Compliance in Practice: Nokia Perspective on the CRA

Code & Compliance

Oct 23rd 2025 Brussels

Timo Perälä

  | Apply a document ID (if applicable).

Nokia at a glance

We are a B2B technology innovation leader pioneering networks that sense, think and act

Enabling our customers to realize the full potential of digital:

- Service providers
- Enterprises
- Hyperscalers
- Defense
- Technology licensees

€19.2bn
net sales in 2024

~130
countries of operation

7k+
patent families declared as essential to 5G

€150bn+
invested in R&D since 2000

155+
years in business

10
Nobel Prizes for ground-breaking inventions

Delivering networks that sense, think and act across our best-of-breed portfolio

Network Infrastructure

- IP networks
- Fixed networks
- Optical networks
- Submarine networks

Mobile Networks

- Radio access networks
- Microwave radio links
- Related network management software and services

Cloud & Network Services

- Business applications
- Core networks
- Cloud and cognitive services
- Enterprise campus edge

Nokia Technologies

- Patent licensing
- Technology licensing
- Brand licensing

Nokia Bell Labs

- Core research
- Solutions research

€150bn+ invested in R&D since 2000

Open Source is vital for Nokia

Part of R&D

Nokia uses significant amounts of open source part of its products in non-differentiated parts

Ecosystem compatibility

Being part of bigger ecosystems including cloud

Ensuring compatibility & interoperability

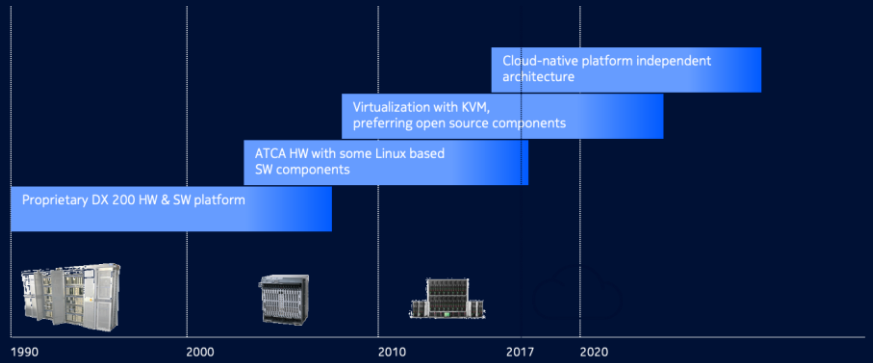
Shaping the industry environment

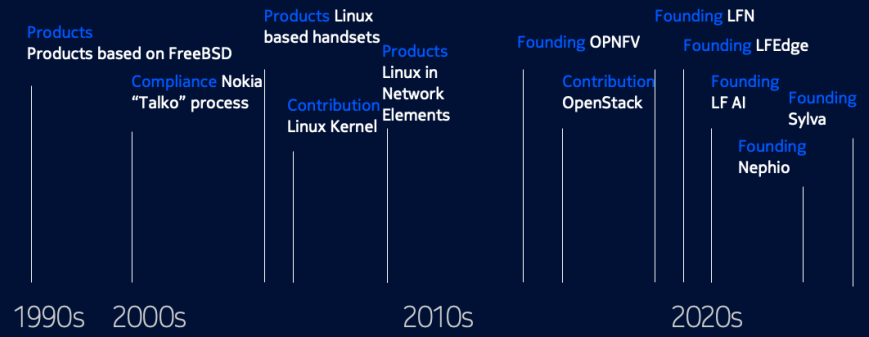
Nokia has a long open source journey

All Nokia products have some open source, some products are based on open source

Open source used for replacing proprietary systems such as operating systems with open source (Linux)

Used in areas of **low differentiation** (e.g. operating systems), where **compatibility with the ecosystem** is needed (e.g. cloud), and to **access technology**





Motivation for Cyber Resilience Act (CRA)(*)

" Cyberattacks represent a matter of public interest as they have a critical impact not only on the Union's economy, but also on democracy, consumer safety and health."

"Two major problems adding costs for users and society should be addressed:

- **A low level of cybersecurity** of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
- **An insufficient understanding and access** to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner."

(*) Available in pdf and in Word

Intended impact of the CRA

*"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."*

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

*"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."*

CE marking for the software

Non-compliance penalties

€15M/€10/€5M or 2.5%/2%/1% of global annual turnover, which ever is higher depending on severity of the case

CRA will strongly impact how products are created, distributed and maintained

Documenting software and its security including SBOMs	Product configuration	Product design
Product security and vulnerability management	Software distribution	Certification and testing
Vulnerability reporting	Other security aspects including access control	Process and product auditing
Usage and patching of open source software	Data protection and storing/confidentiality/etc	Open source software development, OS Steward

Obligations for manufacturers - Art 13 CRA

Design for Security

Product designed to be compliance with Essential Requirements

Risk Assessment

Security risks of the product assessed and considered during the planning, design, development, production, delivery and maintenance phases of the product

Risks assessed based on the intended purpose and reasonably use of the product

Risks systematically documented and updated based on the nature and relevant cybersecurity aspects related to the product

Due diligence

When integrating components sourced from 3rd parties

Market Surveillance

Technical documentation incl. SBoM and the EU declaration of conformity to be available for Market Surveillance authorities for at least 10 years

SW Bill of Materials

EC may specify the format and elements of SBoM with implementing act

Identification of the product

Products marked with type, batch or serial number or other element allowing their identification

Alternatively in packaging or in a document accompanying the product

Vulnerability Handling

Effective and timely vulnerability handling throughout the life cycle of the product

Report identified vulnerabilities to maintainer of a component

Share the fixes with the maintainer of a component

Single point of contact for vulnerability reporting

Security Updates

Available minimum of 10 years

Technical Documentation

Information and instructions to the user

Risk assessment

A copy of the EU declaration of conformity or a simplified EU declaration of conformity

Continuous Conformity

Ensure products remain in conformity

Corrective Actions

Corrective measures to bring a product or the processes into conformity, or to withdraw or recall the product

Support Period

Easy and accessible indication of the end date of the support period

End user notification about the end of the support period

There’s more to it than just the CRA legal text

Harmonized standards
Standardisation Request contained 41 (and counting!) standards to be developed by the European Standards Organisations (ESOs), CEN/CENELEC and ETSI.

Additional *Implementing acts, Delegated acts*
E.g. to set up an attestation program

Best practices
Formalized best practices help manufacturers perform due diligence

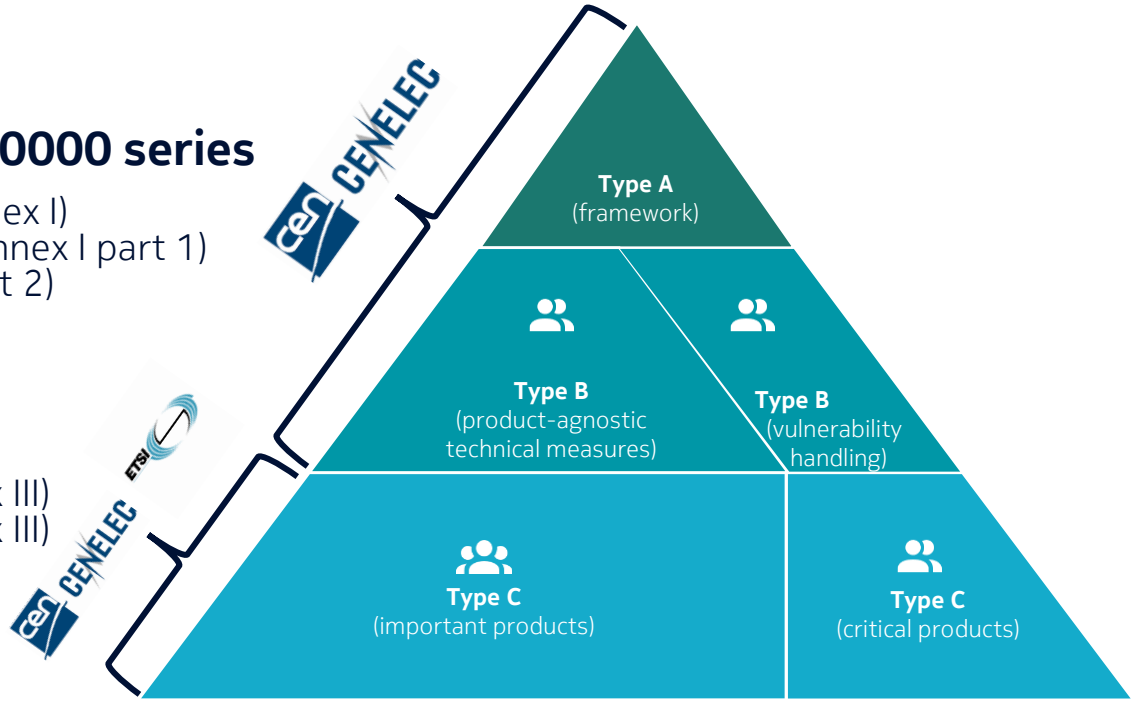
Harmonised Standards provide detailed guidance

Horizontal standards (1-15), EN 40000 series

- Principles for cyber resilience (CRA Annex I)
- Generic Security Requirements (CRA Annex I part 1)
- Vulnerability Handling (CRA Annex I part 2)
- Vocabulary

Vertical standards (16-41+)

- Important products class 1 (CRA Annex III)
- Important products class 2 (CRA Annex III)
- Critical products (CRA Annex IV)
- Specific standard for Telecom System



Open source community response

Open Regulatory Compliance Working Group

https://orcwg.org/, https://github.com/orcwg

Organised in Eclipse Foundation, established 2024

Open Regulatory Compliance

OpenSSF Global Cyber Policy Working Group

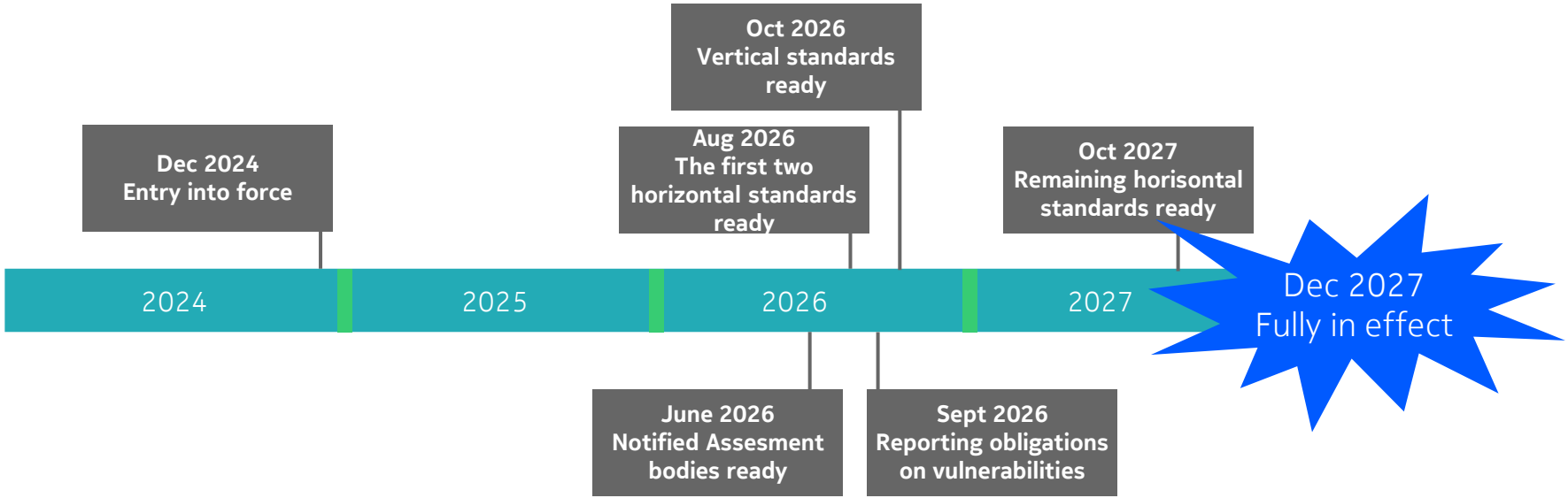
https://openssf.org/groups/global-cyber-policy/
https://github.com/ossf/wg-globalcyberpolicy

Organised in OpenSSF, established 2025

Not only about CRA, but initially the main focus
Steep learning curve to engage with

- European Commission
- The European Standardisation Organisations, CEN/CENELEC and ETSI

CRA timeline is short – so is the time to get prepared



Manufacturer getting ready for the CRA: case Nokia

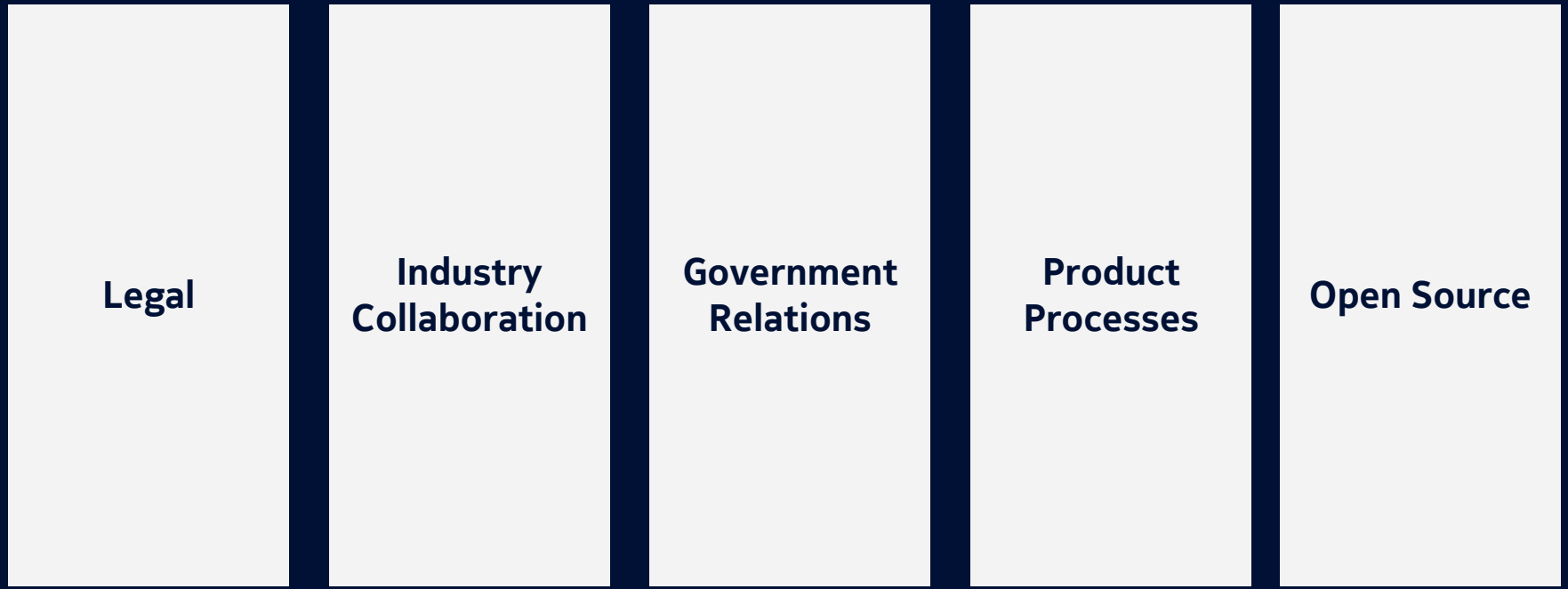
Starting point: Nokia's business environment:

- ❑ Highly regulated
- ❑ Highly standardised
- ❑ Standards are created by the whole industry

We are in a fairly good place to start our journey to comply with the CRA

Target: Nokia is compliant with CRA while the cost of compliance impacting Nokia, and its customers is minimized

Nokia is prepared for the CRA: cross company program



Being prepared, with challenges … and observations

Challenges

- Two groups, doesn't that introduce overhead?
- Manufacturer's Due Diligence requirement on open source
- OS Attestation, what is it?
- We have our assesment criteria, but howw do OS projects show they are reliable, how can a manufacturer conclude it is safe to use?
- How do all these come together within the given timeline

Observations

- Fulfilling assesment criteria might serve as an avenue for higher adoption, higher engagement. This may have a spill effect on non-vulnearibility related contributions.
- When manufacturer gains better understanding of open source, their assesment criteria may evolve: projects adopting attestasion criteria may become more attractive.
- CRA teaches manufacturers responsibility in their engagement with open source

Thank you!