Cyber Resilience Act proposal

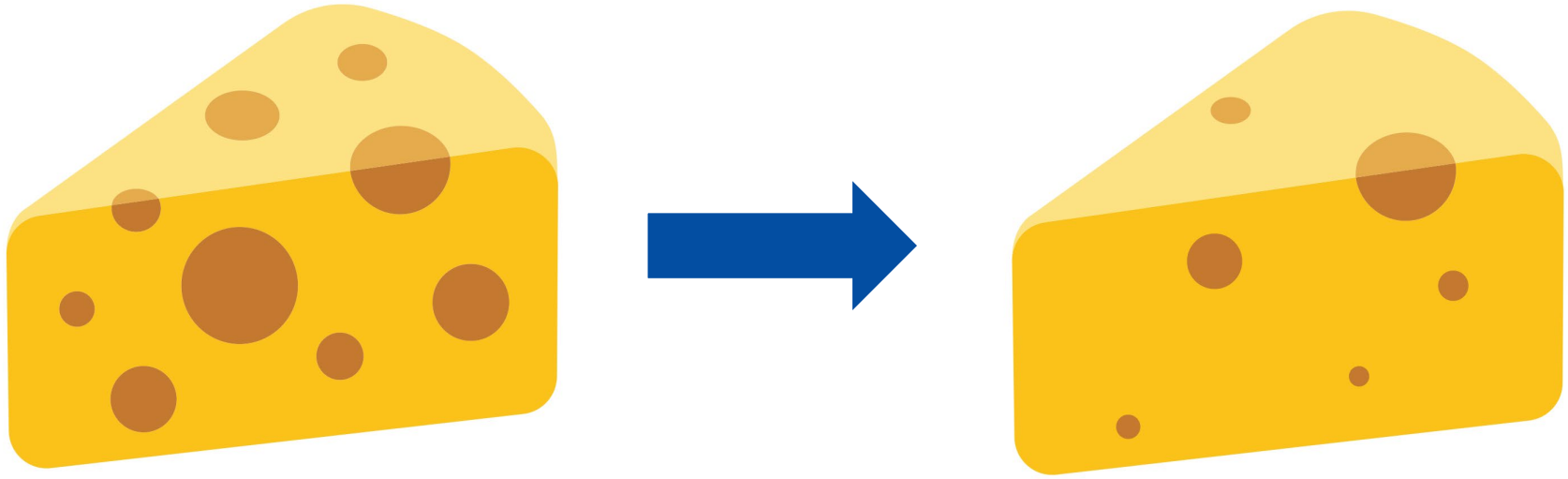
Securing digital products in the EU market

26 January 2023, Cybersecurity Policy Conference, Brussels

Raluca Stefanuc, Team Leader

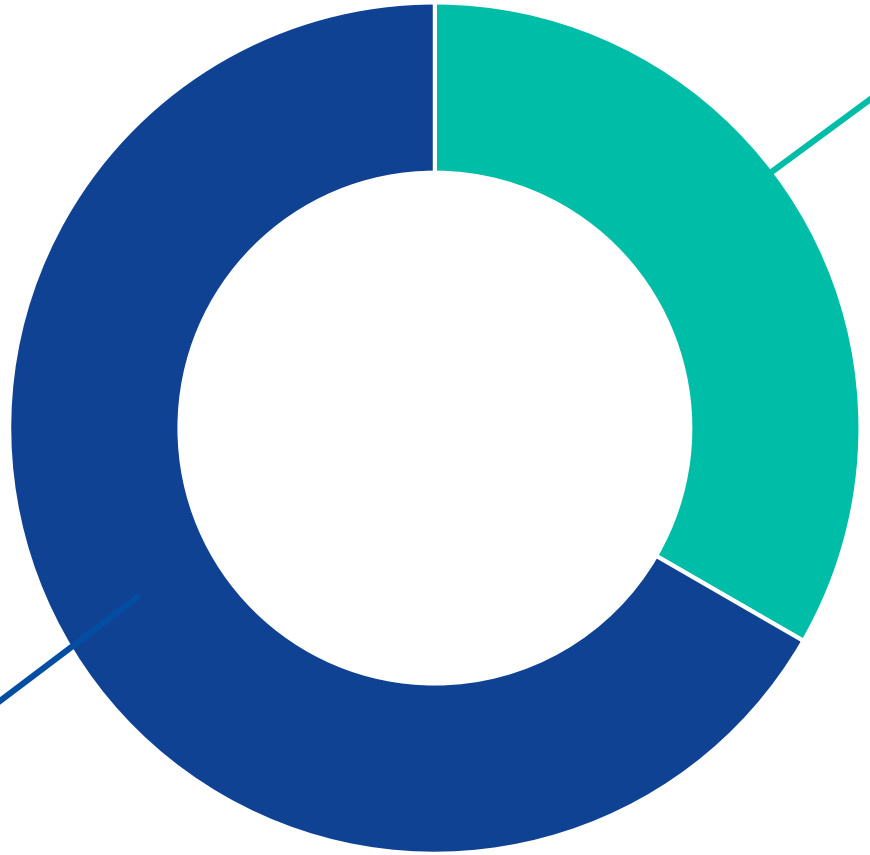
European Commission, DG CONNECT, Unit H2

Cyber Resilience Act (CRA) in a nutshell



European Commission

Role of vulnerabilities in NIS incidents



Other causes
(such as phishing, credential theft etc.)

Two thirds of NIS incidents are the result of a vulnerability exploitation.

Source: ENISA/Gartner (2022)

European Commission

Main elements of the CRA 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 (5 years)
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Market surveillance and enforcement**

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 cloud/Software-as-a-Service** – *covered by NIS2*

Outright exclusions:

- ✖ **Certain products sufficiently regulated on cybersecurity** (cars, medical devices, *in vitro*, certified aeronautical equipment) under the new and old approach

Obligations of manufacturers

Assessment of the risks associated with a product

(1) Product-related essential requirements (Annex I, Section 1)
(2) Vulnerability handling essential requirements (Annex 1, Section 2)
(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 life time (Annex I, Section 2)

Design and development phase

Maintenance phase
(5 years or across product lifetime, whichever is shorter)

Obligation to report to the EU Cybersecurity Agency (ENISA) within 24 hours:

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

Reporting obligations to continue

European Commission

Product-related essential requirements

1. Appropriate level of security based on the risks
2. Products to be delivered without known exploitable vulnerabilities
3. Based on the risk assessment and where applicable:
    - Security **by default**
    - Protection from **unauthorised access**
    - **Confidentiality** and **integrity of data**, commands and programs
    - **Minimisation** of data
    - Availability of **essential functions**
    - Minimise **own negative impact** on other devices
    - Limit **attack surfaces**
    - Reduce **impact of an incident**
    - **Record and monitor** security relevant events
    - Enable adequate **security updates**

Vulnerability handling requirements

- **Identify and document dependencies** and vulnerabilities, including **SBOM**
- No known vulnerabilities and **address vulnerabilities** without delay
- **Test the security** of the digital product
- Publically **disclose information** about fixed vulnerabilities
- **Coordinated vulnerability disclosure** policy
- Facilitate the **sharing of information** about potential vulnerabilities
- Mechanisms allowing the **secure updating**
- Patches are delivered **without delay**, **free of charge** and with **advisory messages**

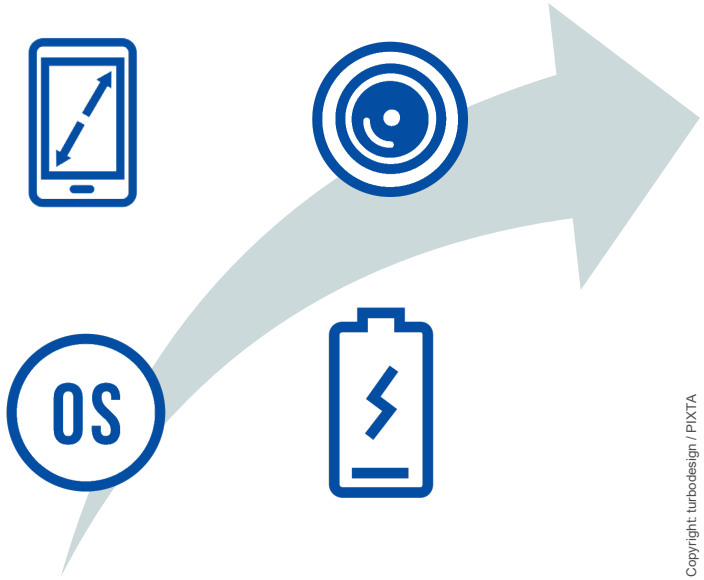
Information and instructions

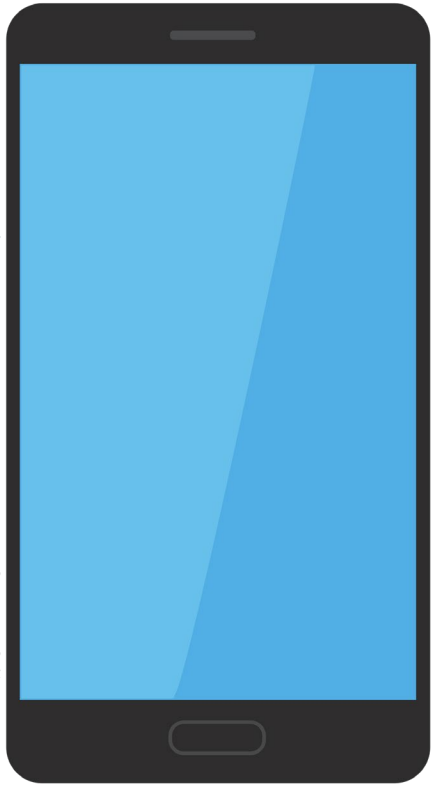
- **CE marking**
- **Contact** information for reporting vulnerabilities
- **Intended use**, including the security environment foreseen
- Security **properties** of the product
- Where the **SBOM** can be accessed (if publicly available)
- EU **Declaration of Conformity**
- Type of **support offered** by the manufacturer and for how long
- Instructions on **secure use** and secure removal of data

A simplified example of smartphones

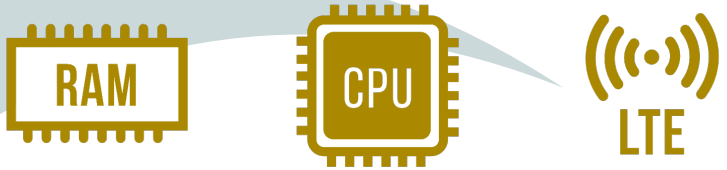
*As a rule, whoever places on the market a **"final" product or a component** is required to comply with the **essential requirements**, undergo **conformity assessment** and affix the **CE marking.***

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

Conformity assessment – risk categorisation

90% of products	10% of products		
Default category	**Critical "Class I"**	**Critical "Class II"**	**Highly critical**
Self-assessment	**Application of a standard or third party assessment**	**Third party assessment**	**Mandatory EU certification**
Criteria: **n/a**	**Criteria:** • **Functionality** (e.g. critical software) • **Intended use** (e.g. industrial control/NIS2) • **Other criteria** (e.g. extent of impact)		**Additional criteria:** • Used by **NIS2** entities • Resilience of **supply chain**
	To be amended/specified via delegated acts		
Examples: Photo editing, word processing, smart speakers, hard drives, games etc.	**Examples (Annex III):** Password managers, network interfaces, firewalls, microcontrollers etc.	**Examples (Annex III):** Operating systems, industrial firewalls, CPUs, secure elements etc.	**Examples:** **n/a** (empowerment to future-proof the CRA)

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, the European Commission may require the EU Cybersecurity Agency (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 consultations with Member States).

Timeline and adoption process

- The European Commission **proposal** published on 15 September 2022: [available here: Cyber Resilience Act | Shaping Europe's digital future (europa.eu)].
- **Co-decision procedure ongoing with co-legislators**: the European Parliament and the Council (Member States).
- Transition period proposed by the European Commission for the main obligations: 2 years (from entry into force until these obligations start applying) + grandfathering clause.
- Transition period proposed by the European Commission for the reporting obligations (Article 11 of the proposal): 1 year (from entry into force until these obligations start applying).

Thank you.

European Commission