29 January

2026

{code & compliance}

FOSDEM EDITION

{ CRA vs Your Calendar }

Making Time for Compliance in Open Source Projects

Rachel Foucard – TYPO3 Board member

Conflict of Interest

Cyber Resilience Act

Other regulations

Diversity & Internationalisation

Ethical & Legal compliance

Open-source

Board member

Governance

TYPO3

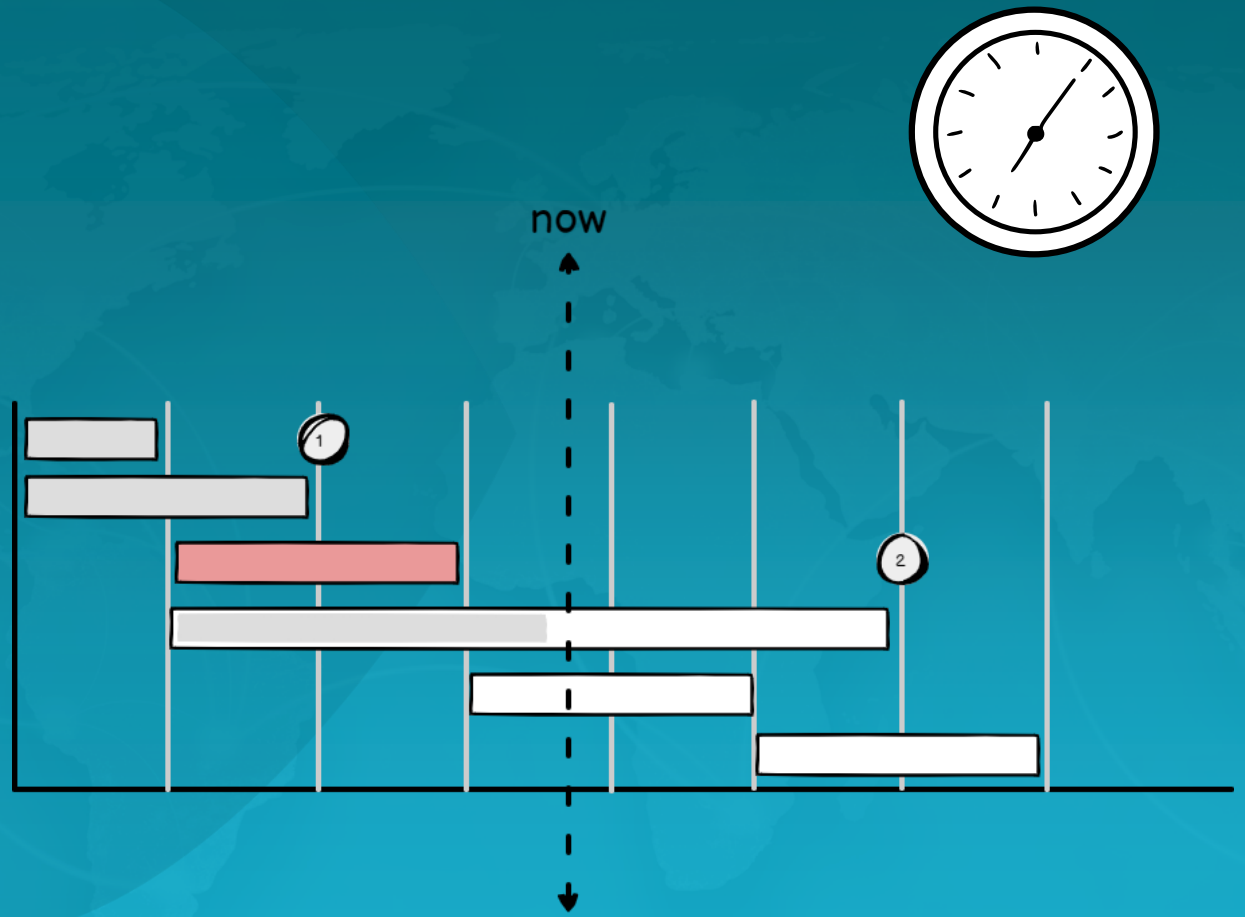
Risk management

UX team lead

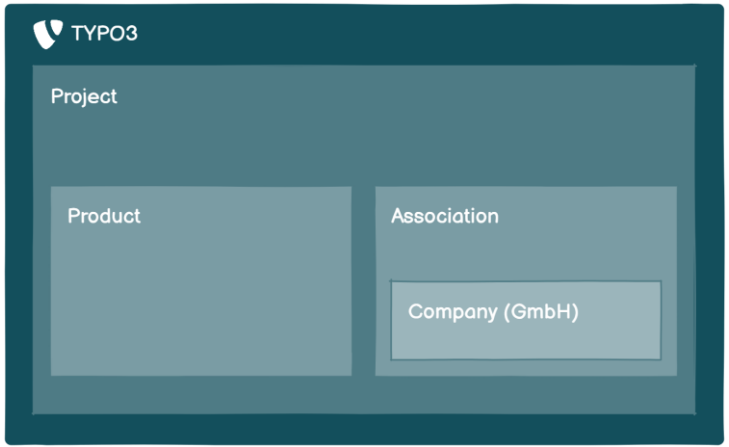
Web agency

Product Strategy

French community



TYPO3 at a Glance



Source https://docs.typo3.org

- x An Enterprise open-source Content Management System
- x A democratic open-source community with solid governance
- x Recognised as a Digital Public Good

Stewardship “time buckets”

- x Staying informed
- x influencing and defending your community’s interests
- x implementing and communicating changes in your organization

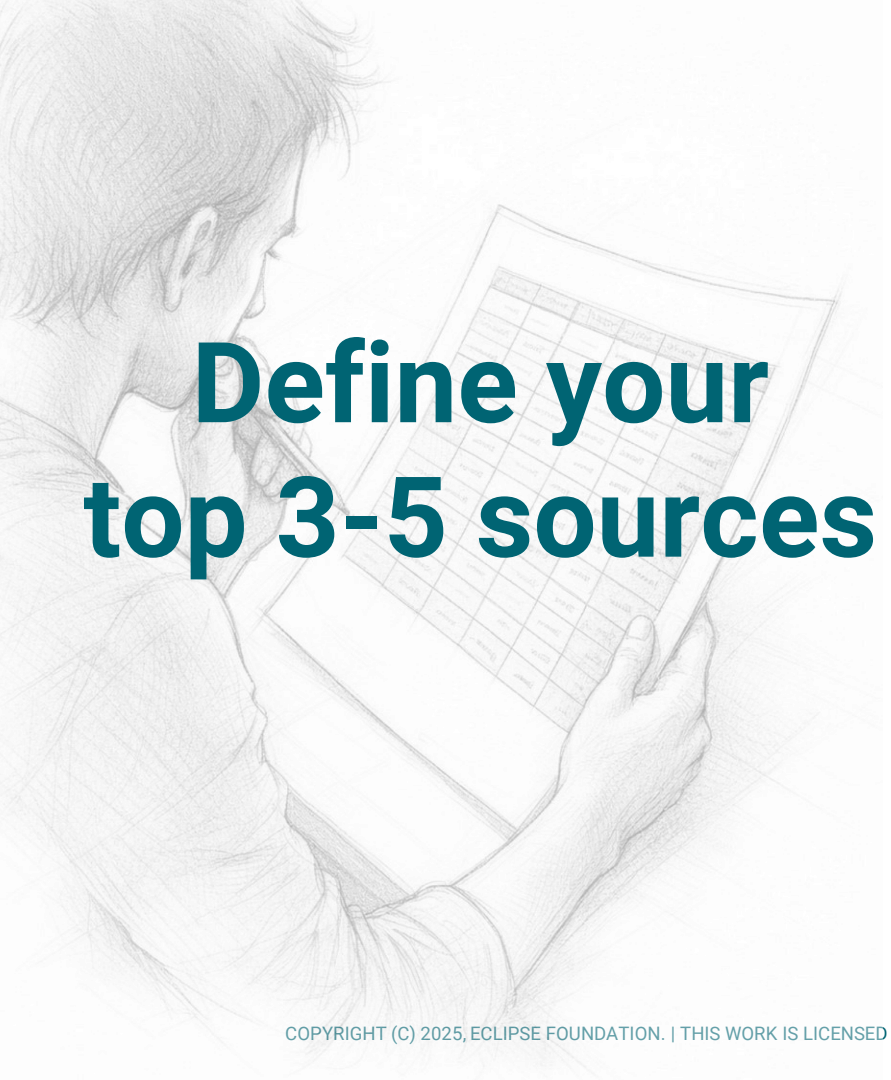
Define your time budget level

Who is available now, and for how much time?

x Level 1
1–2 h / week → essential stewardship

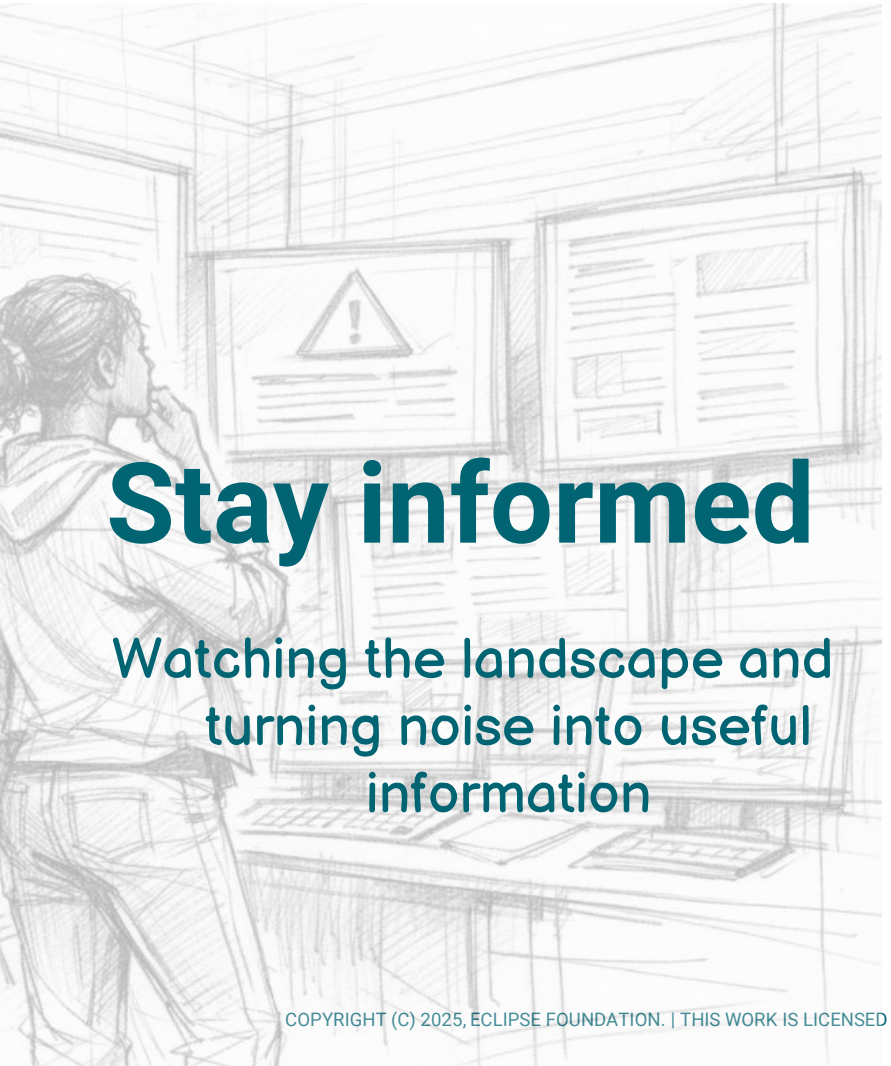
x Level 2 ✓
3–6 h / week → structured stewardship

x Level 3 ✓
7+ h / week → mature stewardship



Define your top 3-5 sources

- x European Commission (DG GROW – DG CONNECT)
- x ORC WG (Eclipse Foundation)
- x OpenSSF & Linux Foundation CRA WG



Stay informed

Watching the landscape and turning noise into useful information

- x **Read** the doc!
- x **Track** the changes
- x **Report** and share

Stay informed

Read

- ORCWG's OSS Stewards CRA Whitepaper (link) 1,2,3
- The regulation (summary) (fast-track) 1,2,3
- ORCWG's FAQ (link) 1,2,3
- EC's FAQ (link) 1,2,3
- ORC's events slides (link) 2,3
- The full ORCWG github repo (link) 3

Track

- Watch ORCWG cra-hub (link) 1,2,3
- Subscribe to DG GROW (link) 2,3 and DG CONNECT(link) 2,3 newsletters
- CRA expert group notifications (link) 3
- ENISA newsletter (link) 3

Report 1,2,3

- Top 3–5 signals (new guidance, consultations, deadlines, standards work, buyer expectations)
- Potential impact for your project (low / medium / high)
- "Possible future decisions" to flag early to the board.

Cyber Resilience Act – Enacting Terms

The enacting terms are the binding core of the Regulation: they set out the actual legal rules that apply in practice. They define scope, definitions, roles and responsibilities, and they establish concrete obligations, procedures, deadlines, and enforcement mechanisms. They also specify who must do what, when, and how, and they may empower the Commission to adopt delegated and implementing acts to fill in technical details over time. **In short: enacting terms provide the "what" and "how".**

This version proposes simplified summaries as "TLDR;", but you can read the original text clicking on the summaries.

- **Estimated reading time (summaries only):** ~20 minutes
- **Estimated reading time (full text + summaries):** ~3 hours

Chapter I - General Provisions

▶ **Article 1 - Subject matter** This Regulation sets cybersecurity rules and duties for placing digital products on the EU market, handling their vulnerabilities, and supervising compliance.

▶ **Article 2 - Scope** This Regulation applies to connected digital products placed on the market, with key exclusions (certain sector-regulated/certified products, spare parts, and security/defence) and a power for the Commission to refine scope via delegated acts.

▶ **Article 3 - Definitions** the following definitions apply.

▶ **Article 23 - Identification of economic operators** Economic operators must, on request, identify their suppliers and (where possible) their customers for digital products, and keep this traceability data for 10 years after receiving and 10 years after supplying the product.

▼ **Article 24 - Obligations of open-source software stewards** Open-source software stewards must maintain a verifiable cybersecurity and vulnerability-handling policy, cooperate and share that documentation with market surveillance authorities on request, and may have limited Article 14 reporting duties depending on their role and whether incidents affect their development infrastructure.

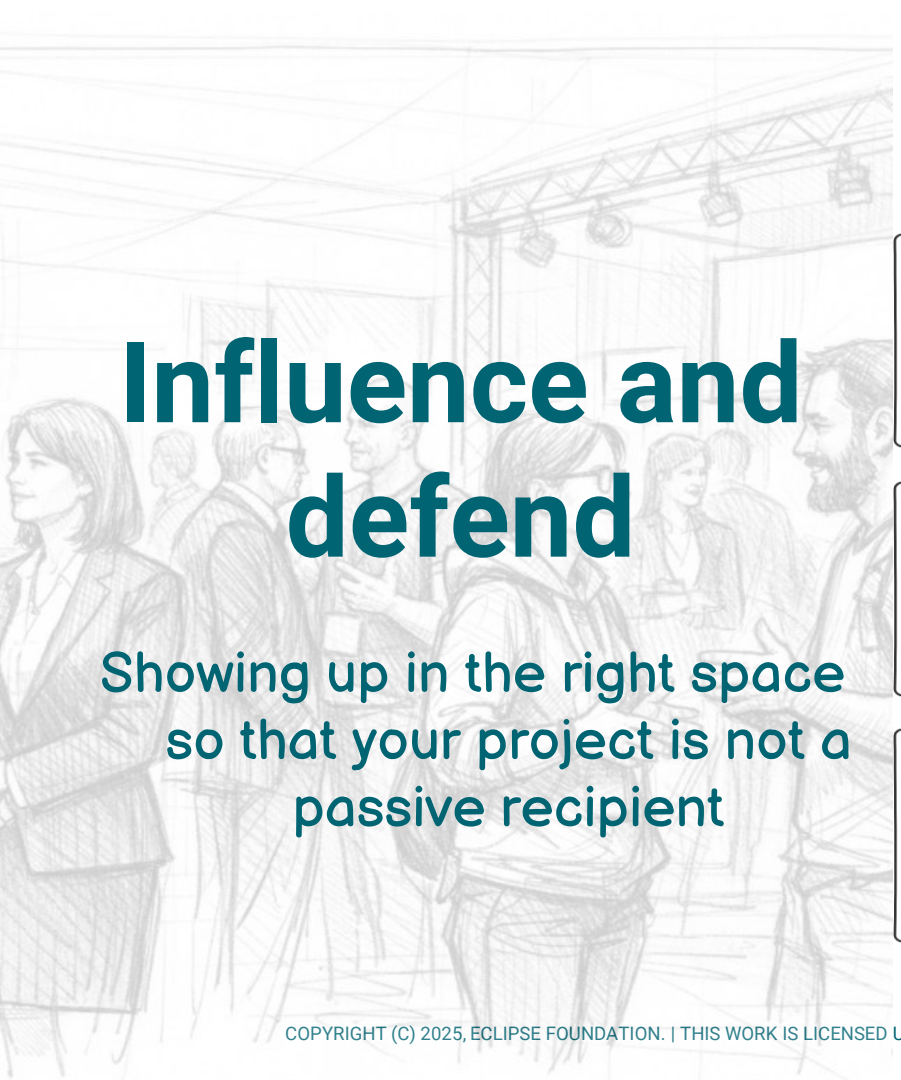
1. Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. That policy shall also foster the voluntary reporting of vulnerabilities as laid down in Article 15 by the developers of that product and take into account the specific nature of the open-source software steward and the legal and organisational arrangements to which it is subject. That policy shall, in particular, include aspects related to documenting, addressing and remediating vulnerabilities and promote the sharing of information concerning discovered vulnerabilities within the open-source community.
2. Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software.

   Further to a reasoned request from a market surveillance authority, open-source software stewards shall provide that authority, in a language which can be easily understood by that authority, with the documentation referred to in paragraph 1, in paper or electronic form.

3. The obligations laid down in Article 14(1) shall apply to open-source software stewards to the extent that they are involved in the development of the products with digital elements. The obligations laid down in Article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products.

▶ **Article 25 - Security attestation of free and open-source software** The Commission may create voluntary security attestation programmes (via delegated acts) to help manufacturers—especially those using open-source components—assess whether open-source products meet some or all CRA cybersecurity requirements.

▶ **Article 26 - Guidance** The Commission must publish stakeholder-informed guidance (especially for SMEs) on CRA scope, support periods, overlaps with other EU laws, and "substantial modification", and must keep an easy-to-access list of CRA delegated and implementing acts.

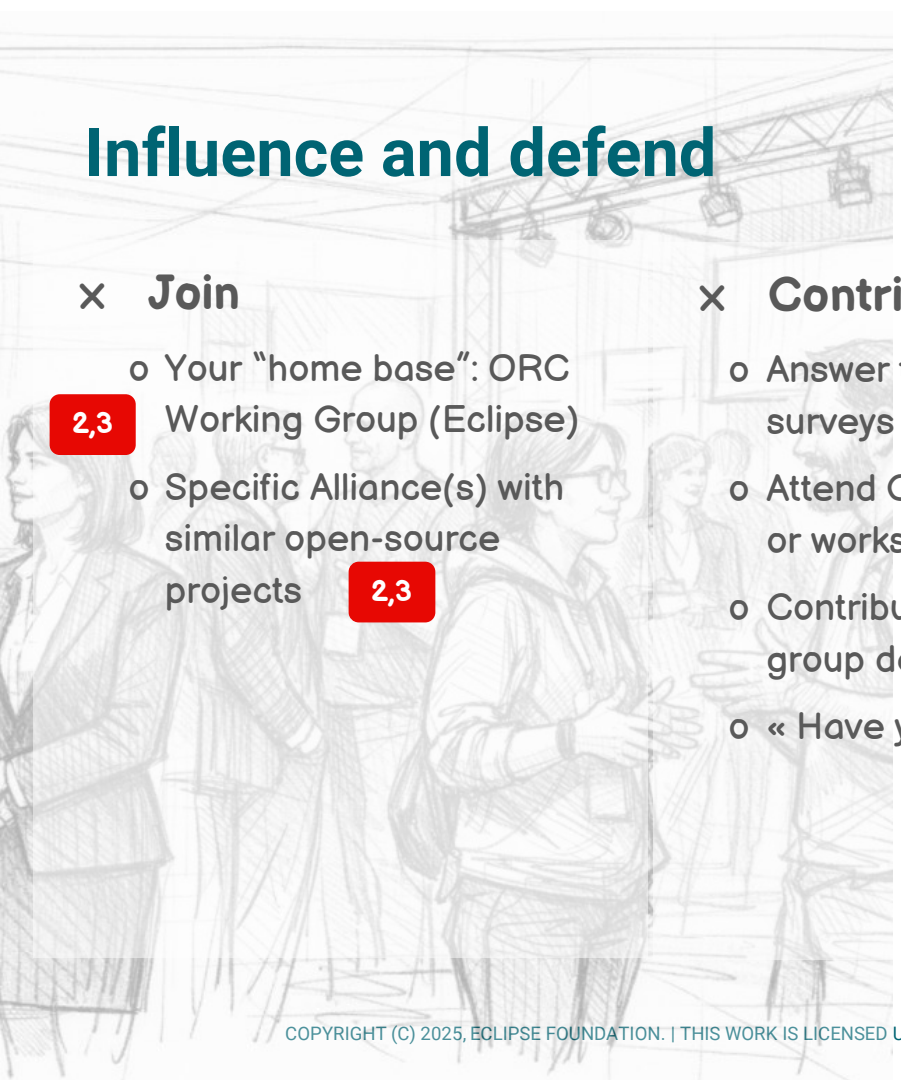


Influence and defend

Showing up in the right space so that your project is not a passive recipient

- x **Join** the existing alliances
- x **Contribute** with the existing working groups
- x **Share** your ecosystem use case

Influence and defend



× Join

- o Your "home base": ORC Working Group (Eclipse) 2,3
- o Specific Alliance(s) with similar open-source projects 2,3

× Contribute

- o Answer to CRA related surveys (example) 2,3
- o Attend CRA related events or workshops 2,3
- o Contribute in ORC working group deliverables (link) 2,3
- o « Have your say » (link) 3

× Share 3

- o Your use case experiment
- o Your resources

CRA Time Filter – 5 questions

For any **event / call / working group / consultation**, ask:

1 - Impact in the next 12–18 months?

Does this have a realistic chance of impacting our obligations, deadlines, or what our main users expect from us in the next 12–18 months?
- If it's just generic "security awareness", it's probably **no**.
- If it's guidance on reporting, support periods, standards → more likely **yes**.

2 - Are *we* actually the target?

Is this specifically about open-source stewards / maintainers / projects like ours — or is it mainly about large manufacturers or sectors we're not in?
- OSS stewards / FOSS in the agenda → **big plus**.
- Strictly "IoT device manufacturers only" → you can probably just read a summary later.

3 - Is there something concrete to influence or produce?

Will this lead to a text, guideline, template, or position we can help shape — or is it purely informational / marketing?
- Draft guidance, standardisation inputs, joint position → **worth considering**.
- Vendor webinar "How our product solves CRA" → usually **skip**.

4 - Is someone else already there for our ecosystem?

Is a trusted organisation (foundation, alliance, ORC, OpenSSF, national association) already in the room and able to represent concerns similar to ours?
- If yes, ask: *Can we get their notes or contribute written input instead of attending?*
- If no, and impact is high, it may be worth someone from your ecosystem going.

5 - Is this the smallest effective forum?

Is this the place where one hour of our time benefits many projects, or is it just another parallel group duplicating work done elsewhere?
- Cross-project WGs (ORC, OpenSSF, national alliances) → one hour benefits many.
- New micro-WG inside your own ecosystem on the same topic → often redundant.

CRA Time Filter – 5 questions

My simple "rule of thumb"

Go / send someone live if:
Q1 = yes (impact), **and**
at least **2** of Q2–Q5 = yes.

Else, participate asynchronously (send written input, read minutes) if:
Q1 = maybe, **or**
Q2 = no (not really about stewards), but your users care.

Else Skip because:
Q1 = no (no real impact for your obligations or main users),
and nobody in your extended ecosystem treats it as important.

Implement and communicate

making things real inside the project and being able to explain what you do

- x **Fulfill reporting obligations** (11-09-26)
- x **Fulfill all CRA stewards' obligations** (11-12-27)
- x **Communicate** with your community

Implement and communicate

- [ ] **Fulfill reporting obligations (11-09-26)** 1,2,3
  - **Cybersecurity policy**
  - **Process to show** that policy to MSAs
  - **Process to report** exploited vulnerabilities or severe incidents
  - **Process and channel to inform** users about vulnerabilities or incidents
- [ ] **Fulfill all CRA obligations (11-12-27)** 1,2,3
  - Cybersecurity policy aligned with your **governance** and existing processes
  - **Process to cooperate** on corrective actions with authorities
  - (If applicable) Fulfill some **manufacturer-type obligations** (SBOM, etc.)
- [ ] **Communicate with your community**
  - A clear **CRA reference page** explaining your role and limits 1,2,3
  - Publish regularly **articles** about your CRA implementation progress 2,3
  - **"Communication kits"** partners can reuse when they talk about your project and the CRA 3

Questions?