

Cyber Resilience Act (CRA)

CNECT.H2

European Commission, DG CONNECT

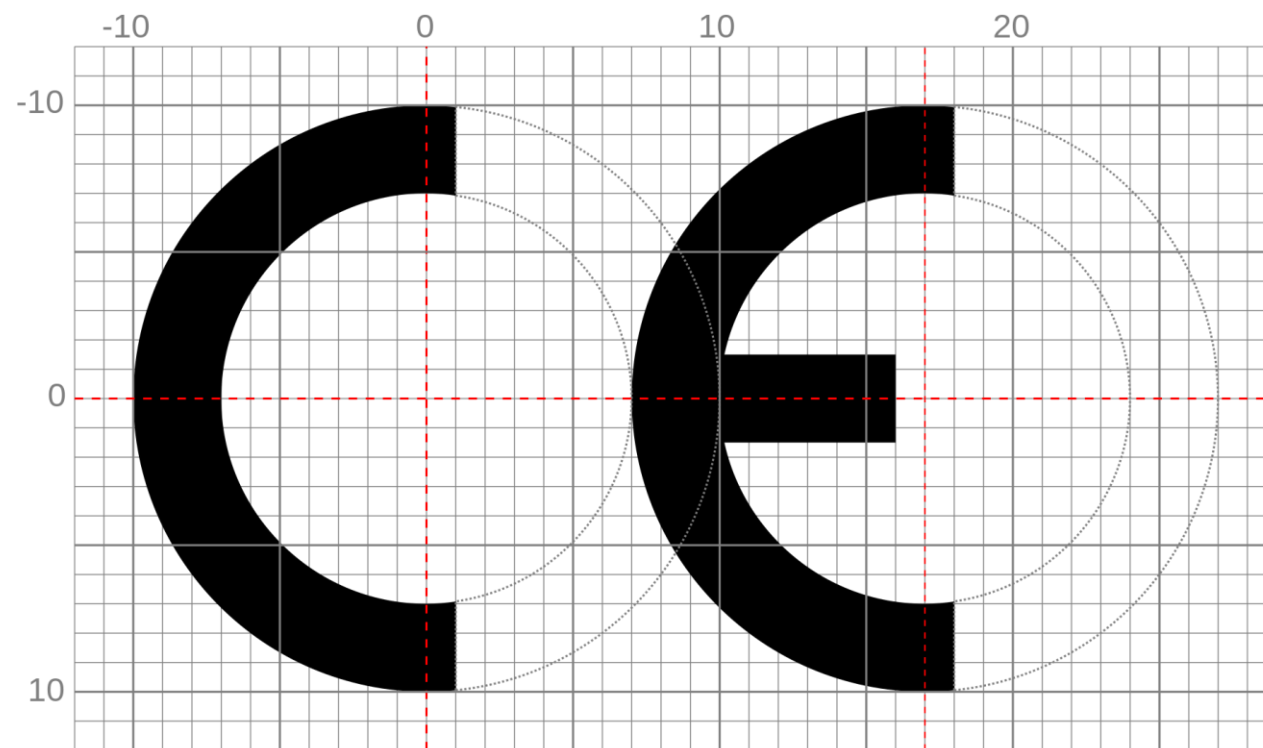
CRA in a nutshell



Main elements of the law

- ❖ **Cybersecurity rules** for the making available on the market of hardware and software
- ❖ **Obligations** for manufacturers, importers and distributors
- ❖ Cybersecurity **essential requirements** across the life cycle
- ❖ **Conformity assessment** – differentiated by product category
- ❖ **Reporting** obligations
- ❖ **Market surveillance and enforcement**
- ❖ **Entry into application: 11 December 2027**
except for reporting obligations: 11 September 2026

CE marking



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)

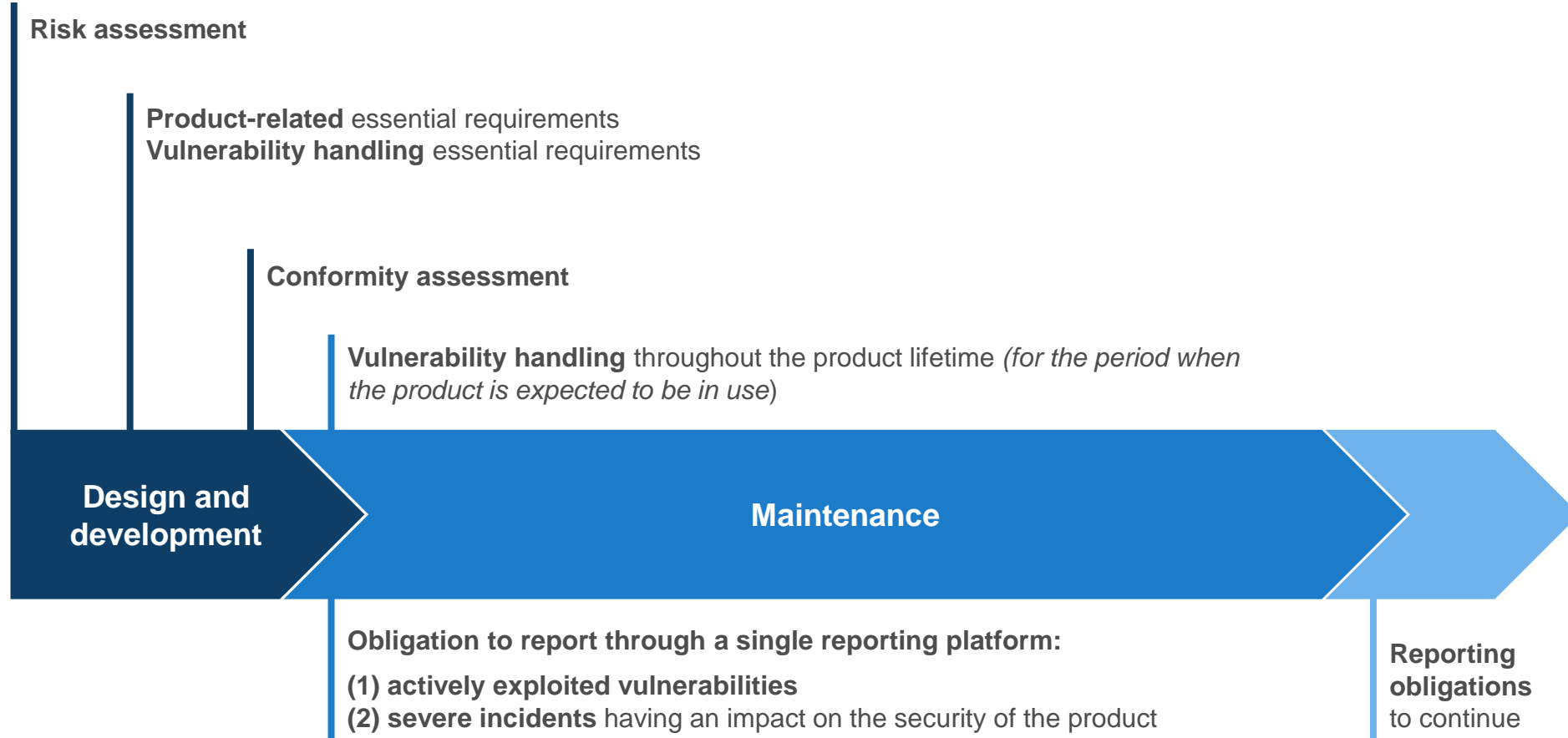
(websites, purely web-based offerings...)



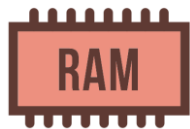
Outright exclusions

(cars, medical devices, in vitro, certified aeronautical equipment, marine equipment)

Obligations of manufacturers



Conformity assessment – product categorisation



Default category — self-assessment

(memory chips, mobile apps, smart speakers, computer games...)



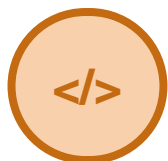
Important products — application of standards/third-party assessment

(operating systems, anti-virus, routers, firewalls...)



Critical products — in the future potentially certification

(smart cards, secure elements, smart meter gateways...)



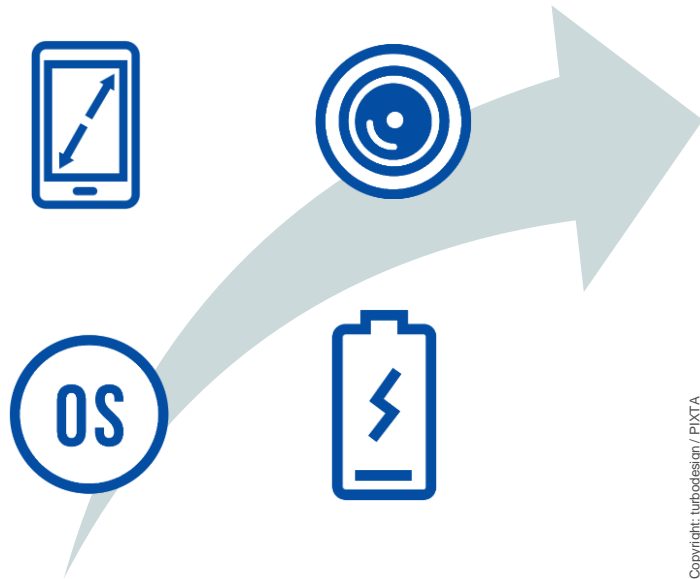
FOSS — self-assessment (unless categorized as “critical products”)

(web development frameworks, operating systems, database management systems...)

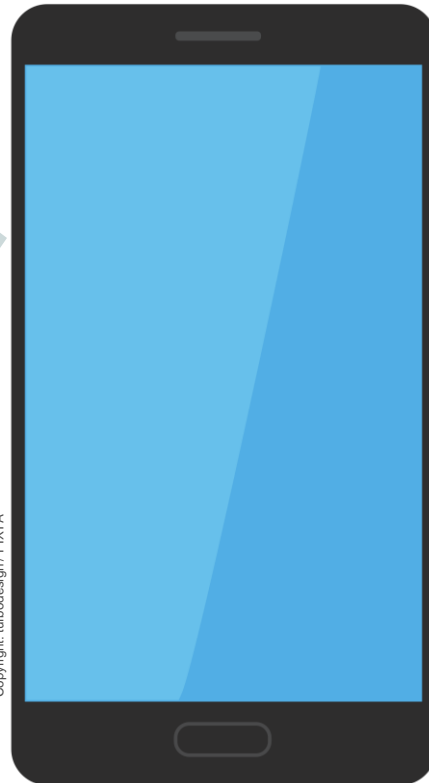
A simplified example of smartphones

As a rule, whoever places on the market a **“final” product or a component** is required to comply with the **essential requirements**, undergo **conformity assessment** and affix the **CE marking**.

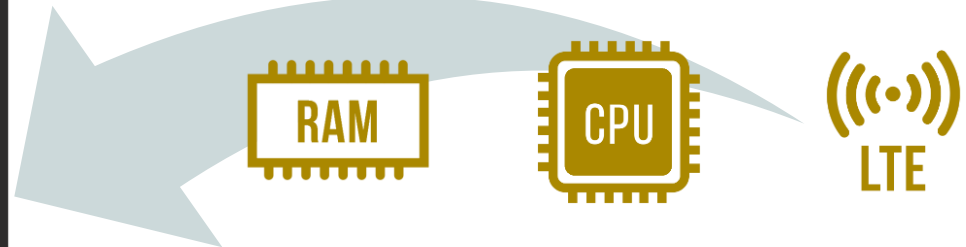
Developed by the manufacturer
placing the smartphone on the market:



Copyright: turbodesign / PIXTA



Developed by upstream manufacturers
for integration into the “final” product:



Deliverables requested

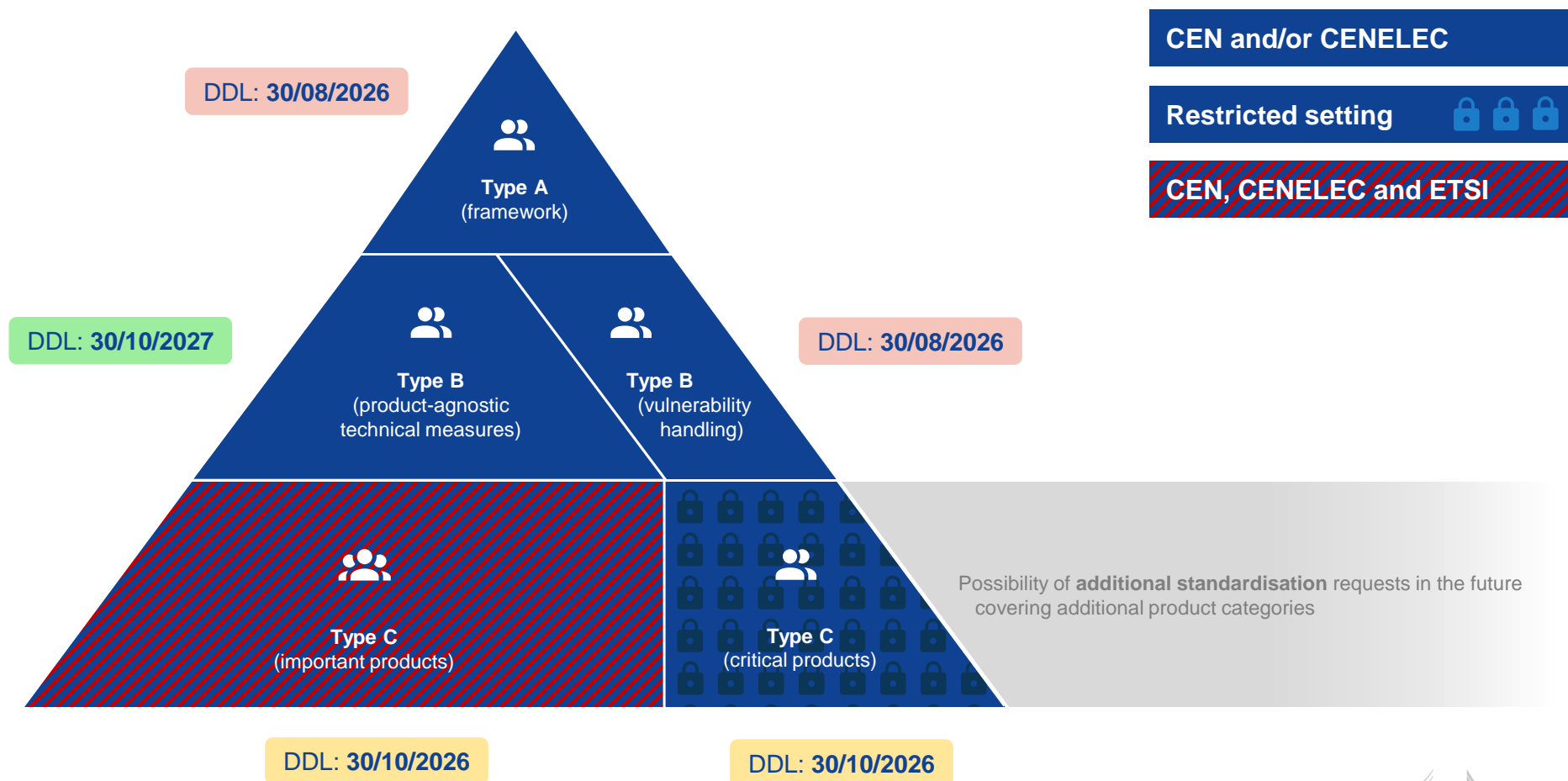
❖ **Horizontal standards (1-15)**

- ❖ 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





EUCC

CNECT.H2

European Commission, DG CONNECT

EUCC at a Glance

- ❖ **Voluntary scheme** under the EU CSA (Regulation (EU) 2019/881)
- ❖ Certification of **ICT products and Protection Profiles**
- ❖ Two assurance levels: **Substantial** (AVA_VAN.1-2) and **High** (AVA_VAN.3-5)
- ❖ Private CABs (ITSEF and CBs) require **accreditation** for Substantial level
- ❖ Both private and public CABs also require **authorisation** for High level
- ❖ CABs are **notified and listed** on the European Commission NANDO website

EUCC at a Glance

- ❖ Certificate **validity**: 5 years
- ❖ Mandatory **monitoring and vulnerability management**
- ❖ CBs issuing High level certificates undergo **Peer Assessment** every 5 yrs
- ❖ **Recognition by the CCRA**, subject to specific conditions
- ❖ Ongoing maintenance of **state-of-the-art and guidance documents**

Presumption of conformity

CNECT.H2

European Commission, DG CONNECT

Presumption of conformity (Article 27 of CRA)

- ❖ Products certified pursuant to a European cybersecurity certification scheme shall be presumed to be in conformity with cybersecurity requirements of the CRA.
- ❖ European Commission empowered to adopt a delegated act to specify which schemes can be used to demonstrate conformity.
- ❖ Presumption of conformity via European harmonised standards also possible.

Thank you.