element

Leading the way into CRA compliance

Element’s approach to the incoming regulation

Denise Almeida (denisea@element.io)

Cyber Resilience Act (CRA)

element

- What? **An EU regulation**
- Why? **Enhance the security of hardware and software products.**
- How? **Set uniform standards across the EU** by establishing comprehensive **cybersecurity requirements** for products with digital elements within the European Union.

More specifically...

element

- In place since December 2024, currently in implementation period. Full set of obligations will start being enforced from July to December 2027.
- Applies to all Products with Digital Elements (PDEs), which must all be designed and developed in accordance with the CRA.
- Applicable on a product level, not an organisational level. This means Element will be a manufacturer, distributor and open source steward, depending on the product.
- Product definition and scope are based on when it was **first placed on the market** (art. 21.3)

To what does it apply?

element

Scope is mainly determined at a product level:

- Any product with digital elements, be it hardware or software, that can connect to a network or device
  - Rationale here is that if a product can connect to a network/device it can create a risk, therefore it's automatically in scope
  - This might seem very broad - this is intentional
- Remote data processing solutions and its components

Following that, it applies to different layers of the supply chain: manufacturers, importers and distributors

What is out of scope?

element

- Cloud or other SaaS regulated under NIS2
- Software developed exclusively for classified information
- *Technically* non-commercial open source software is out of scope, however some immediate ques:
  - *How can we define what is non-commercial when using permissive licences which allow for commercial and non-commercial use?*
  - *Whose responsibility is it to figure all of this out? What if I'm just maintaining a small project by myself?!*
  - *What if I develop open source and proprietary software which can be commercial or non-commercial?*

Different roles

- **Open-source Software Stewards**, i.e. foundations supporting open source software
  - a legal person [...] that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products.
- **Manufacturer**, i.e. companies building and selling software
  - means a natural or legal person who develops or manufactures products with digital elements [...] and markets them under its name or trademark, whether for payment, monetisation or free of charge.
- **Importers**
  - a natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union.
- **Distributor**
  - a natural or legal person in the supply chain[...] that makes a product with digital elements available on the Union market without affecting its properties.

What will be the obligations?

element

Main requirements are:

1. Minimum cybersecurity measures in place
2. Conformity assessments
3. User transparency around security risks
4. Vulnerability patching and documentation
5. Incident and vulnerability reporting

⇒ **Manufacturers** hold the responsibility for CE marking, demonstrating compliance and reporting.

⇒ **Importers & distributors** verify that products comply with the CRA before placing them on the market.

What will be the obligations?

Old slide

element

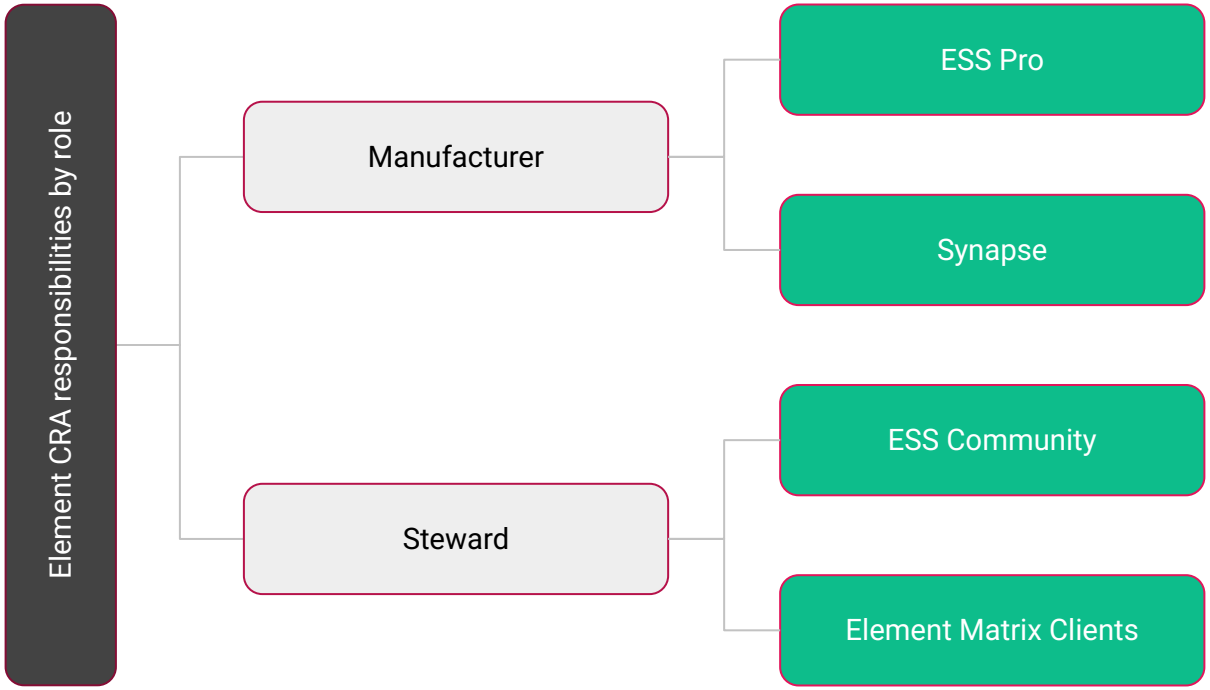
Main requirements are:

1. Minimum cybersecurity measures in place
2. Conformity assessments
3. User transparency around security risks
4. Vulnerability patching and documentation
5. Incident and vulnerability reporting

Manufacturers hold the responsibility for CE marking, demonstrating compliance and reporting.

CRA compliance: the Element case

element



CRA compliance: the Element case

element

- As original manufacturer of ESS Pro and Synapse Element will, in due course, make available more of our internal thinking and preparations for the CRA
- As both the creators of Matrix and the developers of Element products we are uniquely positioned by having deep knowledge of the security of protocol, whilst being able to provide a streamlined single source of reporting and disclosure of security communications
- We are working through the potential challenges around our distinct roles as both manufacturers and stewards, particularly as FOSS Guidance on the CRA is still being worked on

Integrating compliance into an open source business strategy

element

Funding open source businesses can be challenging and regulatory compliance adds an additional layer of complexity and costs.

Example of what is currently on our roadmap:

- Evaluate and list all potentially in scope products, as well as roles;
- Conduct a gap analysis on internal preparedness for the new CRA requirements;
- Develop a plan of works to address any gaps and maintain compliance posture;
- Review staffing and resource levels and be prepared to revisit ways to reflect changed budgets in pricing.

What could this mean for open source?
Risks

We hope the CRA delivers on its aims of increased security, harmonised coordination and improved supply chain management. However, there are some risks we would like to see clarified:

- How can we ensure open source projects are **sufficiently funded** and informed to implement all requirements?
- What mechanisms will be put in place to **ensure that distributors and importers are meeting their reporting obligations**?
- What will be done to **support open source manufacturers who also take on the role of stewards**?
- Could the CRA **unintentionally steer organisations towards proprietary software** for ease of supply chain management? How can we ensure a focus on open source remains?

What could this mean for open source?
Opportunities

element

However, the CRA also presents us with an opportunity to demonstrate how the values of open source are aligned with the aims of the regulation:

- **Transparency** and communication are crucial for open source development, as they are for the implementation of the CRA
- Creates an opportunity for organisations to have a **clearer understanding of their dependencies and roles**
- Increased **focus on security** and secure development
- Opportunity for organisations using open source software to **evaluate their own approach to open source and how they might be supporting its secure development**

Next steps

element

- Legislation is written in vague terms on purpose, especially when its scope is so vast. **More clarity will come** as implementation guidance comes out - this is being actively worked on by the Commission, in consultation with civil society, businesses and FOSS community members.
- The CRA has an explicit aim to support a rebalancing of the market, however it is our responsibility to prepare and educate ourselves as a community.
- It is crucial to engage with the wider open source community as we work towards a more sustainable and secure space.

element

Thank you for your time!

Denise Almeida (denisea@element.io)