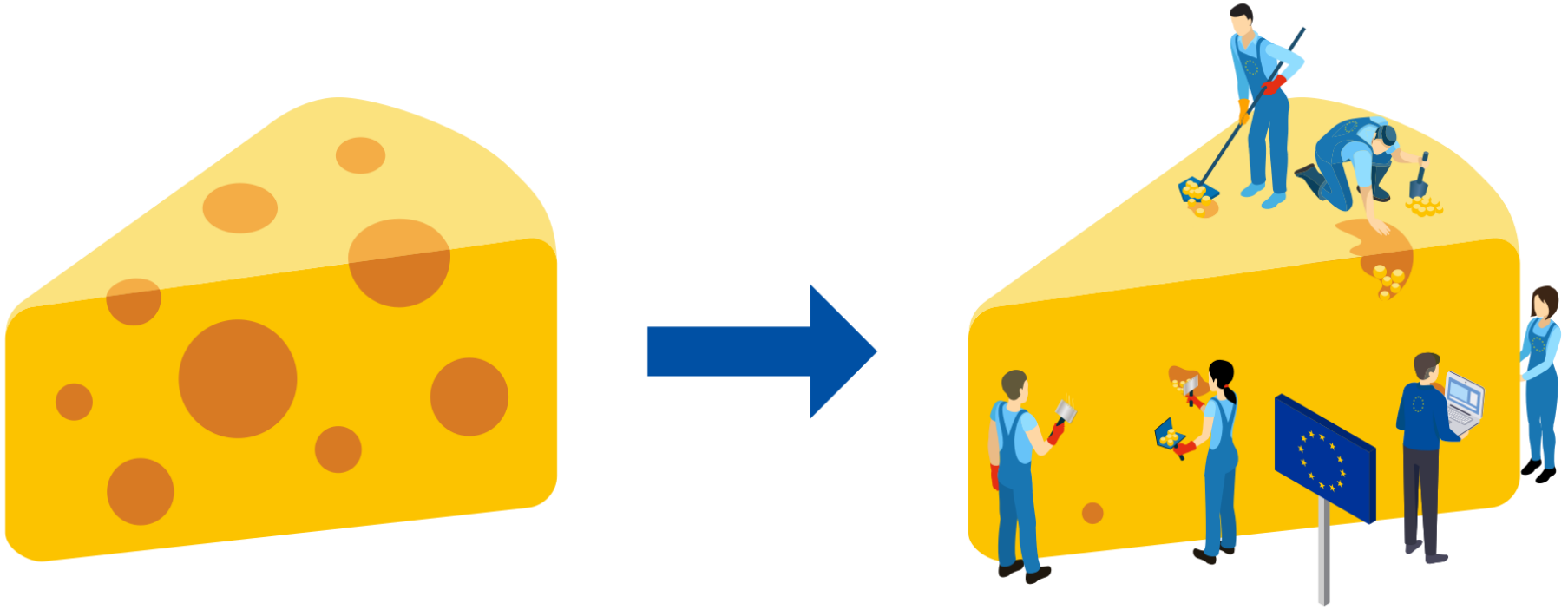
Cyber Resilience Act

CNECT.H2

European Commission, DG CONNECT

CRA in a nutshell



European Commission

Main elements of the law

- **Cybersecurity rules** for the placing on the market of hardware and software
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the life cycle
- Harmonised **standards** to follow
- **Conformity assessment –** differentiated by level of risk
- **Reporting** obligations
- **Market surveillance and enforcement**

In scope: “products with digital elements”

✓ **Hardware products** (including components placed on the market)
(laptops, smart appliances, mobile phones, network equipment or CPUs…)

✓ **Software products** (including components placed on the market)
(operating systems, word processing, games or mobile apps, software libraries…)

…including their **remote data processing solutions**!

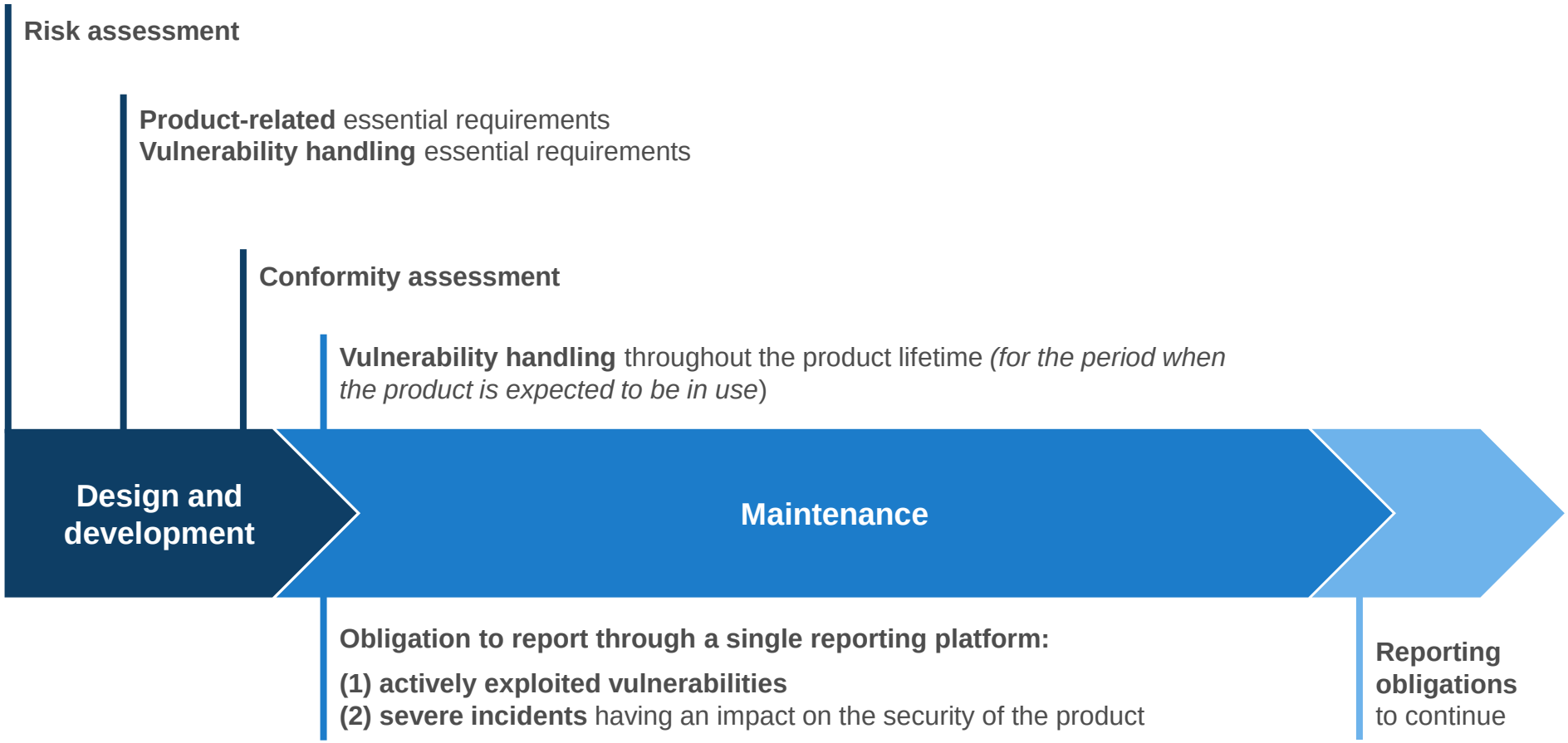
Outside the scope

✗ **Non-commercial products**
(hobby products)

✗ **Services, in particular standalone SaaS** (covered by NIS2)
(websites, purely web-based offerings…)

✗ **Outright exclusions**
(cars, medical devices, in vitro, certified aeronautical equipment, marine equipment)

Obligations of manufacturers



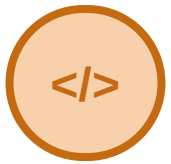
European Commission

Conformity assessment – risk categorisation

Default category — self-assessment
(memory chips, mobile apps, smart speakers, computer games...)

Important products — application of standards/third-party assessment
(operating systems, anti-virus, routers, firewalls…)

Critical products — in the future potentially certification
(smart cards, secure elements, smart meter gateways…)



FOSS — self-assessment (unless categorized as “critical products”)
(web development frameworks, operating systems, database management systems…)

CRA implementation underway

- Development of harmonised standards
- Technical descriptions of important and critical products
  - *To be adopted by 11 December 2025*
- Terms and conditions for CSIRTs to withhold notifications
  - *To be adopted by 11 December 2025*
- Single Reporting Platform by ENISA
  - *To be operational by 11 September 2026*

CRA implementation underway - continued

- Guidance to support implementation
  - *Covering at least RDPS, OSS, support period, interplay with other Union legislation, substantial modification + targeting SMEs*
- Member States to set up notifying & market surveillance authorities
- CRA Expert Group
  - First meeting on 12 February; additional fora for involvement

CRA implementation – SME support

- Support measures in Art. 33 – may include:
  - Member States to organise awareness-raising & support testing and conformity assessment activities
  - Regulatory sandboxes
  - Empowerment for simplified technical documentation
- Support under Digital Europe Programme

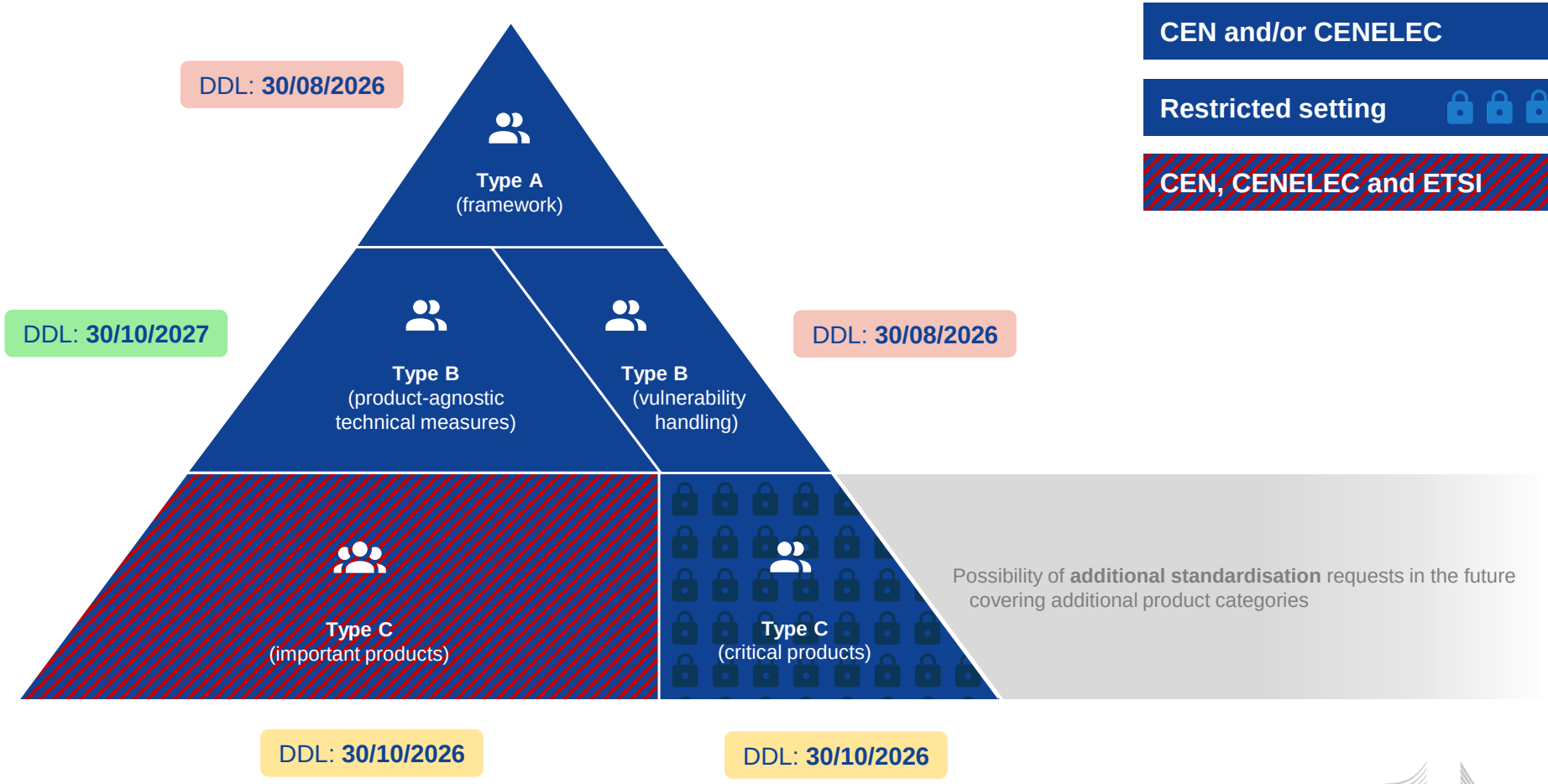
Standardisation

- Standardisation request for harmonised standards adopted by COM and notified to ESOs
- Building on existing international and European standards
- 2-tiered approach: horizontal and vertical standards
- Prioritising important/critical products (CRA Annex III/IV)
- First building blocks for product security ecosystem of standards

Deliverables requested

- **Horizontal standards (1-15)**
  - Risk-based approach (CRA Annex I)
  - Essential Requirements (CRA Annex I part 1)
  - Vulnerability Handling (CRA Annex I part 2)
- **Vertical standards (16-41)**
  - Important products class 1 (CRA Annex III)
  - Important products class 2 (CRA Annex III)
  - Critical products (CRA Annex IV)

CRA standardisation request in a nutshell



European Commission

Thank you.

European Commission