Cyber Resilience Act

22.11.2022

Christiane Kirketerp de Viron
European Commission, DG CONNECT

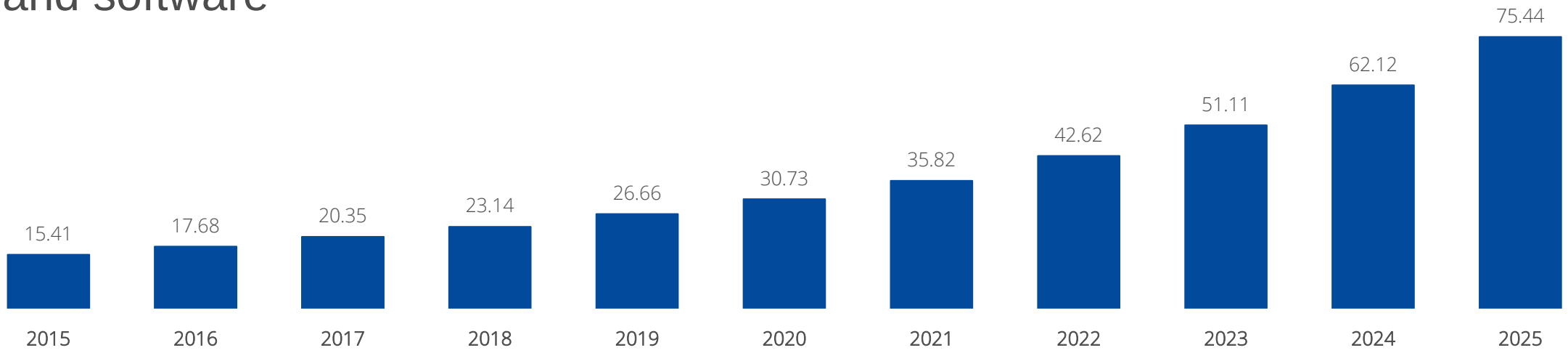
If everything is connected, everything can be hacked.

(SOTEU address, 15 September 2021)

European Commission

Everything is connected

- Large majority of vulnerabilities exploitable **over the Internet**
- **Impact assessment: no incentives** to produce secure by design hardware and software



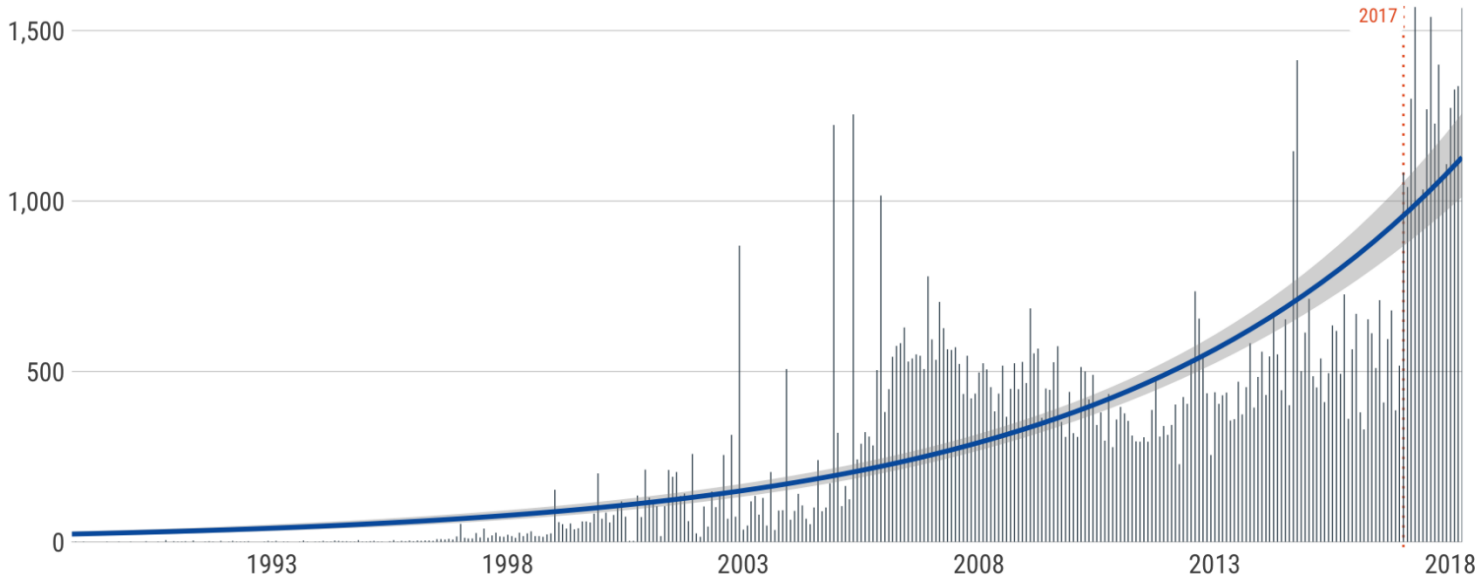
Internet of Things devices worldwide from 2015 to 2025 (in billions)

Source: Forbes/IHS

European Commission

Discovered vulnerabilities increasing

- **70% of Windows** systems have at least one open vulnerability with known exploits.
- **63% of mobile applications** contain an average of 39 known vulnerabilities in open source components.
- **57% of IoT devices** are vulnerable to medium- or high-severity attacks.



Number of CVE (Common Vulnerabilities and Exposures) per month

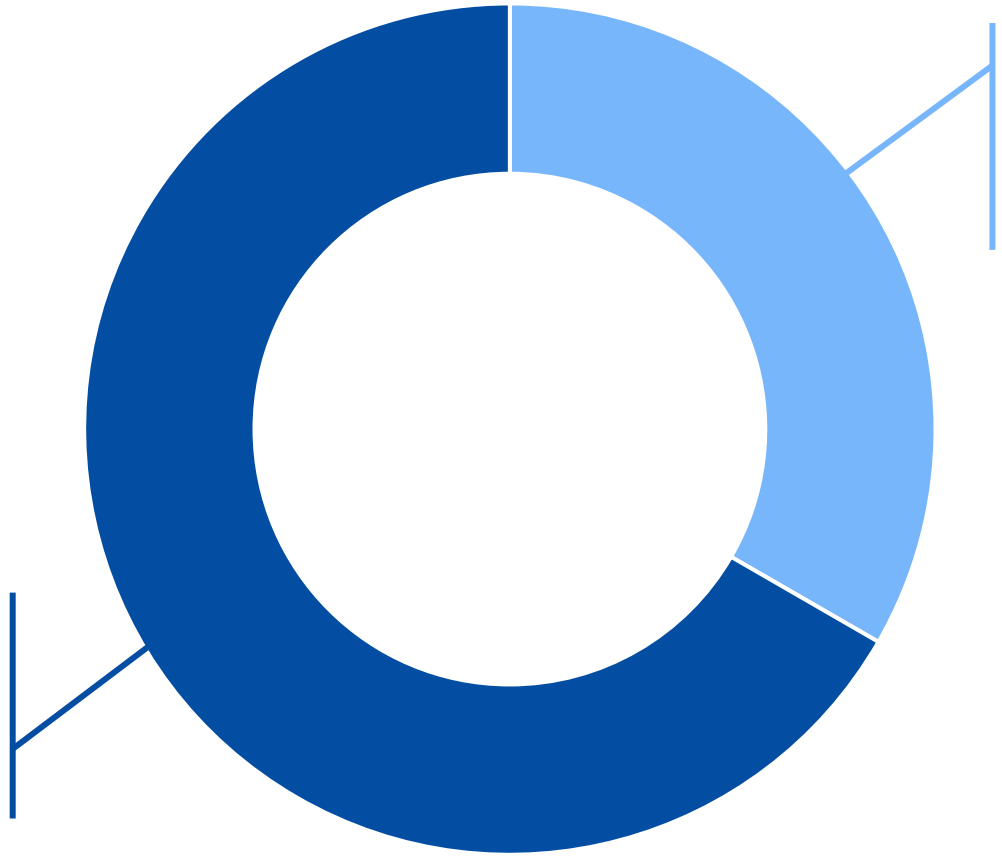
Sources: Kenna Security, Synopsis, Palo Alto Networks, Rapid7

European Commission

Noteworthy examples

- **“WannaCry” (2017):** North Korean ransomware worm exploiting a Windows vulnerability. Affected 200.000 computers across 150 countries. Damage amounting to billions of USD.
- **Pulse Connect Secure Gateway (since 2020):** By exploiting a vulnerability in the VPN’s gateway, attackers were able to bypass authentication and gain access to the networks of a number of US agencies and critical infrastructures.
- **Kaseya VSA (2021):** A vulnerability in Kaseya’s network administration software was exploited by attackers affecting over 1.000 companies and forcing the supermarket chain Coop to close all its shops across Sweden.
- **Verkada (2021):** A group of hackers has gained access to the footage of Verkada cameras deployed in organisations, such as Tesla’s warehouses and factories, Cloudflare’s offices, health clinics and psychiatric hospitals.

Role of vulnerabilities in NIS incidents



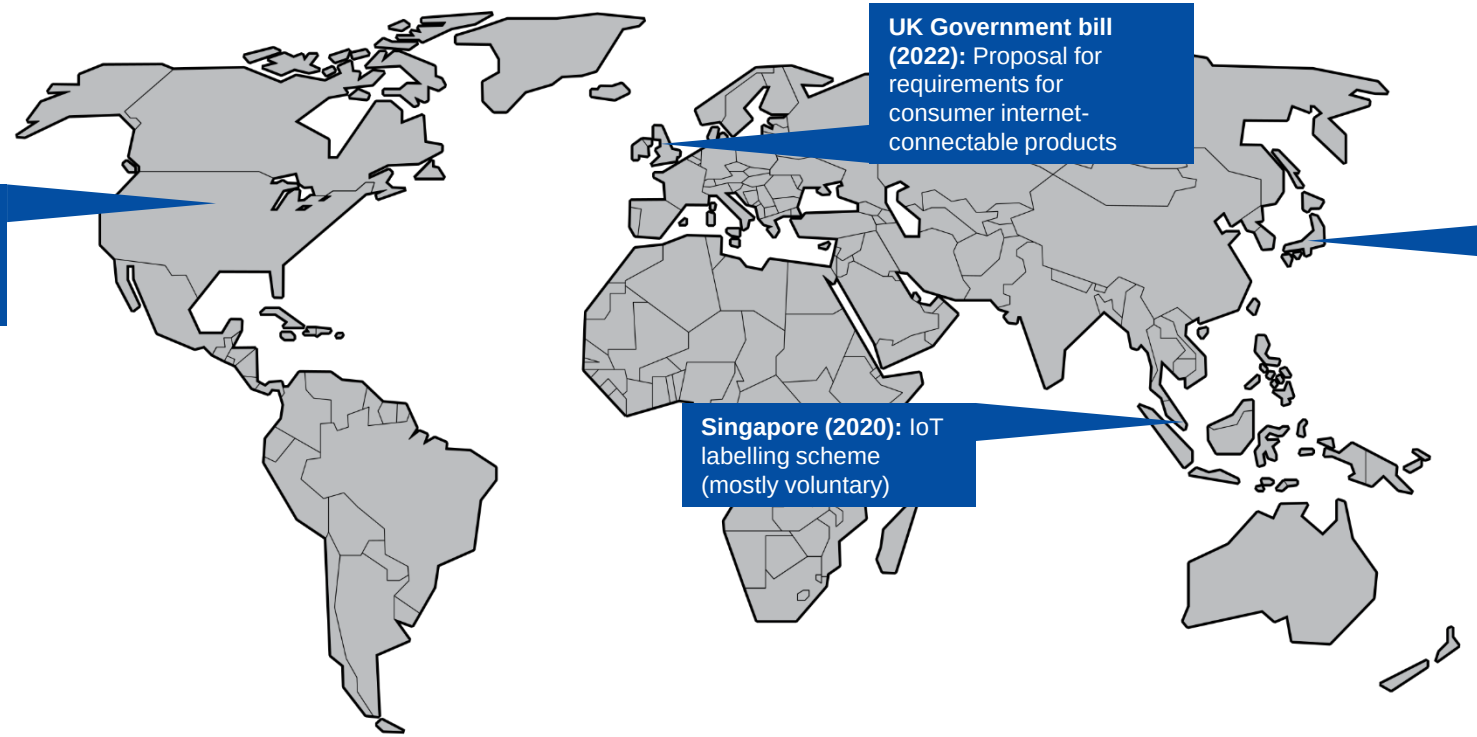
Other causes
(such as phishing, credential theft etc.)

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

Source: ENISA/Gartner (2022)

European Commission

Third-country initiatives



US Executive Order 14028 (May 2021): requirements for critical software delivered to government customers

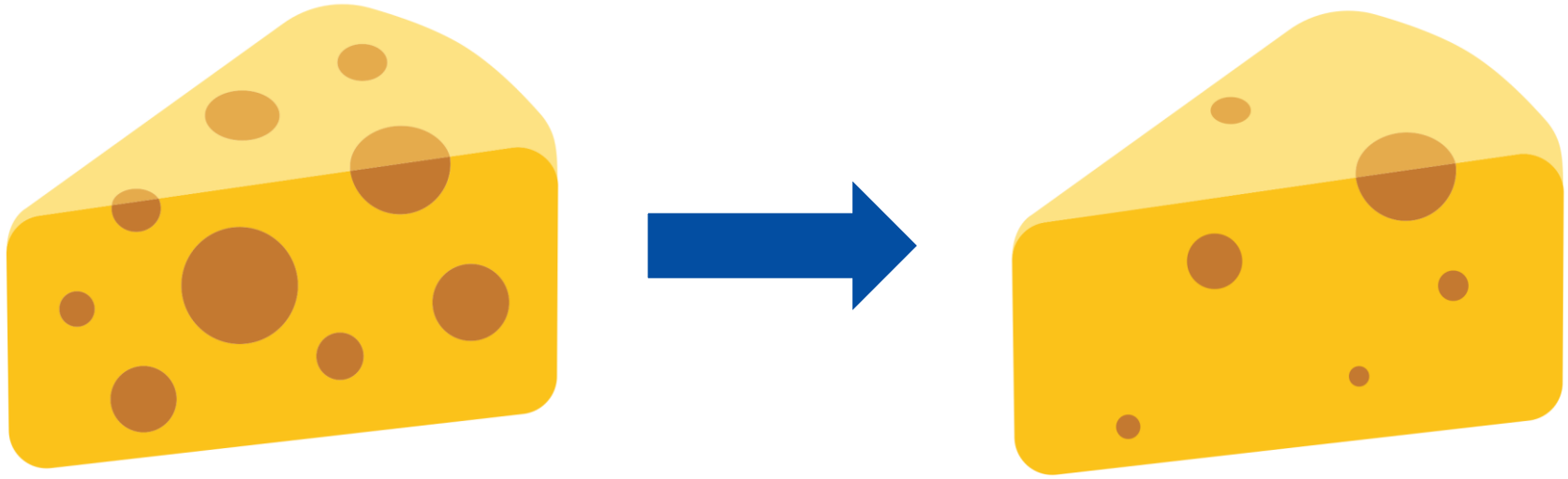
UK Government bill (2022): Proposal for requirements for consumer internet-connectable products

Japan (2020): guidelines for IoT devices and systems

Singapore (2020): IoT labelling scheme (mostly voluntary)

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 (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.**

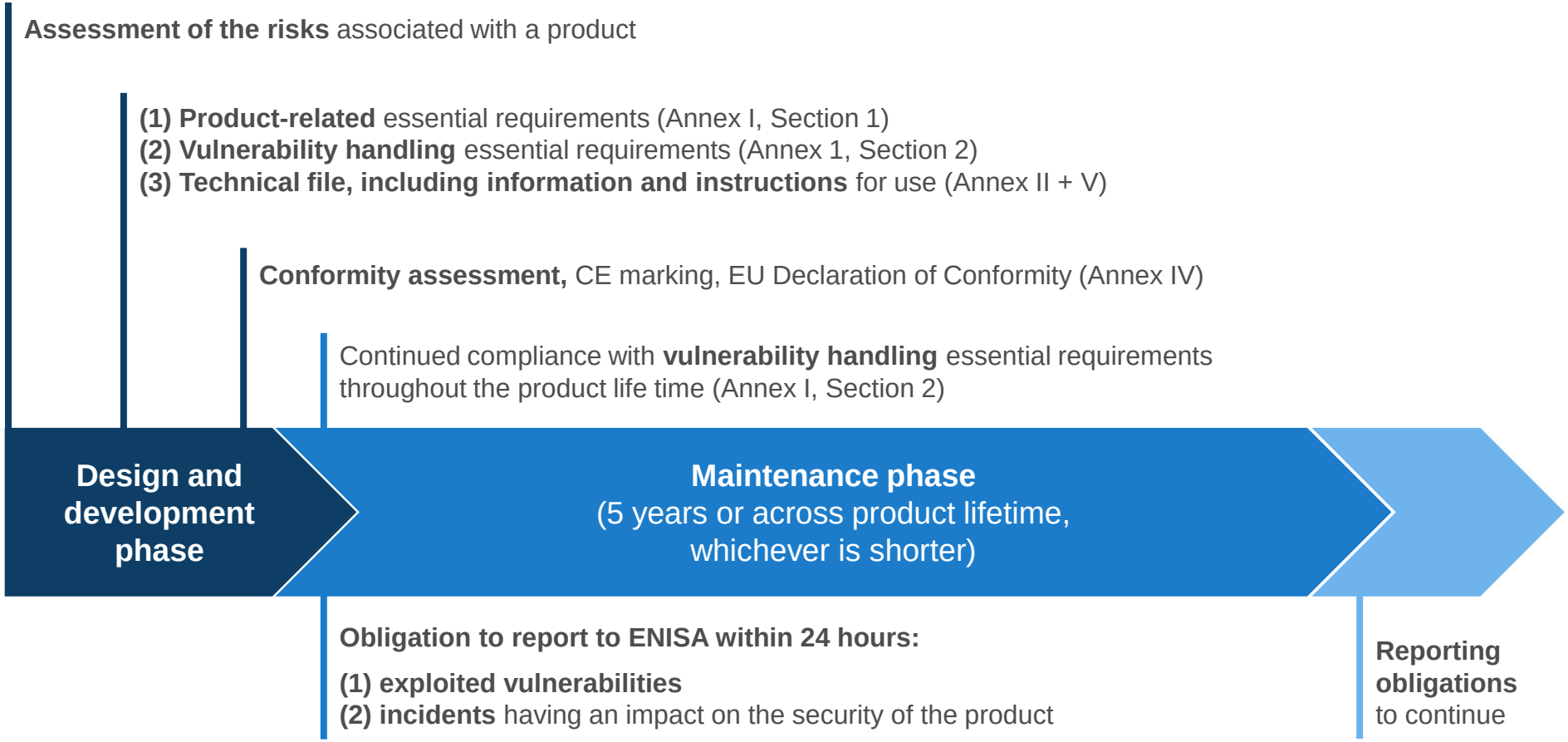
Not covered:

- ✖ **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



European Commission

Product-related essential requirements

1. Appropriate level of security
2. Products to be delivered without known vulnerability
3. Based on the risk 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**

Example

2. *Products with digital elements shall be delivered **without any known exploitable vulnerabilities**;*

- **Security (2020):** Almost 50 % of manufacturers knowingly place products with digital elements on the marked that contain vulnerabilities.
- **ENISA/Gartner (2022):** Two-thirds of incidents affecting operators of essential services (NIS) are the result of an exploited vulnerability.

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**

Example

Manufacturers of the products with digital elements shall:

*3) apply **effective and regular tests** and reviews of the security of the product with digital elements;*

- **Piskachev et al (2022):** Only half of German manufacturers use so-called static program analysis tools, even though many of such tools are available free of charge.

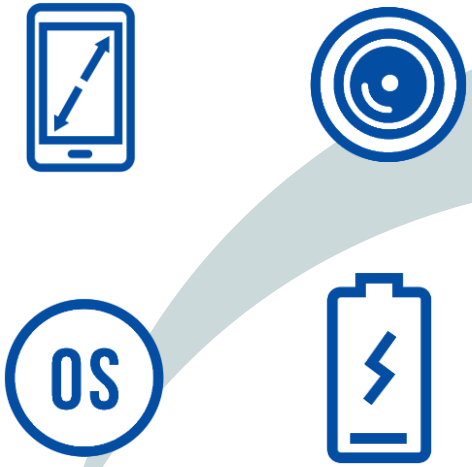
Information and instructions

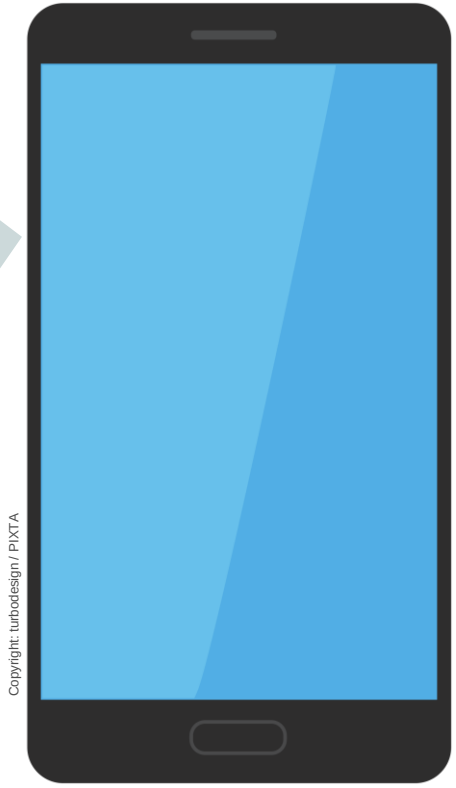
- **CE marking**
- **Contact** information for reporting vulnerabilities
- **Intended use**, including the security environment foreseen
- Security **properties** of the product
- Where the **SBOM** can be accessed (if publicly available)
- EU **Declaration of Conformity**
- Type of **support offered**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

A simplified example of smartphones

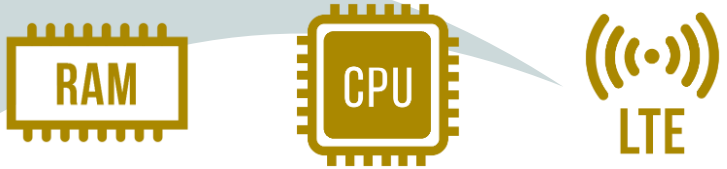
*As a rule, whoever places on the market a **"final" product or a component** is required to comply with the **essential requirements**, undergo **conformity assessment** and affix the **CE marking.***

Developed by the manufacturer placing the smartphone on the market:





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



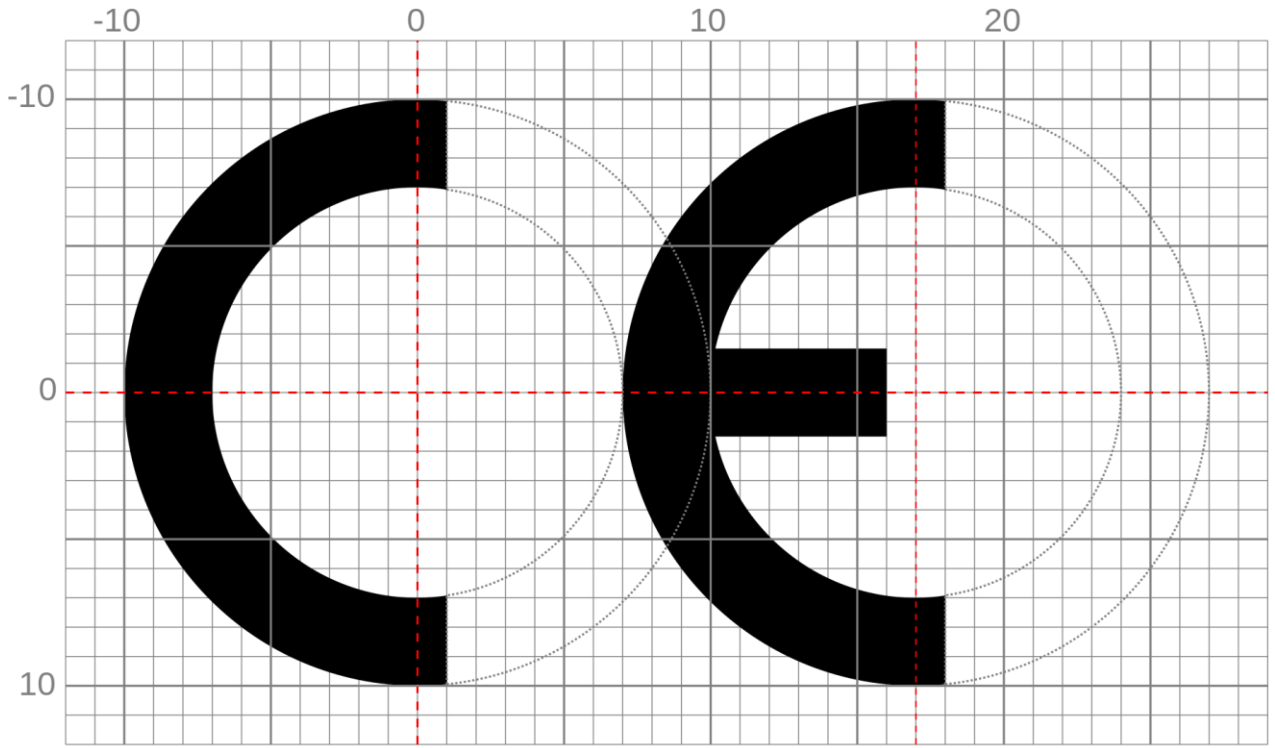
Placed on the market separately for users to buy and integrate:

European Commission

Which conformity assessment to follow?

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)

CE marking



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).

Costs and benefits

Costs

- Compliance costs up to EUR 29 billion (2% of the total market turnover)
- Costs for public authorities for monitoring and enforcement
- SMEs and public authorities to benefit from DEP and Horizon Europe

Benefits

- More transparent and secure products
- Reduction of cybersecurity incidents for businesses, roughly €180-290 billion annually
- Prevention of internal market fragmentation
- Reduction of compliance costs for NIS2 entities
- Enhanced reputation for EU and non-EU manufacturers
- EU as first mover to shape global standards

Thank you.

New Legislative Framework

- Manufacturers, authorised representatives, distributors and importers
- Notified bodies
- Notifying authorities
- National accreditation bodies
- Market surveillance authorities

(Harmonised) standards

- Based on **Commission request** according to Regulation (EU) No 1025/2012 + Annual Union Work Programme of Standardisation
- To be developed by **European Standardisation Organisations** (ESOs)
- Steps:
  - ✓ **As of now**, preparatory work to start early on
  - ✓ EC to adopt standardisation request (comitology procedure) with close involvement of stakeholders and ESOs
  - ✓ 1 months for ESOs to accept (or otherwise) standardisation request
  - ✓ Standardisation work led by ESOs
  - ✓ EC accepts or rejects the harmonised standards

Interplay with other legislation

Repeal/amend
(Radio Equipment Delegated Regulation)

Complementarity
(electronic health records, toys, machinery, marine equipment etc.)

Exclusion
(motor vehicles, (*in vitro*) medical devices, certified aeronautical equipment)

Only one conformity assessment
(AI, electronic health records)

Presumption of conformity
(Cybersecurity Act)

Lex specialis

Interplay with the Cybersecurity Act

- EU cybersecurity certification schemes may provide presumption of conformity and possible exemption from conformity assessment under CRA.
- Possibility to make EU cybersecurity certification mandatory for “highly critical products”
- Market surveillance authorities and National cybersecurity certification authorities to cooperate (if they are not the same)
- EU cybersecurity certification schemes under development and Union Rolling Work Programme to take into account CRA

Interplay with the AI Act

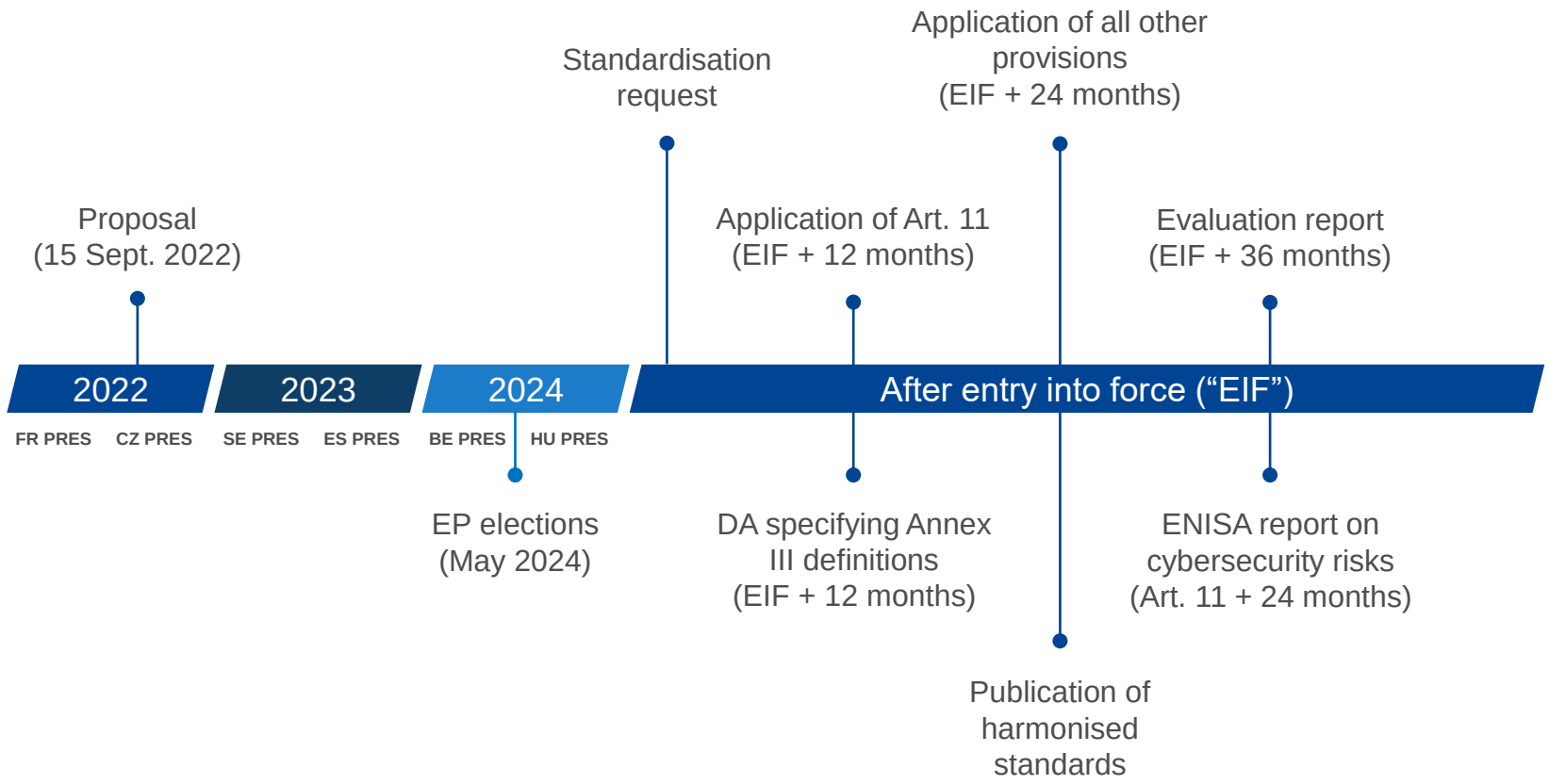
As a rule, high-risk AI systems covered by both the CRA as well as the AI Act should only be subject to **one single conformity assessment**. One specific exception for high-risk AI systems qualified as critical products in CRA.

	Required assessment under the CRA	Required assessment under the AI Act	Conformity assessment to be followed
Case 1	Self-assessment	Self-assessment	AI Act
Case 2	Self-assessment	Third-party assessment	AI Act
Case 3	Third-party assessment	Self-assessment	CRA + AI Act
Case 4	Third-party assessment	Third-party assessment	AI Act

Interplay with GPSR & Machinery Regulation

- **General Product Safety Regulation** continues to apply to non-cybersecurity related safety aspects of products with digital elements (where such products are not subject to other legislation).
- **Machinery products** conformant with the CRA's essential requirements are considered compliant with the proposed Machinery Regulation as regards the essential requirement "protection against corruption and safety and reliability of control systems".

Tentative timeline



European Commission

Remote data processing, including SaaS, in relation to CRA scope

EXAMPLES

European Commission, DG CONNECT

Introductory remarks

- This is a set of examples illustrating the concept of “remote data processing solutions” in the European Commission’s proposal for a Cyber Resilience Act.
- ✓ In scope means that the product or data processing activity is inside the scope of the CRA.
- ✗ Outside the scope means that the product or data processing activity is out of scope of the CRA.
- Explanations in purple indicate if an operator/manufacturer is covered or not covered by the NIS2 Directive.

Article 3 of the CRA proposal (definitions)

- **‘product with digital elements’** means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately;
- **‘remote data processing’** means any *(1) data processing at a distance* for which the software is *(2) designed and developed by the manufacturer or under the responsibility of the manufacturer*, and *(3) the absence of which would prevent the product with digital elements from performing one of its functions*;

Criteria for SaaS coverage by CRA & NIS2

CRA

SaaS are only covered if they are:

- Data processing at a distance
- Designed and developed by or under the responsibility of the manufacturer (i.e. outsourced) of the underlying product
- Necessary for the hardware or software product to function

NIS2

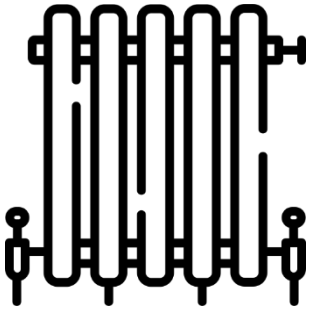
- SaaS providers are covered as cloud computing services (“a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including when those are distributed over several locations”)
- Medium or large in size (or identified by a MS as essential or important entity)

Smart thermostat

Data exchange via SaaS service
(developed under responsibility of the manufacturer “CozyCabin”)

✓ In scope as remote data processing without which the product could not perform its functions

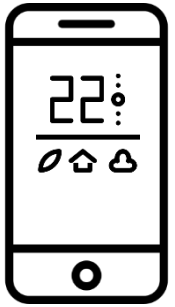
The company “CozyCabin” as a whole is also covered by the NIS2 (subsector “Manufacture of computer, electronic and optical products”).



Smart thermostat
(developed by manufacturer “CozyCabin”)

✓ In scope as hardware

Mobile application to control the thermostat
(developed by manufacturer “CozyCabin”)



✓ In scope as software

European Commission

Word processing provision through SaaS

Document storage on the cloud
(developed under responsibility of the manufacturer “Macrohard”)

✓ In scope as remote data processing

The company “Macrohard” as a whole is also covered by the NIS2, as cloud services as defined in the NIS2 are part of its core activity.

Word processor for PC
(developed by manufacturer “Macrohard”)

✓ In scope as software

Word processor as mobile app
(developed by manufacturer “Macrohard”)

✓ In scope as software

Web browser

Websites
(services provided outside the responsibility of the manufacturer “Noodle”)

✗ Outside the scope for the browser manufacturer

May be covered by NIS2 (such as for example DuckDuckGo, which is a search engine).

Web browser “Silver”
(developed by manufacturer “Noodle”)

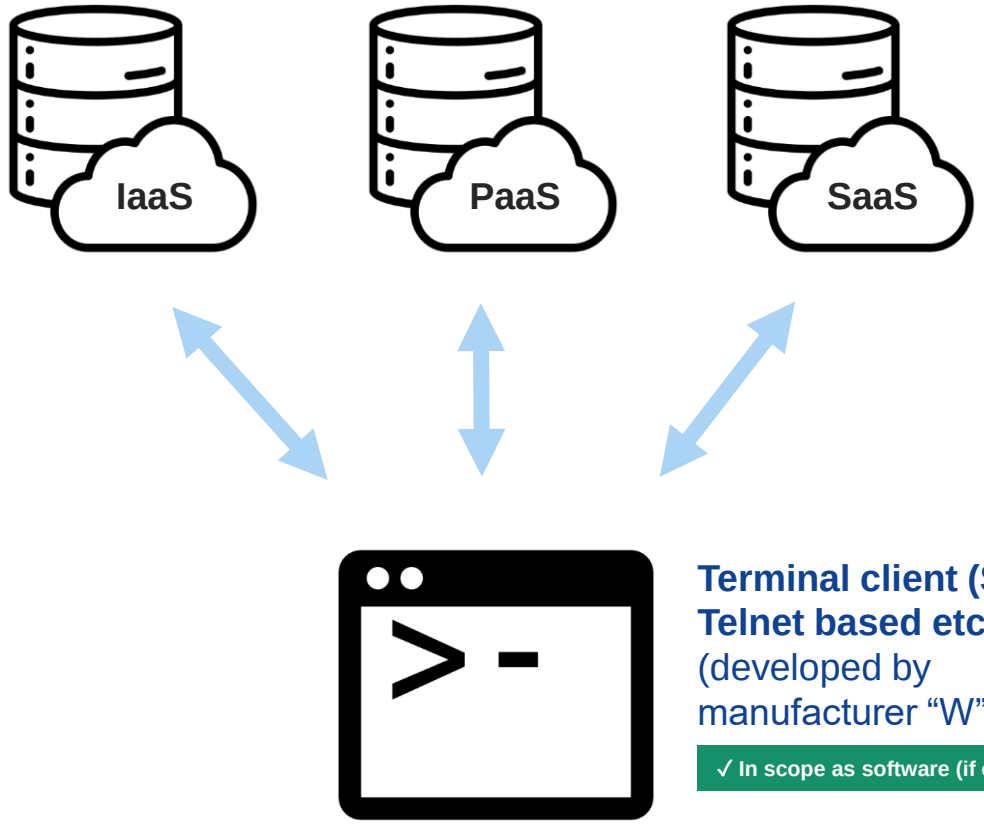
✓ In scope as software

Browser synchronises bookmarks, history and passwords with the cloud
(developed under responsibility of the manufacturer “Noodle”)

✓ In scope as remote data processing

European Commission

Terminal (interface to access cloud services)



Cloud services
(developed under the responsibility of providers "X", "Y", and "Z")

✗ Not considered as a remote data processing activity of the terminal client (as it's not developed under the responsibility of manufacturer "W")

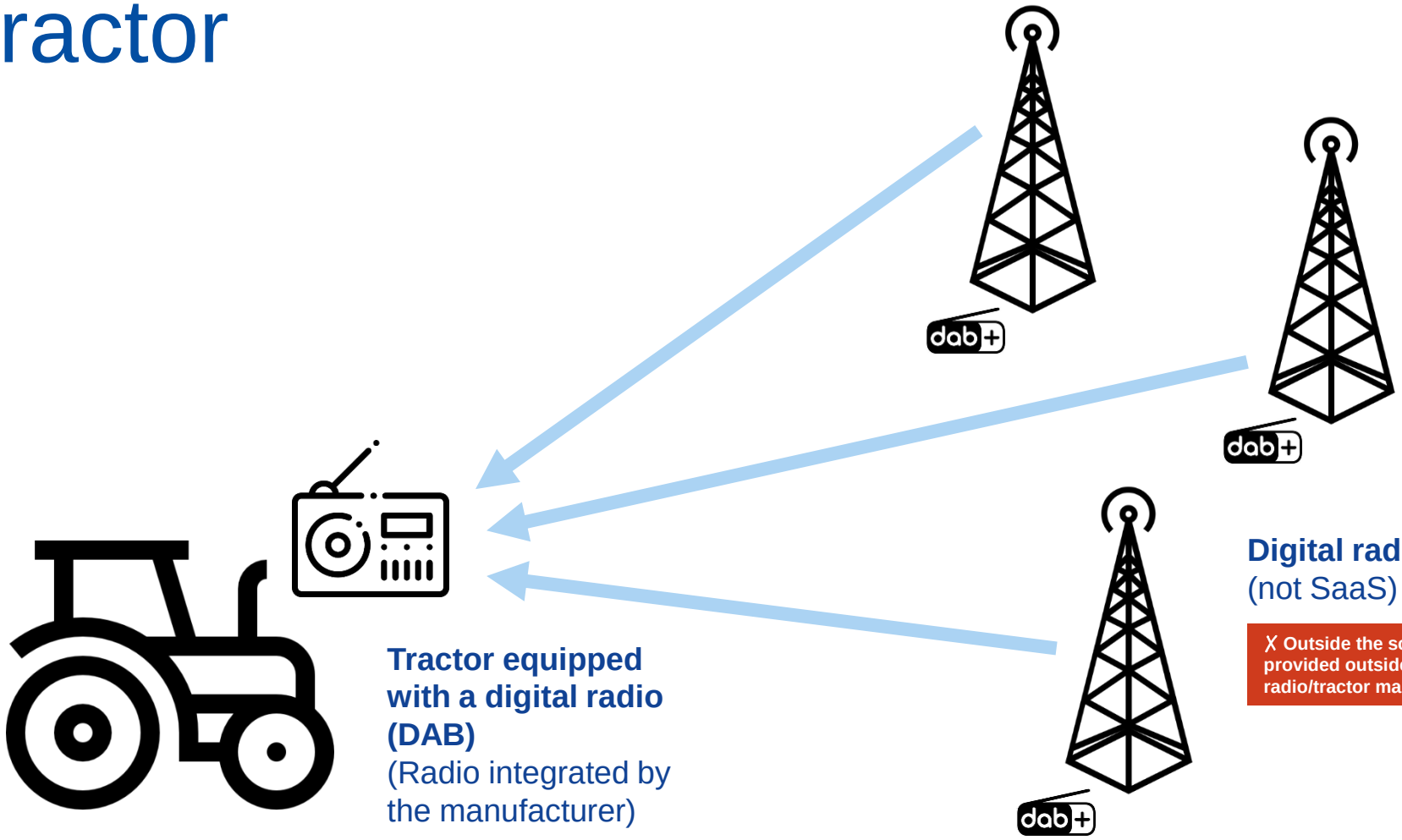
BUT X, Y and Z are covered as cloud providers by the NIS2 if they meet the definition of "cloud computing service" (and if they are medium or large in size, or identified by a Member State).

Terminal client (SSH, Telnet based etc.)
(developed by manufacturer "W")

✓ In scope as software (if commercial)

European Commission

Tractor



Tractor equipped with a digital radio (DAB)
(Radio integrated by the manufacturer)

✓ In scope as hardware

The manufacturer is covered by NIS2 (subsector “Manufacture of machinery and equipment n.e.c.”)

Digital radio stations
(not SaaS)

✗ Outside the scope, as the services are provided outside the responsibility of the radio/tractor manufacturer

European Commission

A simple company website

Website advertising a hamburger chain (developed by restaurant chain “MyJuicyBurgers”)

✗ Outside the scope (it’s a service, not a product)

www.myjuicyburgers.com

The chain “MyJuicyBurgers” is also outside the scope of the NIS2 Directive, as restaurants are neither listed in Annex I nor Annex II.

The company belong to the gastronomy sector and is not covered by the definition of “cloud computing service”. It is therefore also not covered by the NIS2 as cloud service provider.

Customer relationship management software

CRM software provided as SaaS (developed by provider “SellYourProduct”)

✗ Outside the scope (it’s a service and “SellYourProduct” does not provide any desktop or mobile application for that service)

Falls under the definition of cloud provider in NIS2. INSIDE the scope of NIS2 if medium or large in size, OUTSIDE the scope of NIS2 if small in size.

Accessible via the web using a browser (not developed by “SellYourProduct”)

Certain functions exposed via API (open standards, no client product development by manufacturer “SellYourProduct”)

No mobile app or other client available (“SellYourProduct” choice not to develop any own client software)

European Commission

Icon attributions

- Thermostat created by iconixar – Flaticon
- Radiator created by Freepik – Flaticon
- Cloud created by Freepik – Flaticon
- Telephone created by HAJICON – Flaticon
- Tractor created by Freepik – Flaticon
- Radio transmitter antenna by OpenClipart
- Web browser by OpenClipart
- Globe created by srip – Flaticon
- Monitor created by xnimrodx – Flaticon
- Database created by Smashicons – Flaticon
- Json created by juicy_fish - Flaticon

Thank you.

European Commission