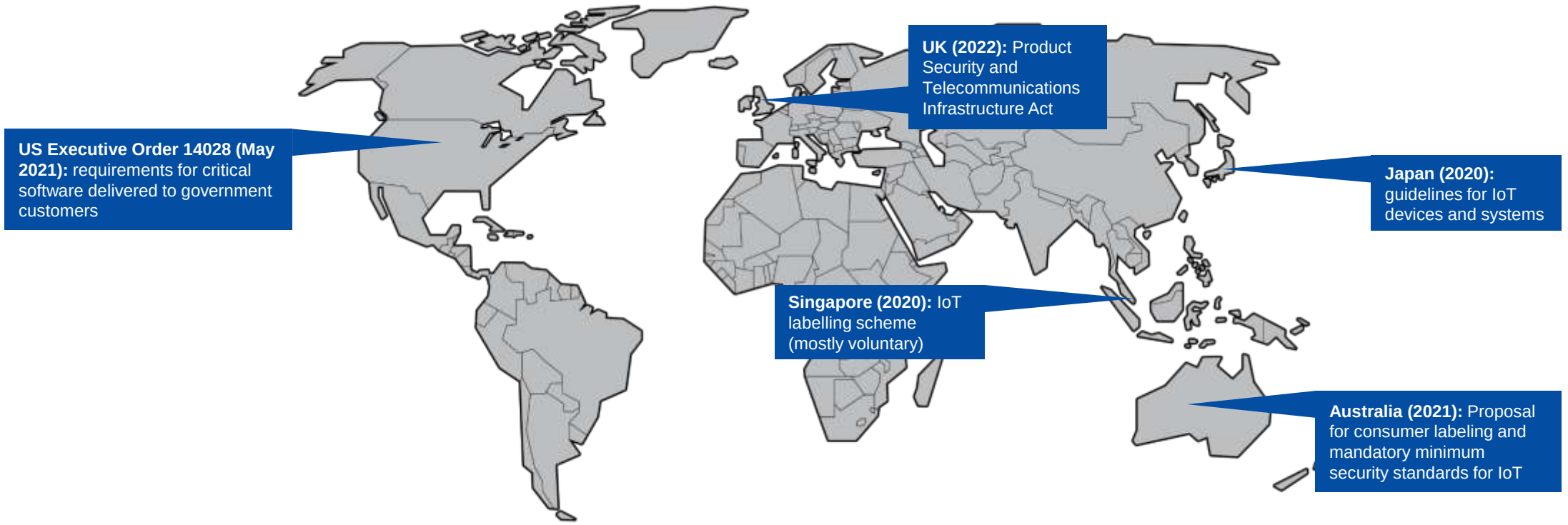
Standards for the Cyber Resilience Act

Filipe Jones Mourao, policy officer

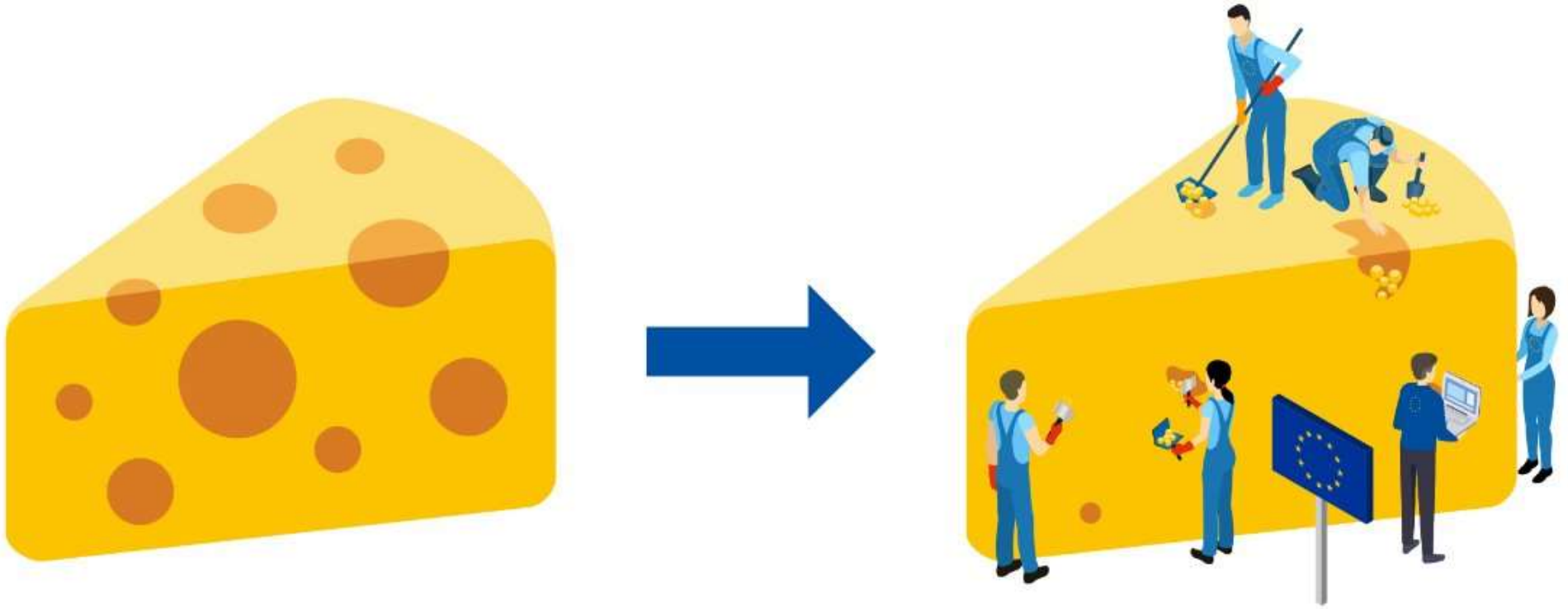
European Commission, DG CONNECT

Global context



European Commission

CRA in a nutshell

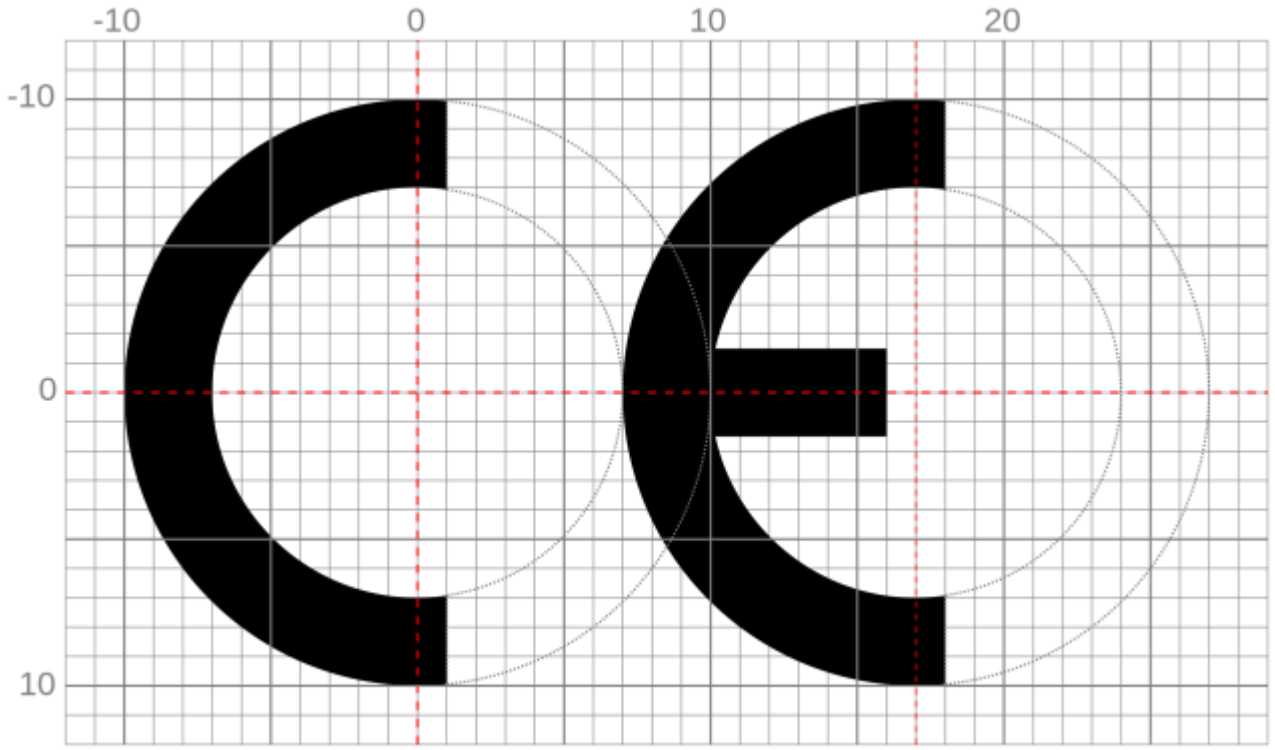


European Commission

Main elements of the proposal

- **Cybersecurity rules** for the placing on the market of hardware and software
- Based on **New Legislative Framework** (well-established EU product-related legislative setting)
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the life cycle
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Market surveillance and enforcement**

CE marking



European Commission

Scope

Products with digital elements:

- ✚ **Hardware products** and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs
- ✚ **Software products** and components placed on the market separately, such as operating systems, word processing, games or mobile apps
- ⓘ The definition of **“products with digital elements”** also includes **remote data processing solutions.**

Not covered:

- ✖ **Non-commercial projects, including open source** in so far as a project is not part of a commercial activity
- ✖ **Services, in particular standalone Software-as-a-Service** – *covered by NIS2*

Outright exclusions:

- ✖ **Certain products sufficiently regulated on cybersecurity** (cars, medical devices, *in vitro*, certified aeronautical equipment, marine equipment)

European Commission

Approach to open-source

- Only **directly monetised** open-source products subject to full set of obligations
- Introduction of the **open-source software steward**:

  Light-touch approach for organisations that do not directly monetise but support on a sustained basis the development of specific open-source products intended for commercial activities.
- **Possibility of self-assessment** for open-source products, irrespective of whether they are considered important products or not
- **Obligation for integrators** to provide maintainers of open-source components with available fixes.

Obligations of manufacturers

Assessment of the risks associated with a product

(1) Product-related essential requirements (Annex I, Part I)
(2) Vulnerability handling essential requirements (Annex 1, Part II)
(3) Technical file, including information and instructions for use (Annex II + V)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product lifetime (Annex I, Part II)

Design and development phase

Maintenance phase

Obligation to report through a single reporting platform:

(1) actively exploited vulnerabilities
(2) incidents having an impact on the security of the product

Reporting obligations to continue

European Commission

Cybersecurity Essential Requirements

Properties of products

- No known exploitable vulnerabilities
- Security updatability (automatic)
- Access control (authentication)
- Confidentiality, Integrity, Accessibility (encryption)
- Data minimisation (intended purpose)
- Resilience of functions (DDoS)
- Reduce attack surface (interfaces)
- Reduce impact of incident (mitigation)
- Monitoring and logging (opt-out)
- Secure erasure

Vulnerability handling

- Identify components (SBOM)
- Document vulnerabilities
- Mitigate without delay
- Regular test and review
- Publicly disclose information once fixed
- Coordinated vulnerability disclosure
- Share information on potential vulnerabilities
- Securely distribute updates
- Disseminate updates free of charge

Software Bill of Materials in the CRA

- **Manufacturers to draw up a SBOM** in a commonly used format covering at the very least the top-level dependencies of the product
- **No requirement** to make the SBOM publicly available
- SBOM to be included in the **technical documentation** and, upon request, to be provided to **market surveillance authorities**
- **Commission empowerment** to specify the format and elements (international standards to be relied upon)

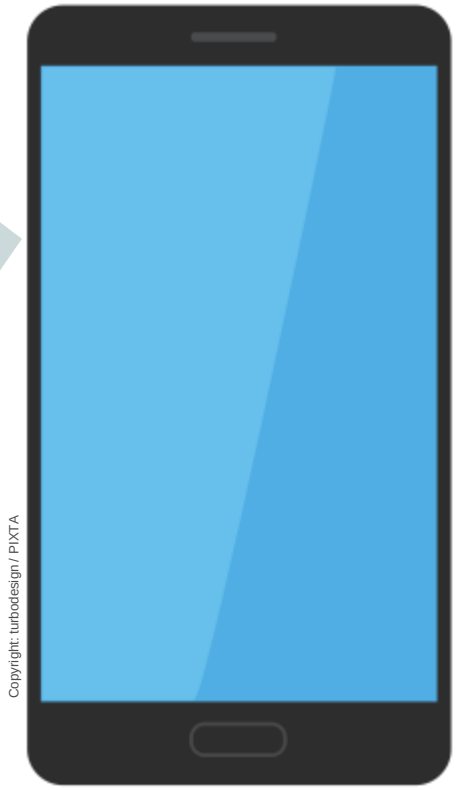
Conformity assessment – risk categorisation

- **Default category (more than 90%):** The vast majority of products will be subject to self-assessment (examples: photo editing, word processing, smart speakers, hard drives, games etc.)
- **Important products (less than 10%):** A small group of critical products listed in the Annex will be subject to *more stringent conformity assessment procedures*, including assessment by an independent third party (examples: firewalls, routers, hypervisors etc.)
- **Critical products:** To future-proof the CRA, the Commission is empowered to adopt secondary legislation requiring *mandatory certification* based on EU cybersecurity certification schemes (Cybersecurity Act) of certain products posing a particularly high risk, such as smart cards.

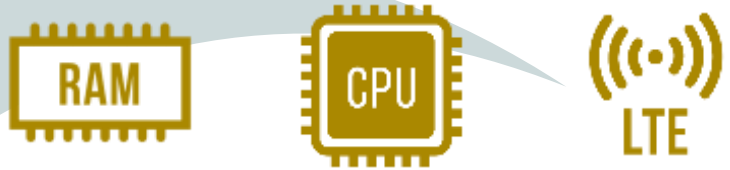
A simplified example of smartphones

*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:



Developed by upstream manufacturers for integration into the "final" product:



Placed on the market separately for users to buy and integrate:

European Commission

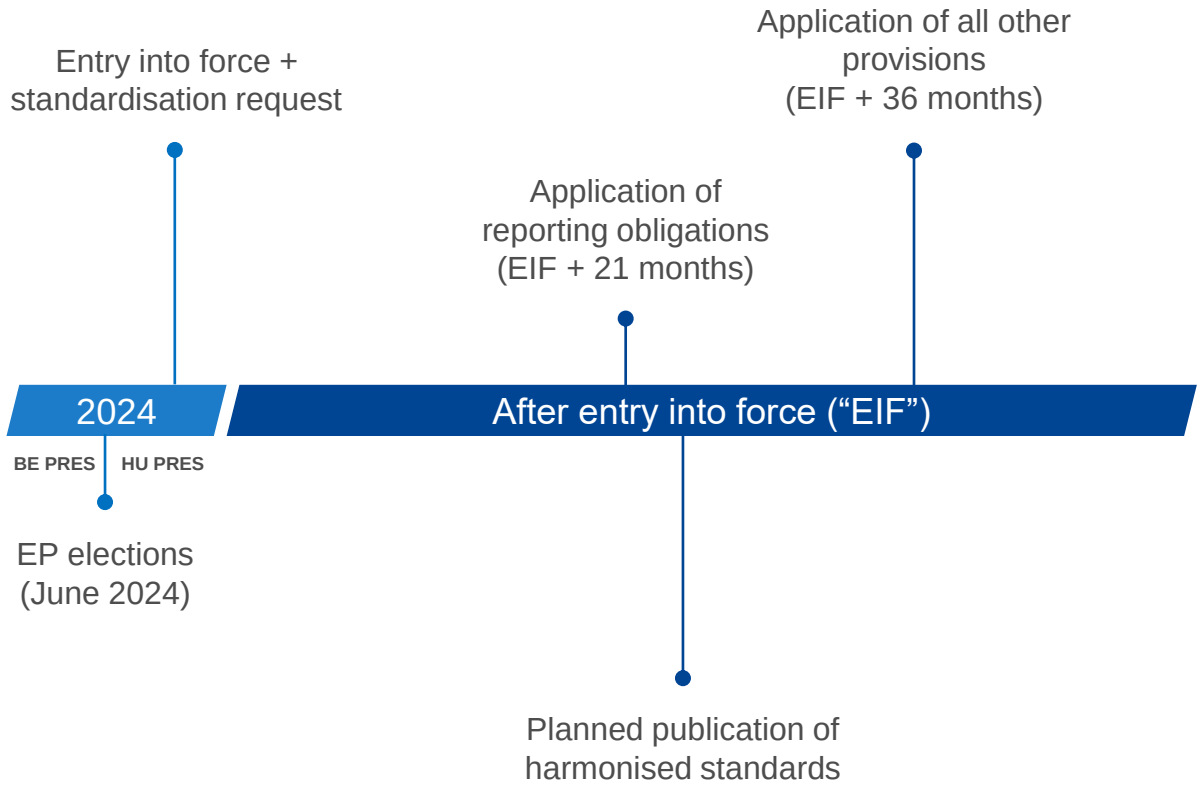
Market surveillance powers and sanctions

- Tools for checks at the disposal of market surveillance authorities (MSAs): documentary checks, requests for information, inspections, laboratory checks etc.
- **When non-compliance found**, MSAs have powers to:

  1) require **manufacturers to bring non-compliance to an end** and eliminate risk;
  2) to **prohibit/restrict the making available** of a product or to order that the product is **withdrawn/recalled**;
  3) impose **penalties** (including fines up to 15 000 000 EUR or up to 2.5 % of worldwide turnover).

- In exceptional circumstances, COM may require ENISA to conduct an evaluation and, based on the results, establish a **corrective or restrictive measure is necessary at Union level** via an Implementing Act (and following MS consultations).

Tentative timeline



Draft Standardisation Request
in support of the

Cyber Resilience Act

European Commission, DG CONNECT

Results of gap analysis

- No single standard covers all the requirements
- For each of the defined requirements there is already at least one reference document
- Good cybersecurity standardisation base is in place
- Harmonisation is needed to ensure a homogeneous horizontal coverage
- Some gaps need to be addressed

Draft Standardisation Request

- **Policy-based Standardisation Request**
  - Aim to gain time and allow technical discussions to start as soon as feasible
  - Amend the Request once CRA is finally adopted

- **Targeted stakeholder consultations**
  - ESOs, Annex III orgs.
  - Expert Group: Multi-stakeholder Platform on ICT standardisation

Draft Standardisation Request

- **Proposed approach:**
  - Building on existing international standards and work done for RED DA (“horizontal” approach)
  - 2-tiered approach with horizontal and vertical standards, prioritising important / critical products (CRA Annex III).
  - Possible inspiration: machine safety Type A, B, C standards
  - 41 European standards plus supporting deliverables (if any)
  - First building blocks for product security ecosystem of standards

Next steps

- Public notification of CRA SR (open until 16 May 2024)
- Possible Action Grant to support NSBs and ESOs
- Adoption of request, acceptance, start of development
- Policy-based SR to be amended once CRA is fully adopted
- **Medium term:** market-led development of more product-specific standards (type C), to propose to COM for harmonisation

Thank you.

European Commission