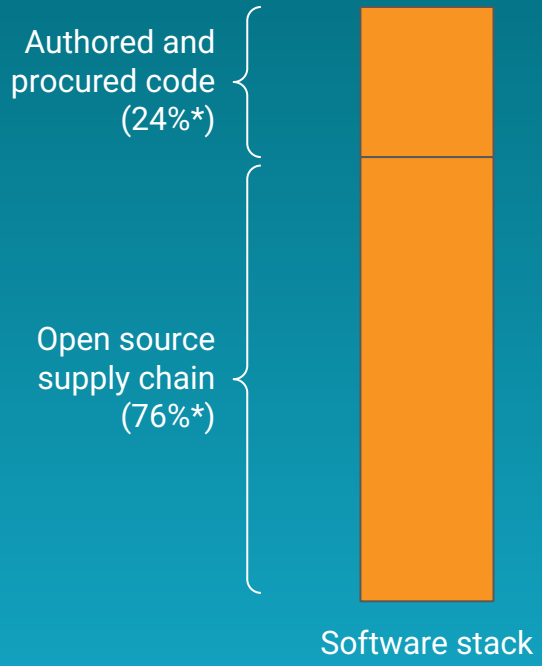


Open source supply chain
Compliance has to be **brokered** with open source community. Compliance requirements stay with manufacturers.

This is new!

* Source: Synopsis OSSRA Report 2023

Impact of full supply chain compliance



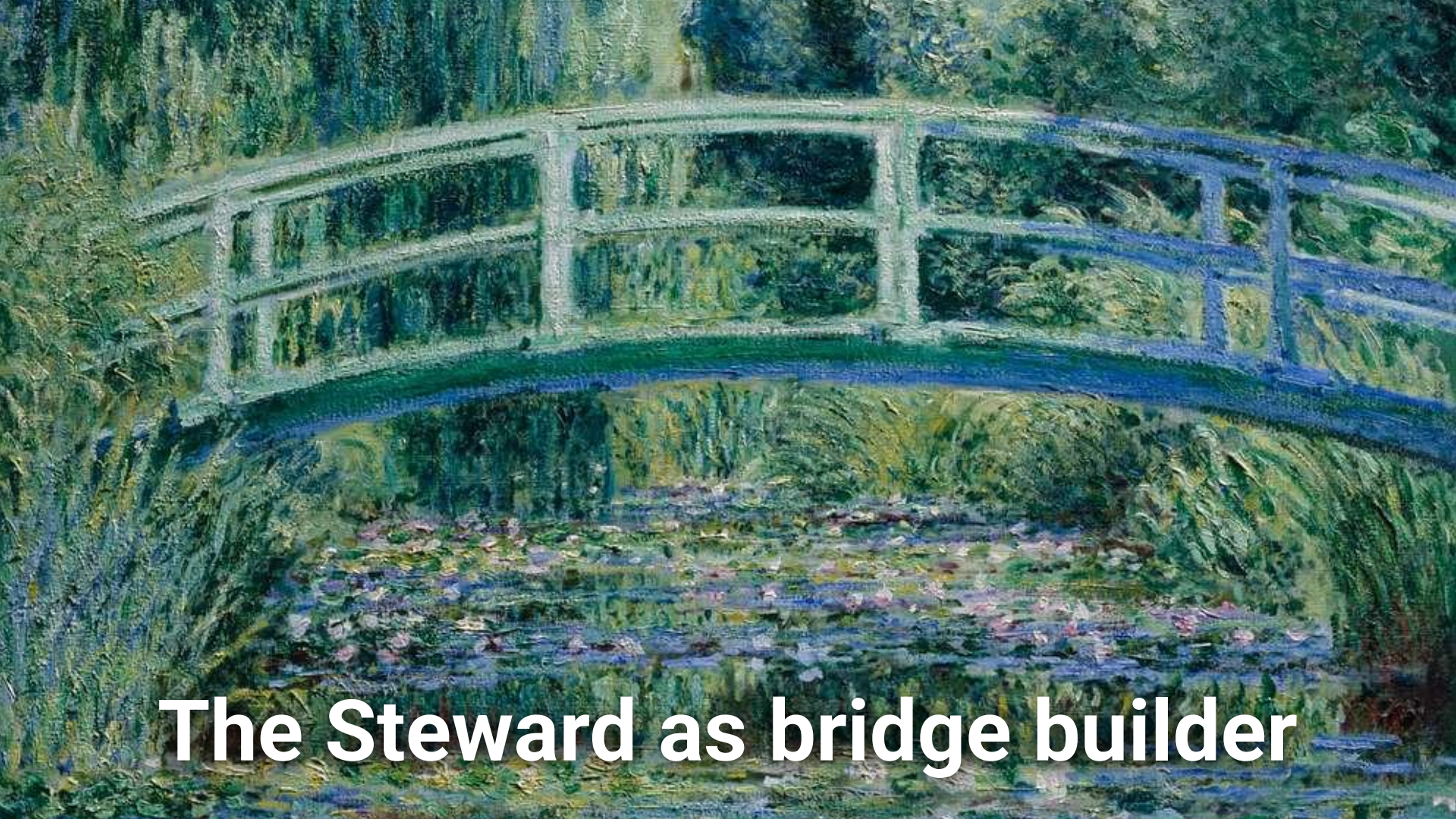
Authored and procured code
Compliance is managed through internal practices and vendor agreements.

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

Commonly-held belief: stewards will solve this for you!

* Source: Synopsis OSSRA Report 2023

Well… let’s see how stewards can help!



The Steward as bridge builder

Open source ecosystem

Wants resources and contributions

Manufacturers

Want to fulfill their due diligence obligations

Open source ecosystem

Wants resources and contributions

Manufacturers

Want to fulfill their due diligence obligations

Shift security left

Open source ecosystem

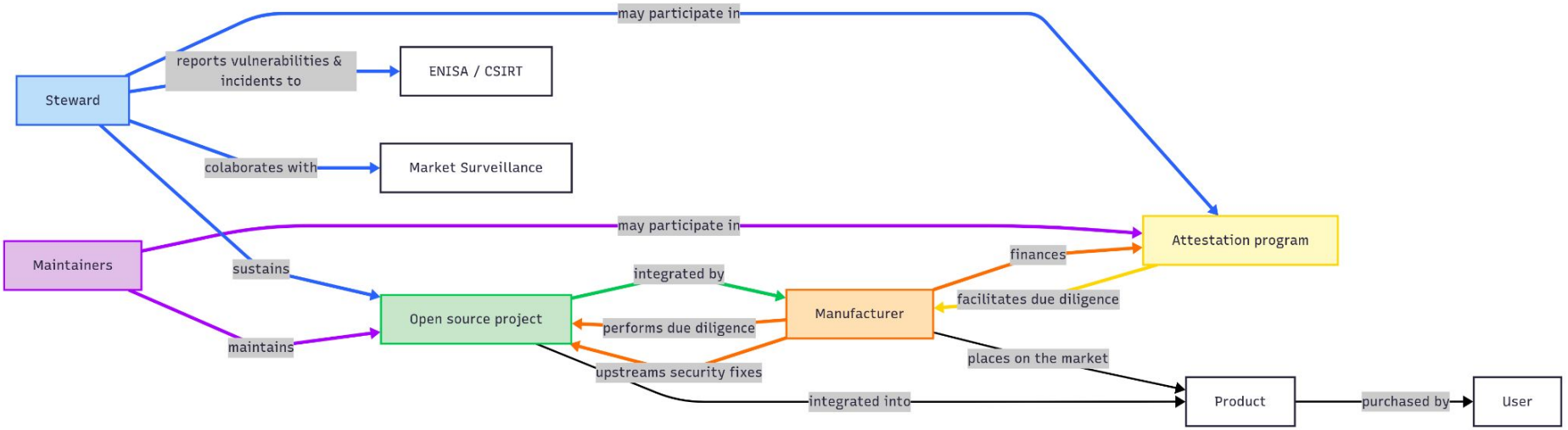
Wants resources and contributions

Manufacturers

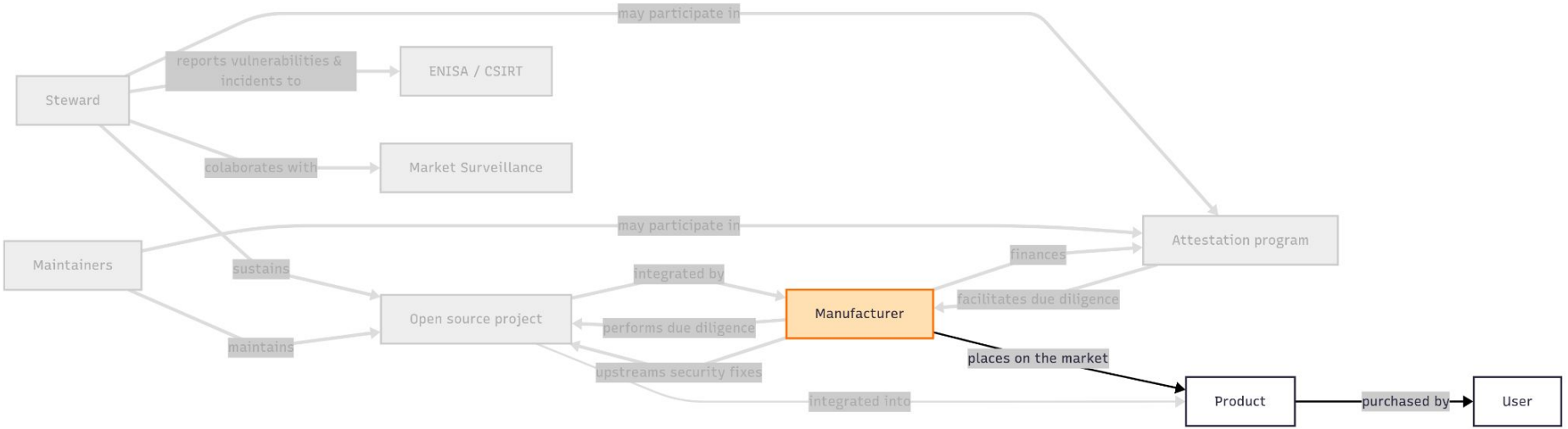
Want to fulfill their due diligence obligations

Shift security left

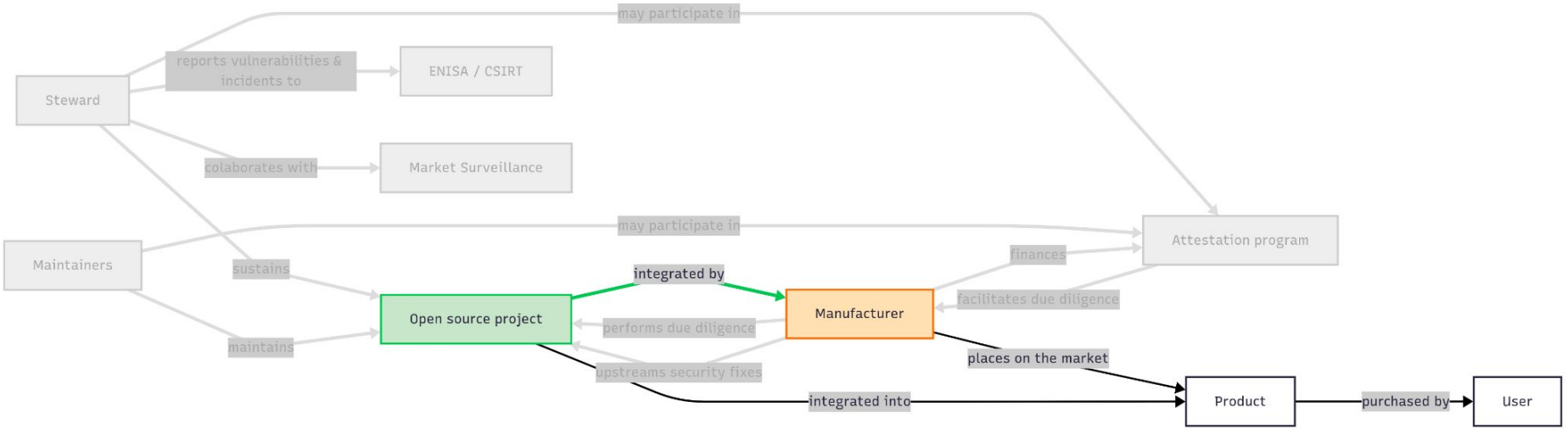
💰💰💰❓



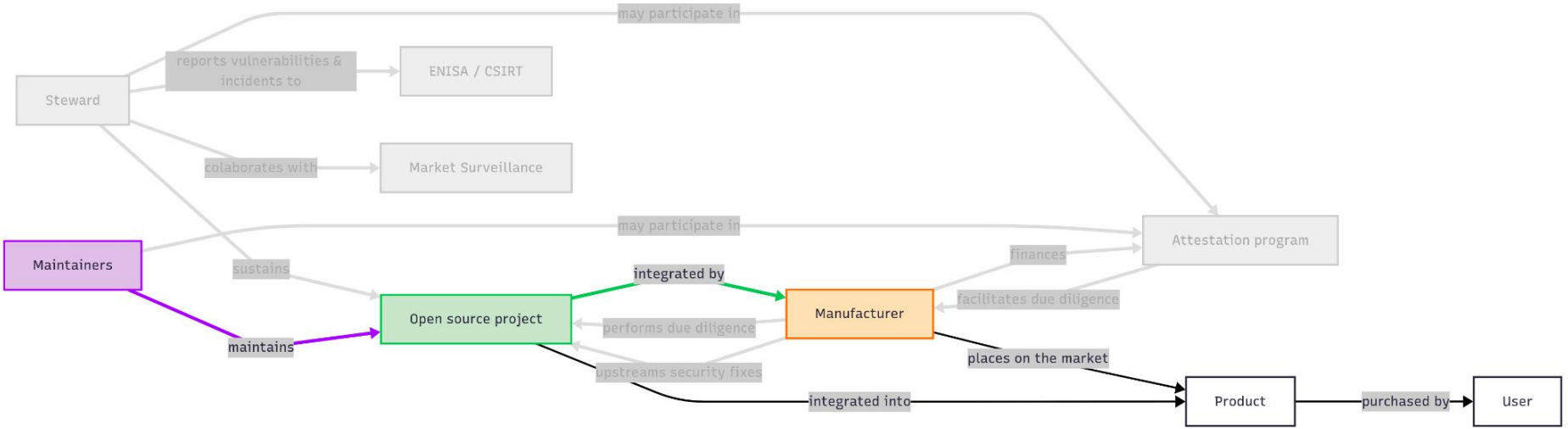
Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope



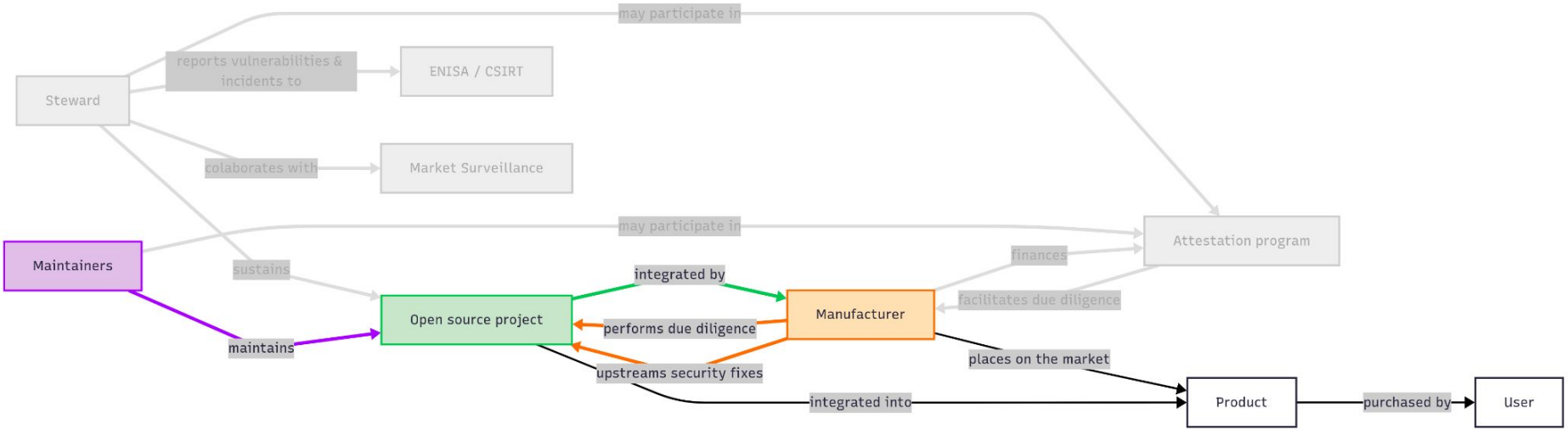
Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope



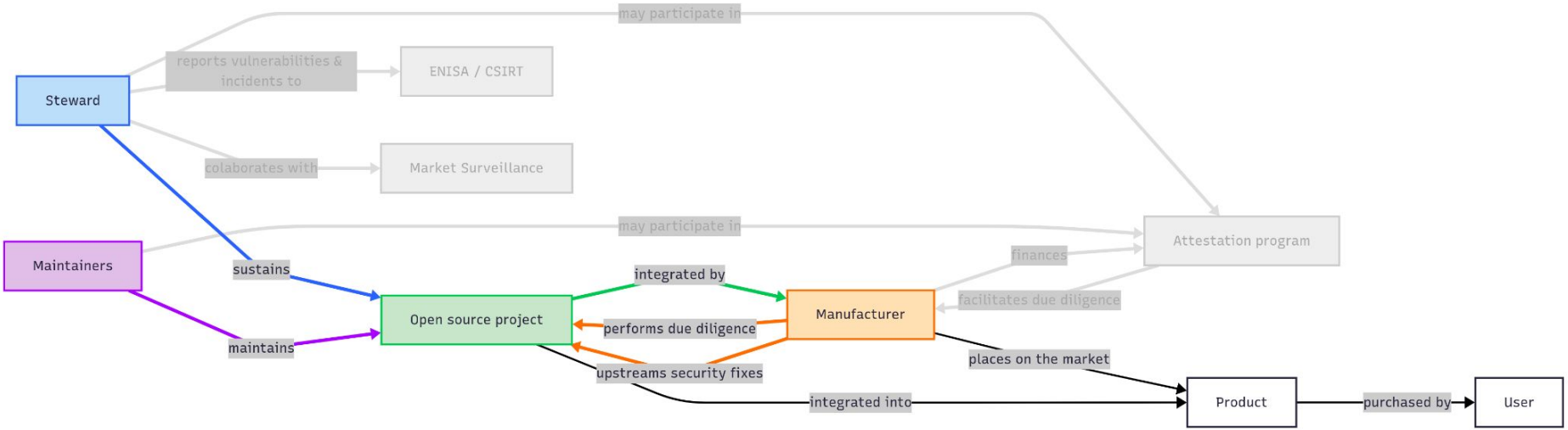
Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope



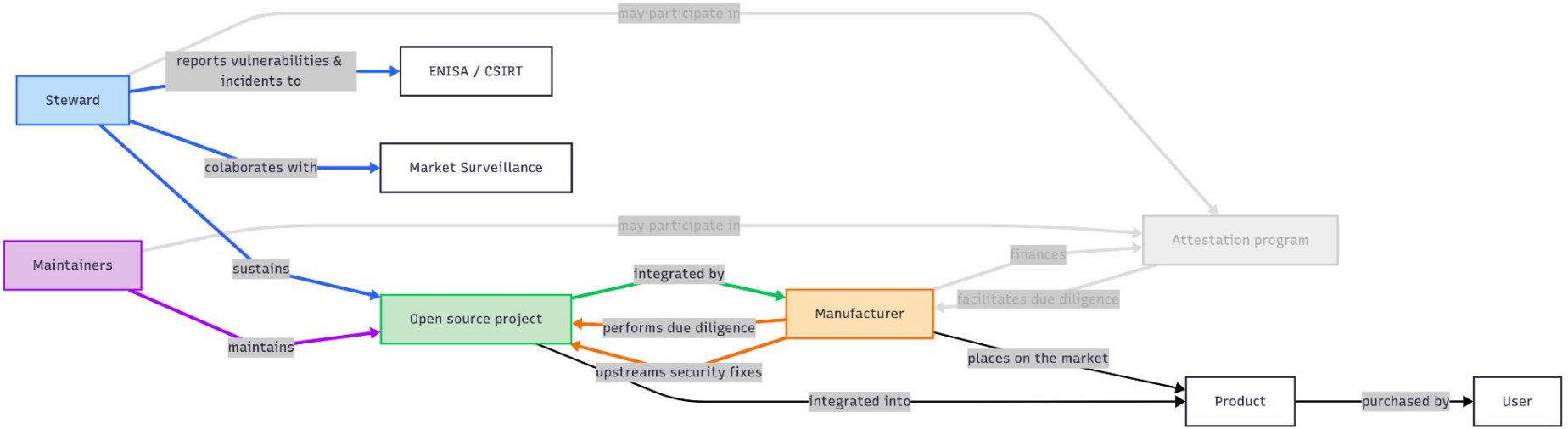
Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope



Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope



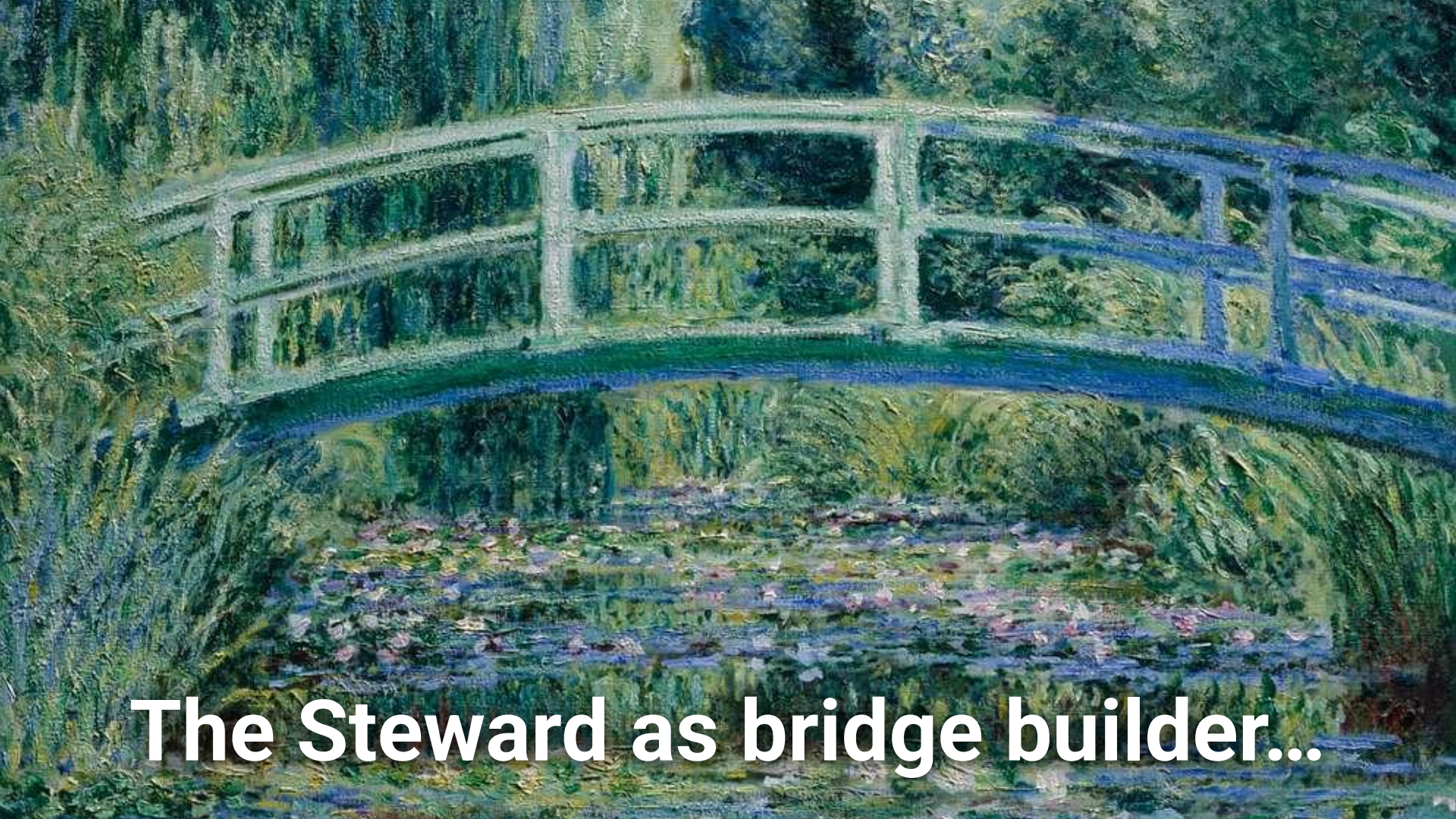
Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope



Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope

⚠️ *Stewards alone won’t solve manufacturer due diligence obligations*

Most projects don’t have a steward!



The Steward as bridge builder…


...security attestations as bridge

Open source ecosystem

Wants resources and contributions

Manufacturers

Want to fulfill their due diligence obligations

Shift security left

💰💰💰❓

Open source ecosystem

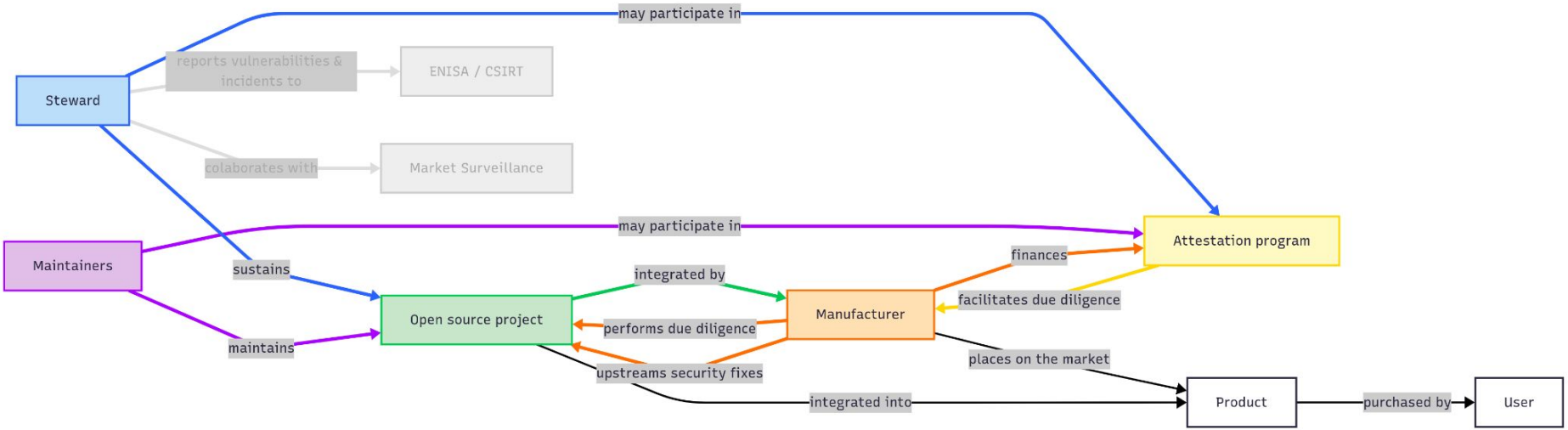
Wants resources and contributions

Manufacturers

Want to fulfill their due diligence obligations

Shift security left

Security attestations



Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope

“OK… but who is working on this?”

Open
Regulatory
Compliance

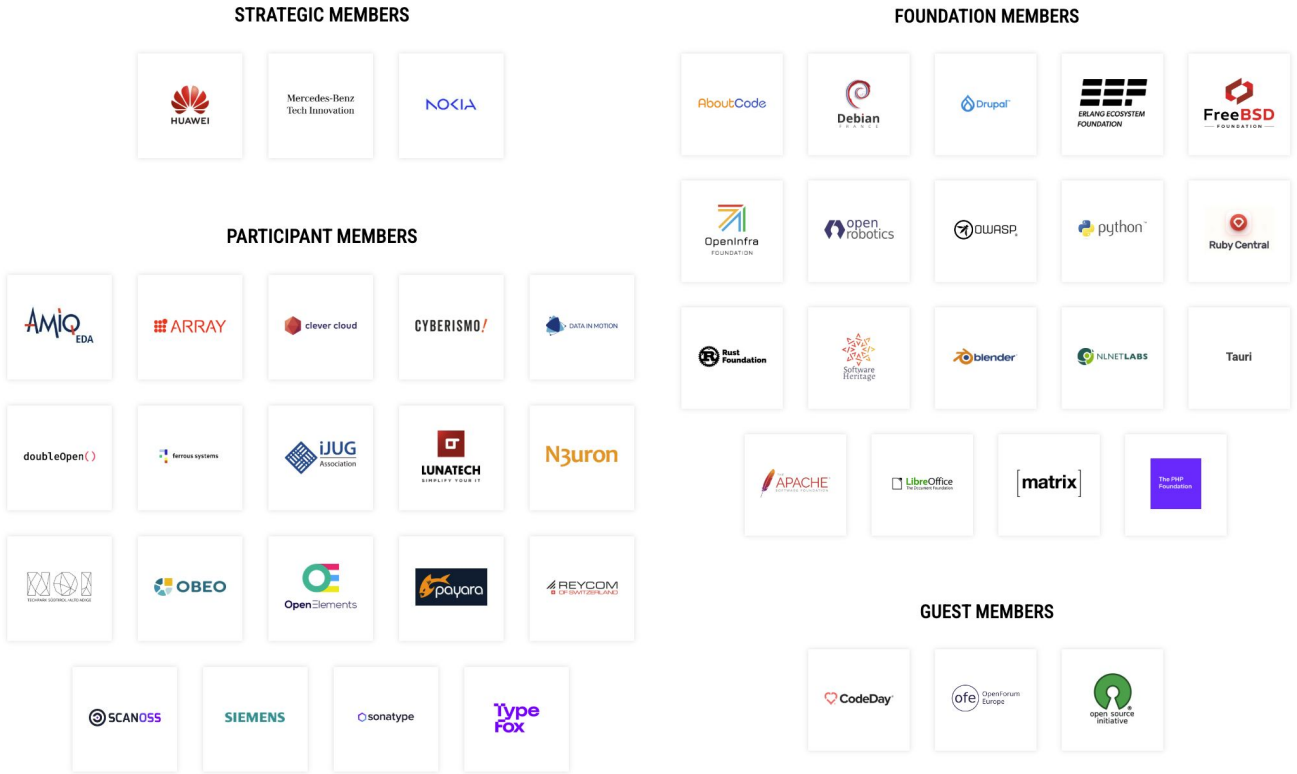
ORC WG

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

The ORC WG today

Membership

- 44 members
  - 3 strategic
  - 19 participants
  - 19 Foundations
  - 3 guests



Open Regulatory Compliance

ORG WG focus

Education & Thought Leadership
Close the knowledge gap!

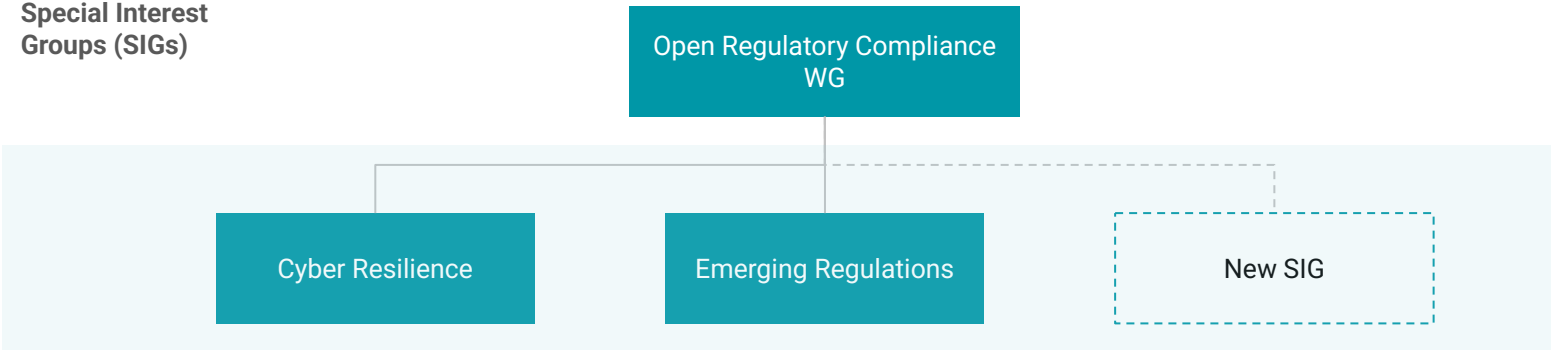
Technical Development
Formalize best practices into specifications.
Channel community and industry input to formal standardization bodies.

Institutional Engagement
Coordinate community and industry collaboration with the institutions.

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

Streamlining contributor experience

1. Organising the work in an easy-to-follow way.



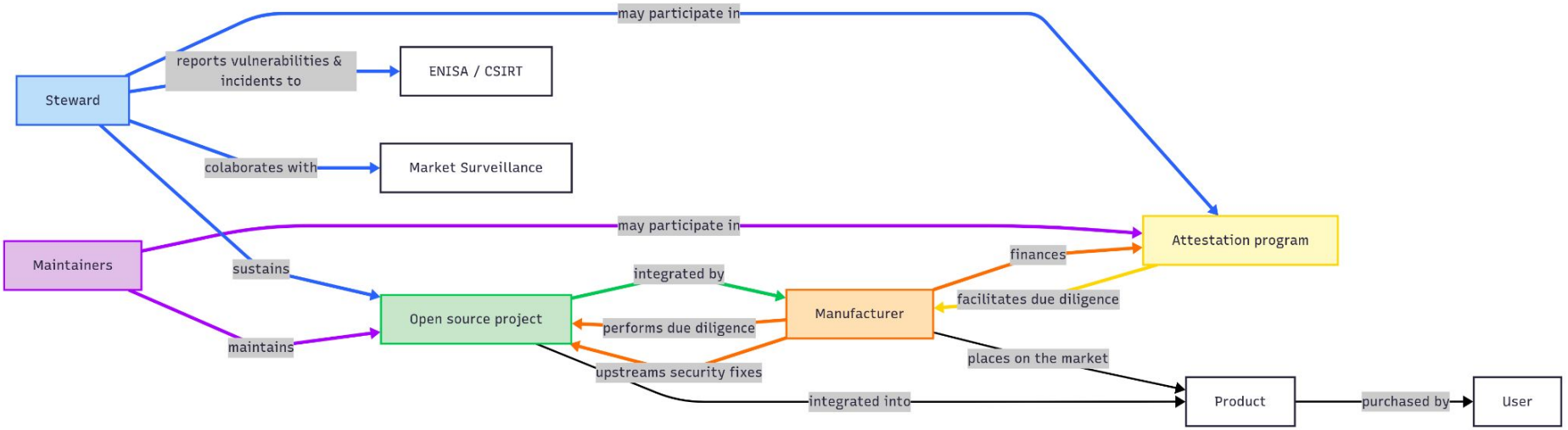
2. Using widely adopted tools and reducing the friction of first contributions.

2025 Deliverables Plan

Deliverable name	Type
CRA FAQ	Documentation
Inventory	Documentation
White paper on SBOMs	White paper
White paper on due diligence requirements for manufacturers	White paper
White paper on Attestations	White paper
Vulnerability handling specification	Specification
Specification on principles for cyber resilience for open source development	Specification
Specification on generic security requirements for open source components	Specification
Security policy for open source software stewards	Specification

Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig

Deliverables map directly to relations & obligations



Source: https://github.com/orcwg/orcwg/tree/main/cyber-resilience-sig#scope

Open Regulatory Compliance

Join us!

https://orcwg.org/

Thank You!