European
Commission

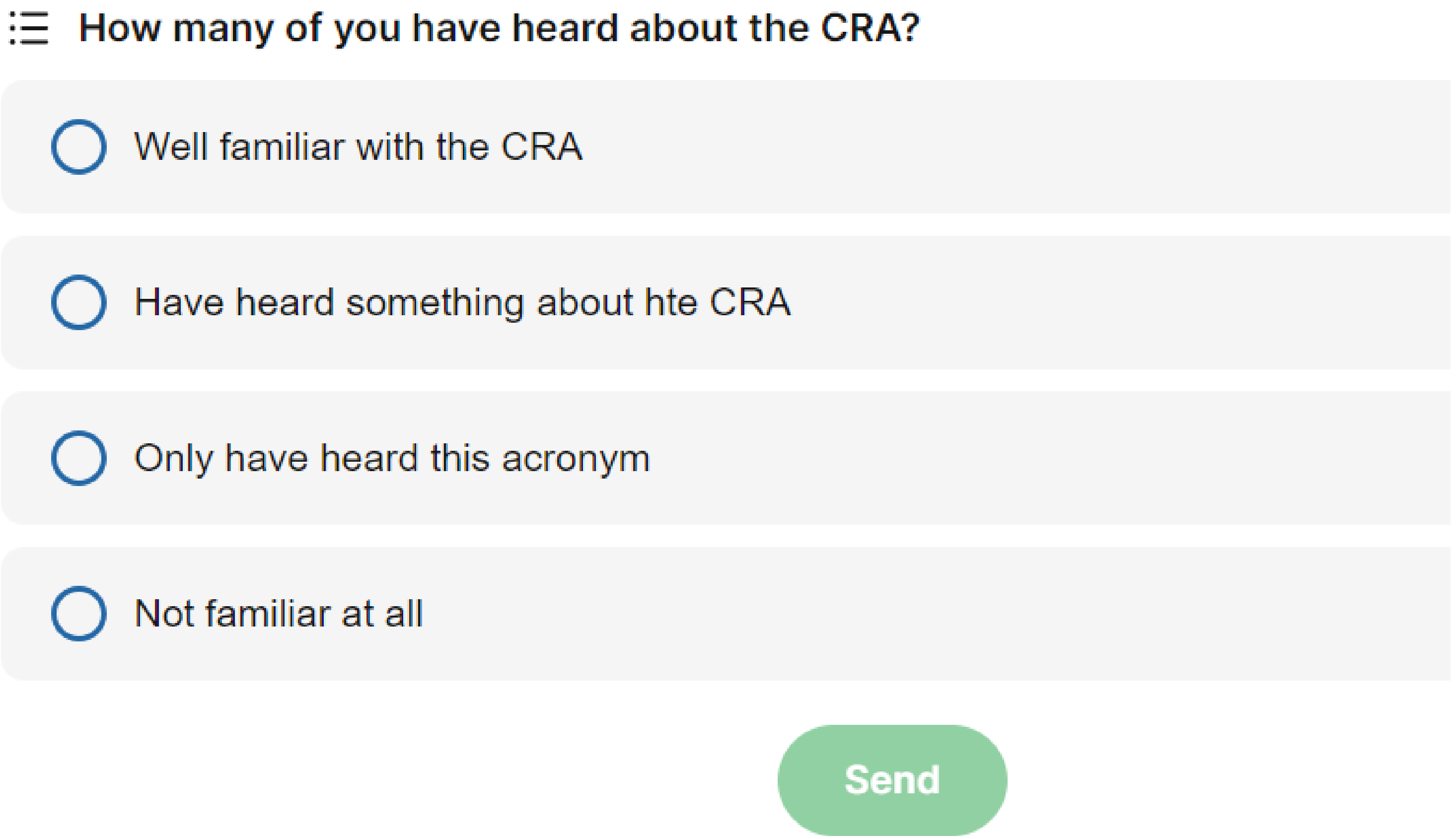
Cyber Resilience Act

12 July 2023

Maika FÖHRENBACH
European Commission, DG CONNECT

Sli.do: How familiar are you with the CRA?

Join Slido.com with **#4226842**



How many of you have heard about the CRA?

○ Well familiar with the CRA

○ Have heard something about hte CRA

○ Only have heard this acronym

○ Not familiar at all

Why the CRA ?

Impact of security incidents - some figures

- Statistically speaking, **every 11 seconds** another organisation is hit by a ransomware attack.
- In 2021 alone cybercriminals were able to leverage hacked devices and **launch 9.75 million DDoS attacks** worldwide.
- **57 % of SMEs** say they would go out of business in the event of a cybersecurity attack.
- The aggregate cost of security incidents affecting businesses in Germany amounts to **EUR 220 billion in 2020**.
- **Supply Chain Compromise of Software Dependencies** as key trend in ENISA report on Emerging Cybersecurity Threats For 2030

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

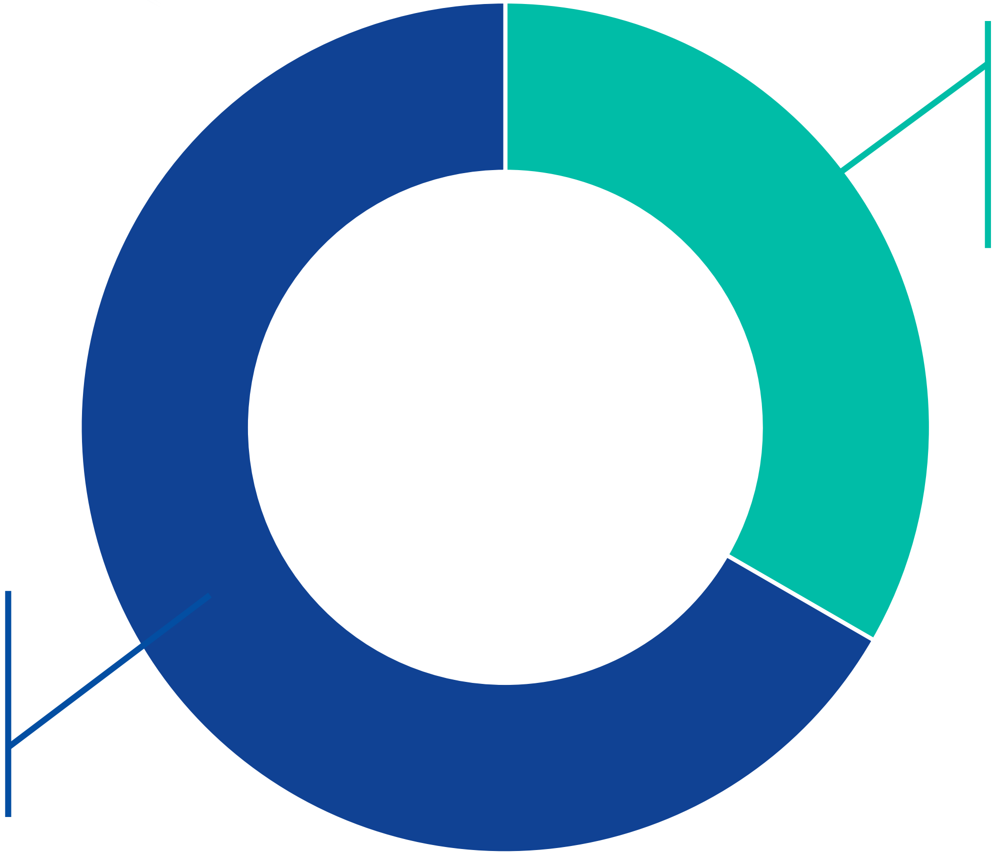
THREATS 2030

IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030

MARCH 2023

Sources: Ponemon Institute, Cybersecurity Ventures, Netscout, ENISA, Bitkom

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.

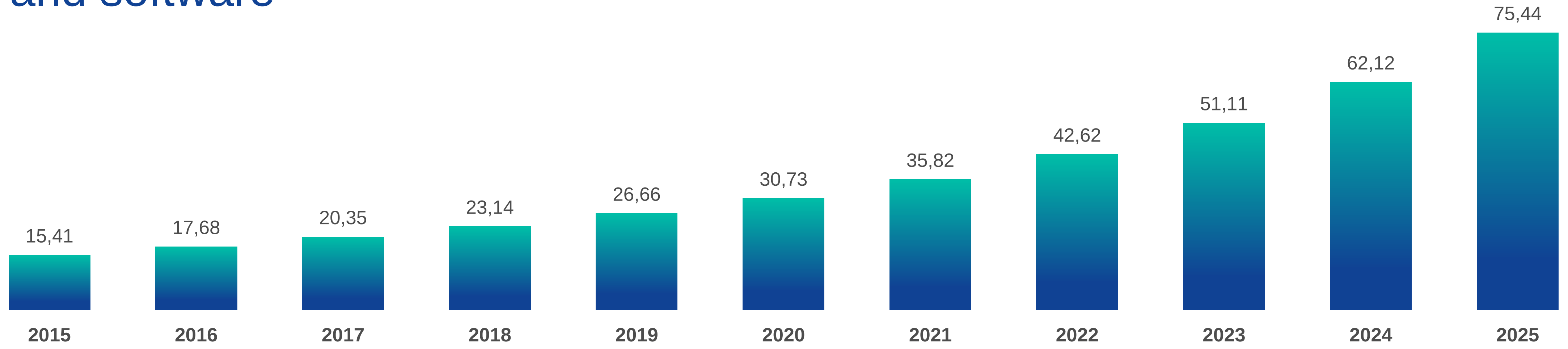
Source: ENISA/Gartner (2022)

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.

Everything is connected

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



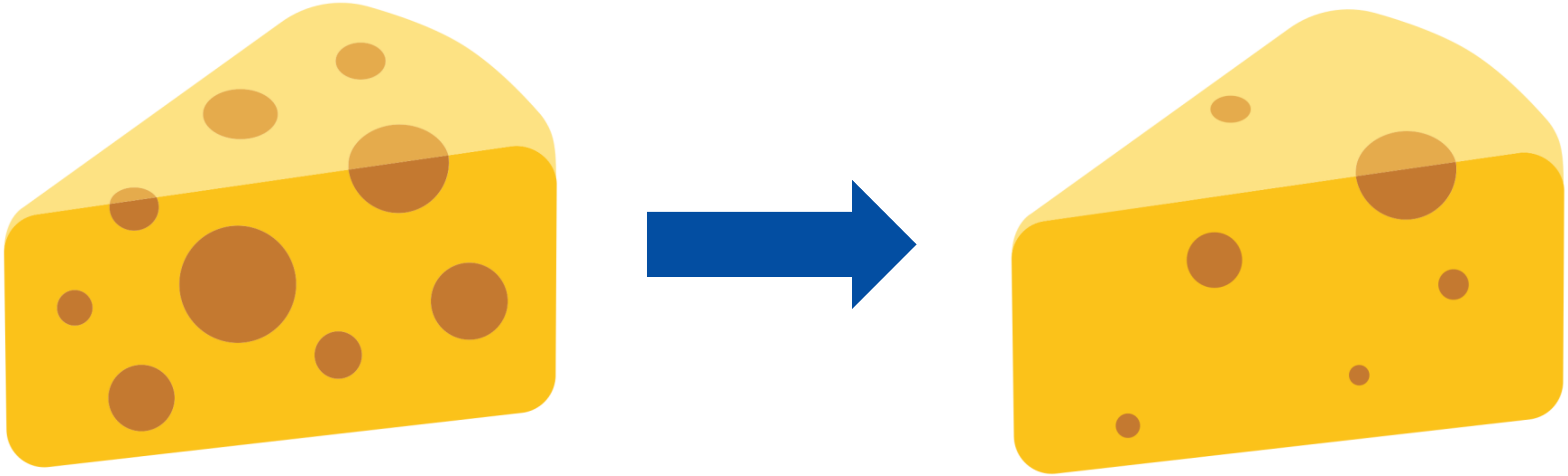
Internet of Things devices worldwide from 2015 to 2025 (in billions)

Source: Forbes/IHS

European Commission

So what will the CRA do about this ?

CRA in a nutshell



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:

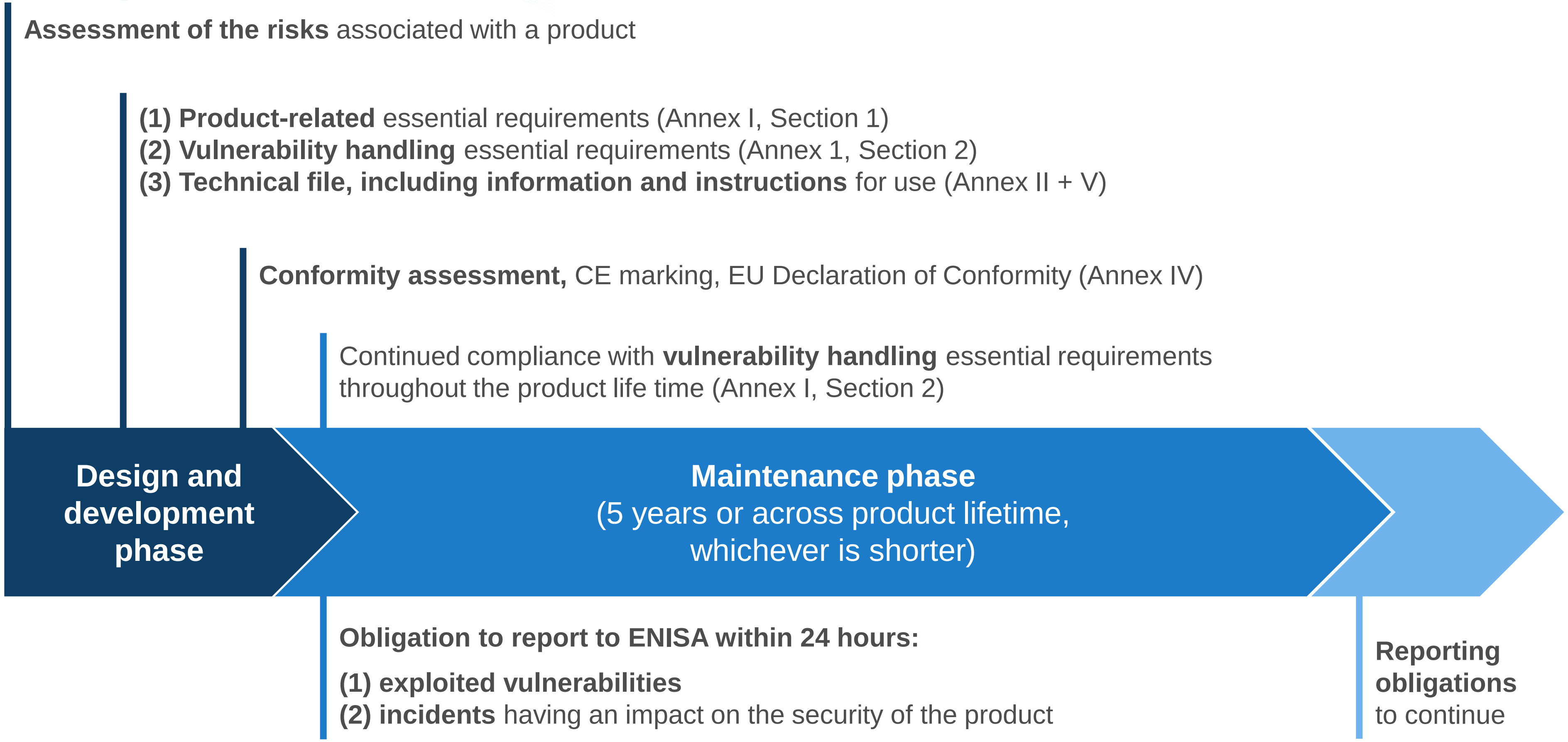
✖ **Non-commercial projects, including open source** in so far as a project is not part of a commercial activity

✖ **Services, in particular cloud/Software-as-a-Service** – *unless as “remote data processing”*

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)

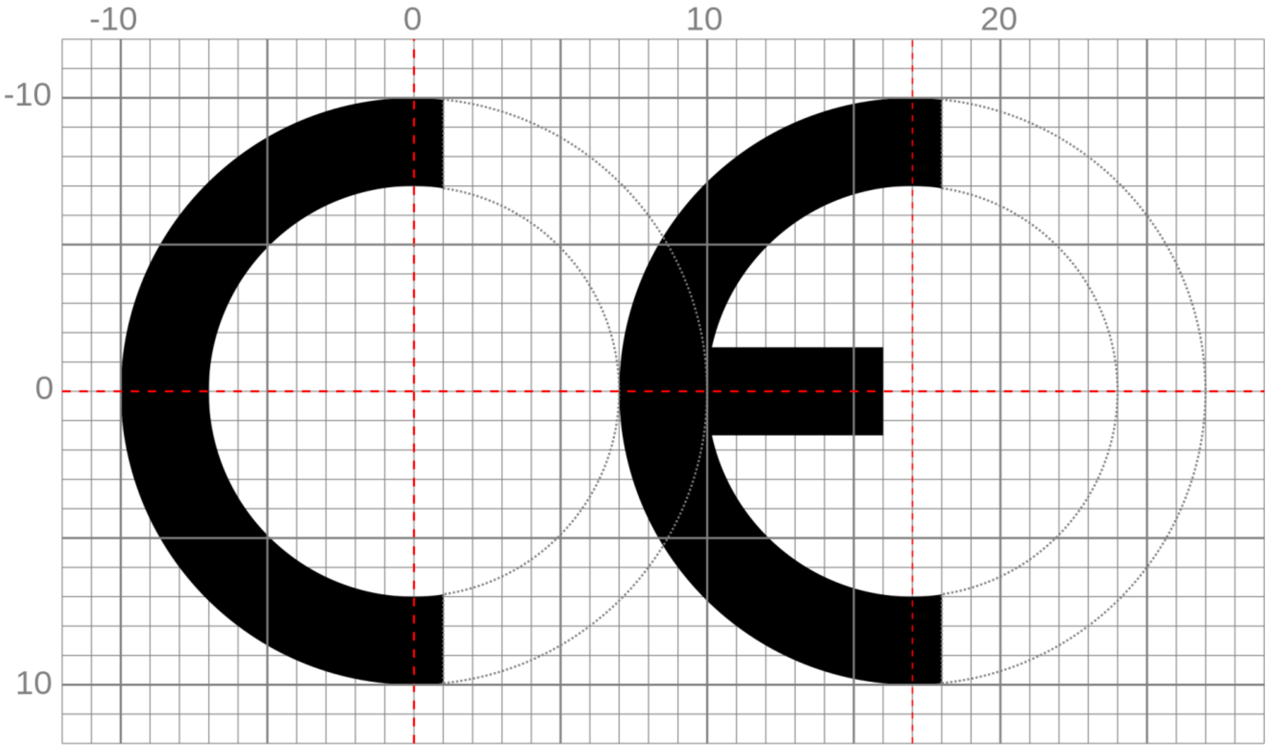
Obligation to report to ENISA within 24 hours:

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

Reporting obligations to continue

European Commission

CE marking



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**

Vulnerability handling requirements

- **Identify and document dependencies** and vulnerabilities, including **SBOM**
- In relation to the risks, **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**

More transparency for users

- **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)
- Type of **support offered** by the manufacturer and for how long
- Instructions on **secure use** and secure removal of data

How will the CRA impact SMEs?

Costs & benefits for SMEs

- 99%+ of the hardware manufacturers and software developers in the EU market are SMEs
- SMEs as end-users
- Targeted outreach during preparatory phase of the proposal (impact assessment)
- Strong support from SMEs for horizontal approach & level playing field with large companies

Cost & benefits for SMEs

Costs

- Compliance costs *(manufacturers)*
  - Secure product development costs
  - Testing
  - Third-party assessment
  - Documentation costs
  - Reporting
- Possible price increase *(users)*

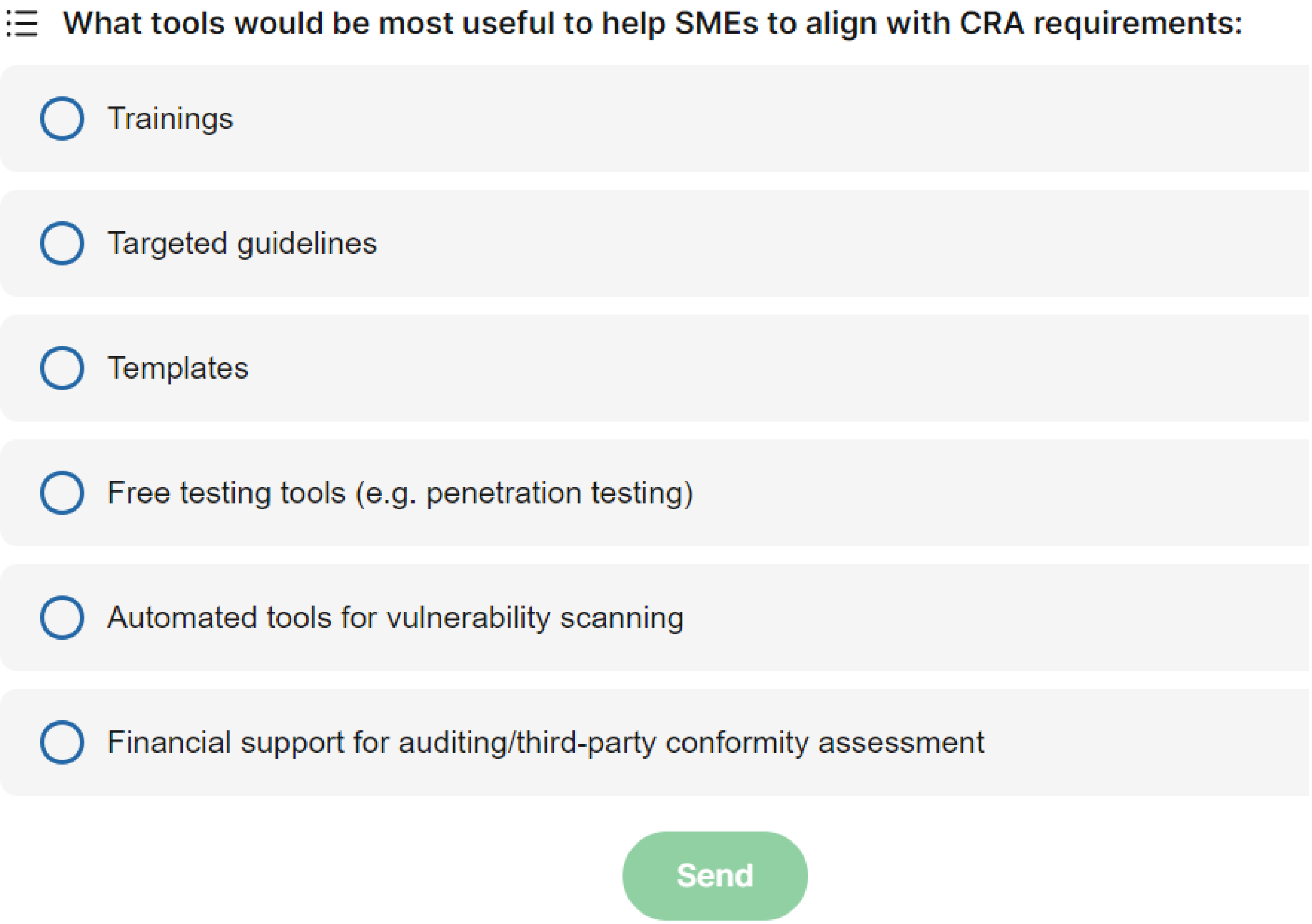
Benefits

- Positive impact on **competitiveness** and **internal market** *(manufactures)*
- Reduction of **cybersecurity incidents** for businesses between 20 % and 33 % *(users)*
  - 90% of SMEs state that a cyber incidents would have a serious negative impact, for 57% possible bankruptcy (*ENISA survey*)

European Commission

How will the implementation of the CRA be facilitated?

Sli.do #4226842



What tools would be most useful to help SMEs to align with CRA requirements:

- ○ Trainings
- ○ Targeted guidelines
- ○ Templates
- ○ Free testing tools (e.g. penetration testing)
- ○ Automated tools for vulnerability scanning
- ○ Financial support for auditing/third-party conformity assessment

A risk-based approach to the obligations

- Objective-driven, technology-neutral and risk-based **essential cybersecurity requirements**

- **Conformity assessment** :

  - **Default category:** The vast majority of products will be subject to *self-assessment* (examples: photo editing, word processing, smart speakers, hard drives, games etc.)

  - **Critical products – *Annex III Class 1 and 2*:** *more stringent conformity assessment procedures*, including assessment by an independent third party; proportionality ensured by two classes.

  - **Highly critical products – *not yet listed* :** the Commission is empowered to adopt secondary legislation requiring *mandatory certification* based on EU cybersecurity certification schemes (Cybersecurity Act).

Alignment with existing standards

✓ **Harmonised standards** to be developed by ESOs – CEN / CENELEC / ETSI.

✓ **Less burdensome compliance** when following Harmonised Standards : Presumption of conformity.

✓ Building on **existing European & international standards** (e.g. IEC 62443 and ISO 27000 series)

✓ Preparatory work has started : mapping, gap analysis …

*How to engage ?*CEN-CENELEC JTC 13 WG 9 & ETSI TC Cyber

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

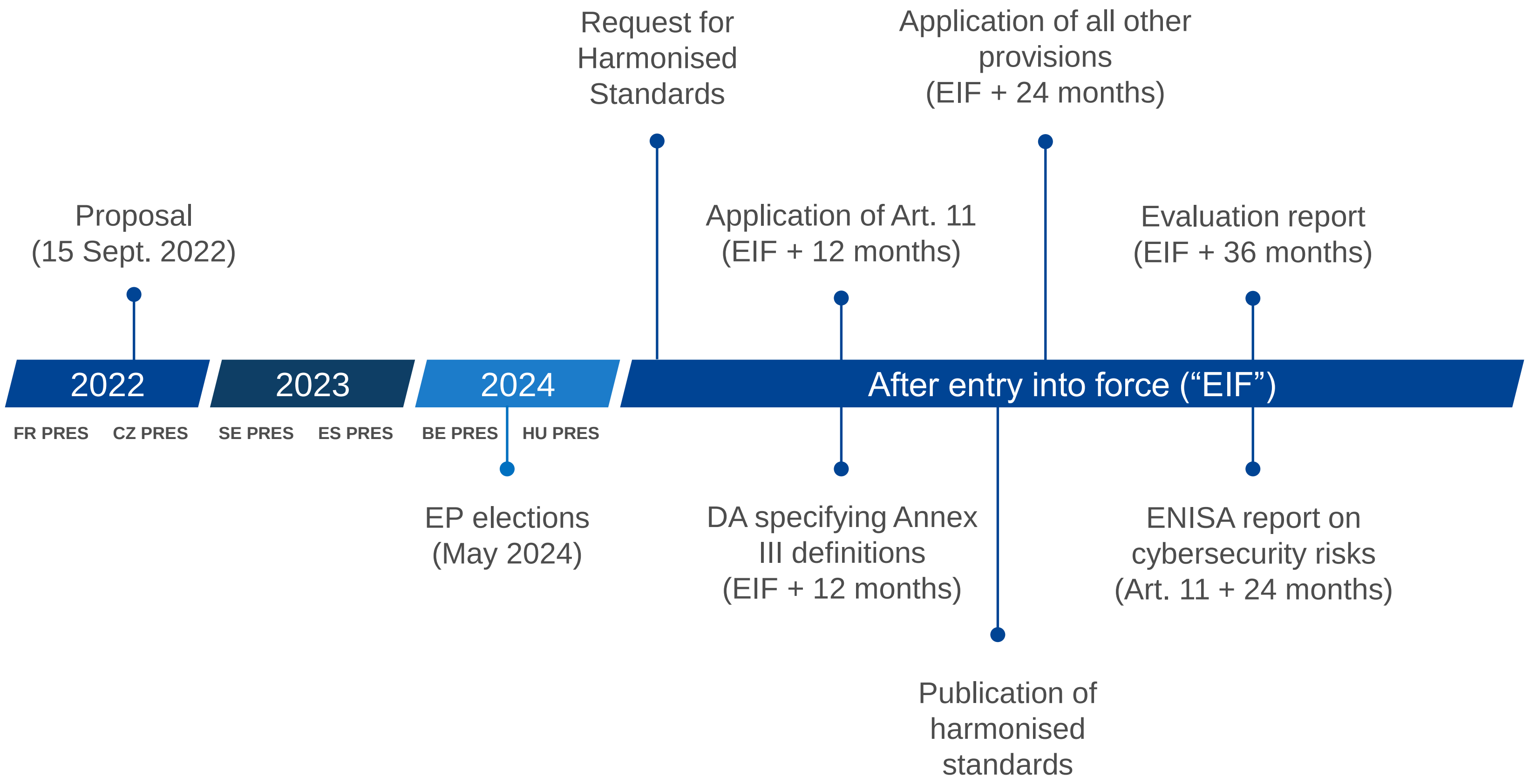
Funding & guidelines

1. Funding, e.g. training and awareness raising, participating in standardisation work, automated compliance tools and supporting platforms

- ✓ Horizon Europe, Digital Europe programme
- ✓ European Digital innovation Hubs
- ✓ National cybersecurity coordination centres

2. Guidelines & templates by the Commission

Tentative timeline



2022 | 2023 | 2024 | After entry into force ("EIF")

FR PRES · CZ PRES · SE PRES · ES PRES · BE PRES · HU PRES

Proposal
(15 Sept. 2022)

EP elections
(May 2024)

Request for
Harmonised
Standards

Application of Art. 11
(EIF + 12 months)

DA specifying Annex
III definitions
(EIF + 12 months)

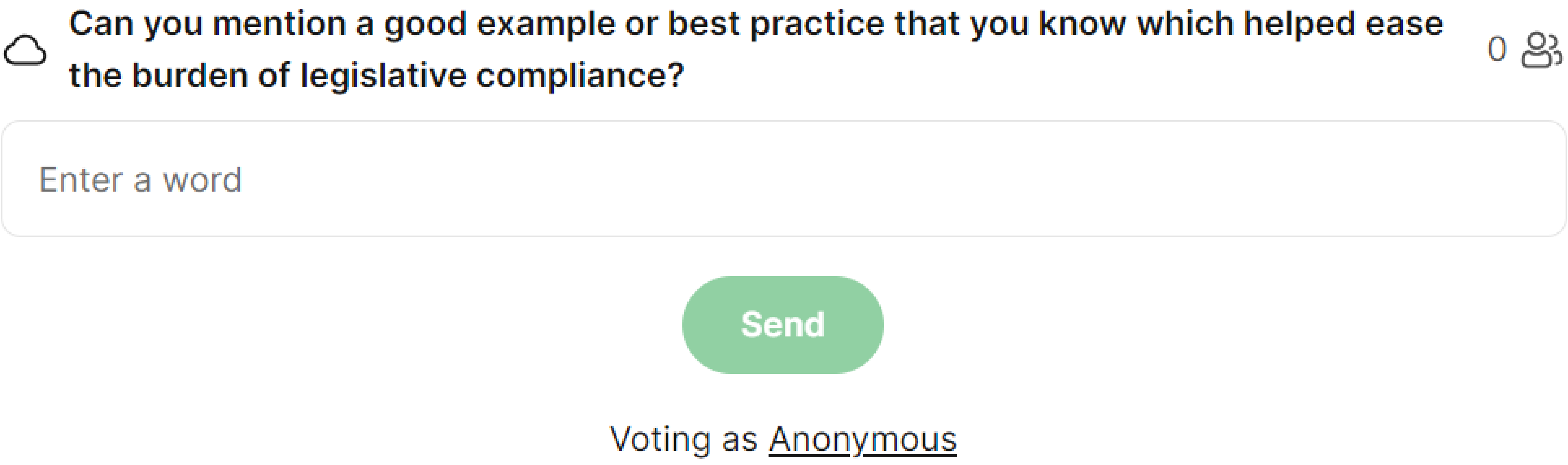
Publication of
harmonised
standards

Application of all other
provisions
(EIF + 24 months)

Evaluation report
(EIF + 36 months)

ENISA report on
cybersecurity risks
(Art. 11 + 24 months)

Sli.do #4226842



Can you mention a good example or best practice that you know which helped ease the burden of legislative compliance?

Thank you.

European
Commission