CYBERSTAND.eu

WEBINAR - 23 SEPTEMBER 2024, 15:00-16:00 CEST

CYBERSTAND.eu

Supporting EU Experts in Standardisation Activities for the Cyber Resilience Act

Funded by
the European Union

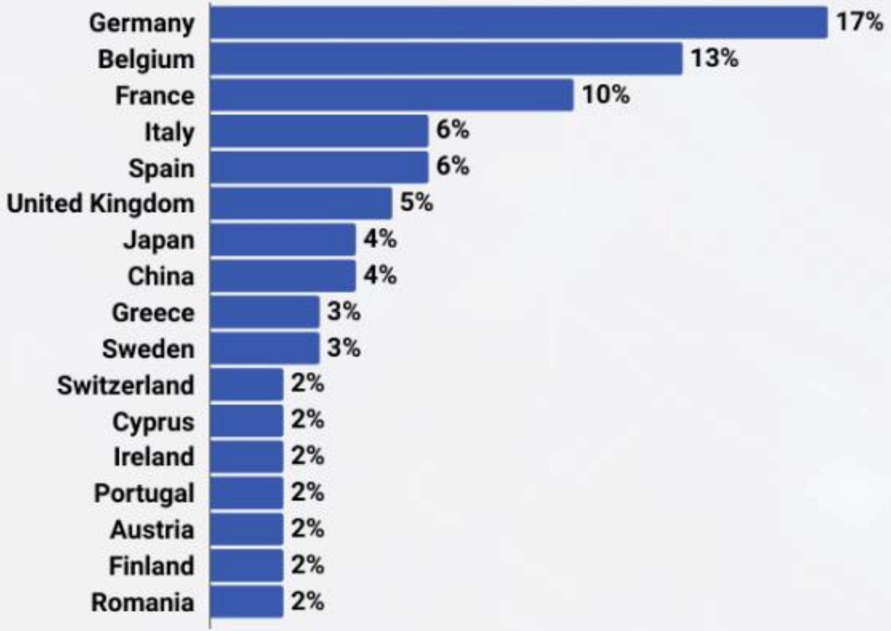
CYBERSTAND.eu

Supporting EU Experts in Standardisation Activities for the Cyber Resilience Act

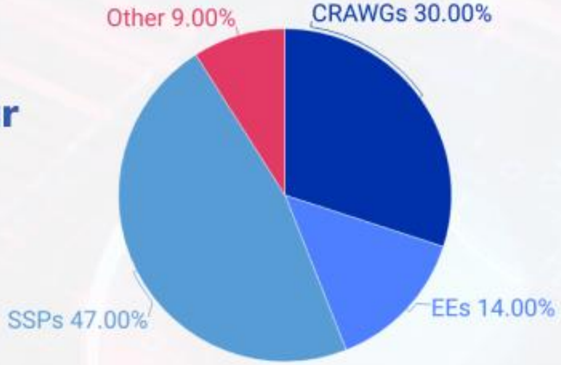
178 Registrants

Gender 66% 🚹 🚺 33%

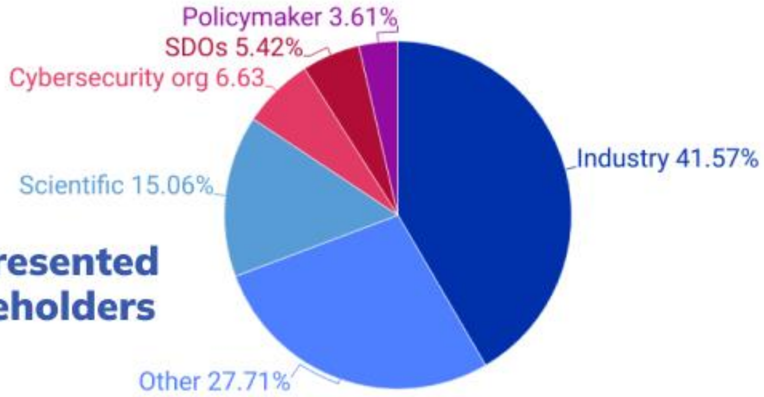
% of participants by country



Which webinar topic are you interested in?



Represented staleholders



Today’s Agenda

- **15:05 | The Cyber Resilience Act and Standardisation priorities - **Filipe Jones Mourão (Cybersecurity & Digital Privacy Policy, DG CONNECT, EC)
- **15:20 | CYBERSTAND.eu - An overview -** Nicholas Ferguson (Trust-IT, CYBERSTAND.eu coordinator)
- **15:30 | Interactive roundtable on the CRA standardisation priority areas and the role of Cyberstand.eu - Chair:** Ultan Mulligan (ETSI). **Participants:** Nooshin Amirifar (CEN-CENELEC), Matteo Molé (ECSO), Filipe Jones Mourão (EC), James Philpot (DIGITAL SME), Teresa Ridolfi (Trust-IT), **15:55 | Closing remarks -** Nicholas Ferguson (Trust-IT, CYBERSTAND.eu coordinator) coordinator)

CYBERSTAND.eu

Supporting EU Experts in Standardisation Activities for the Cyber Resilience Act

23 September 2024

Nicholas Ferguson, Trust-IT Services and CYBERSTAND.eu coordinator.

Funded by
the European Union

Cyberstand.eu: The Essentials

- **Objective**: Engaging & supporting EU experts in cybersecurity standardisation activities
- **Type**: Coordination & Support Action 101158521
- **Duration**: June 2024 – May 2027
- **Budget**: €2,999,999.09
- **Call**: Deployment actions in the area of cybersecurity (DIGITAL-ECCC-2023-DEPLOY-CYBER-04)

Cyberstand.eu Partners

Trust-iT services communicating to markets

COMMpla Communication Platforms and Online Solutions

ECSO EUROPEAN CYBER SECURITY ORGANISATION

European DIGITAL SME Alliance

ETSI

cen

CENELEC

The EU Cyber Resilience Act (CRA)

- *“New EU cybersecurity rules ensure safer hardware and software.”*
- One of the most significant pieces of regulation to come from Europe in recent years.
- Impact will extend well-beyond Europe’s borders.
- Companies large and small, whether based in Europe or wanting to export into Europe will have to comply.
- CRA Standardisation Request in draft and pending publication.
- Clear stakeholder engagement and guidance is a must for the successful implementation of the CRA

Cyberstand.eu in a Nutshell

Mission: Engaging And Supporting EU Experts In Cybersecurity Standardisation Activities

OBJECTIVES

Objective 1: Deliver a coherent and engaging series of events and publications to establish an inclusive community on the CRA

Objective 2: Establish a facility dedicated to support EU experts contributing to standardisation efforts, in EU an Int'l cybersecurity standardisation fora.

Objective 3: Foster the development on harmonised standards, in conformity with the Cyber Resilience Act (CRA).

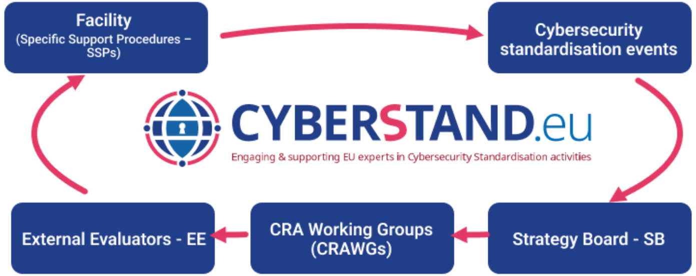
Objective 4: Contributing to implementation of European Values and sustainability of the CRA.

CONTRIBUTION TO STANDARDS

- 200+ EU Experts funded via 6 cycles of Specific Support Procedures (€1,500,000 assigned)
- Contribution to 10+ standardisation Work Items
- Increased international presence of EU experts with SDOs
- ...

REPORTS, TOOLS, AND MATERIALS

- 2 White papers on cybersecurity standards
- 2 Policy Briefs
- Contributions to the Cybersecurity and Networks chapter of the ICT Rolling Plan
- Around 200 impact reports from EU experts
- OA educational materials and tools
- Prioritisation of CRA Work Items
- ...


Facility
(Specific Support Procedures – SSPs)
Cybersecurity standardisation events
CYBERSTAND.eu
Engaging & supporting EU experts in Cybersecurity Standardisation activities
Strategy Board - SB
CRA Working Groups (CRAWGs)
External Evaluators - EE

SYNERGIES UNLOCKED

- Domain-specific collaborations with SDOs and NSBs
- Community-related synergies with NCCs
- Direct dialogues with SMEs and Start-ups
- 30+ selected Use Cases
- Re-use of the StandICT.eu grants platform
- Up-to-date EUOS on cybersecurity standards
- ...

COMMUNITY

- 3000+ community members
- 40+ SMEs actively engaged in harmonisation of standards
- 6+ external SB members
- 30+ External Evaluators
- ...

OUTREACH

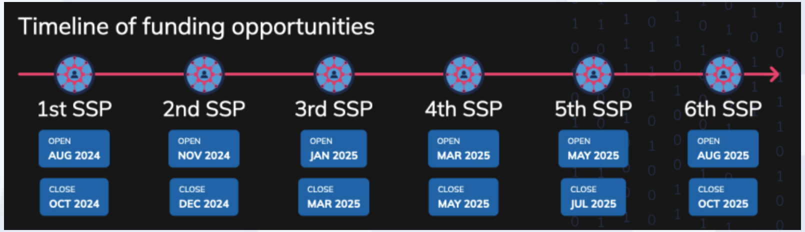
- 3 Annual Impact Events
- 12 Workshops
- 12 Webinars
- 2 public consultations
- 18 Insights Newsletters
- 12 Press Releases
- 9 Professional Videos
- Visibility at 18+ third party events
- ...

SMEs | Start-ups | Consumers | Open-Source Community | DEP & HE EU Projects

SSP – Funds for contributions to standardisation

6 Specific Service procedures for €1.5 million

- **SSP #1: 4th August 5th October**
- Funding types*:
  - **Short term** projects (€3.000 for 3-months activities)
  - **Mid-term** projects (€10.000 for 6-month activities)
  - **long-term** projects (€20.000 for 12-month activities)
- Funding to contribute to standardisation activities related to the draft Cyber Resilience Act Standardisation Request topics
- Apply here



Timeline of funding opportunities

1st SSP	2nd SSP	3rd SSP	4th SSP	5th SSP	6th SSP
OPEN AUG 2024	OPEN NOV 2024	OPEN JAN 2025	OPEN MAR 2025	OPEN MAY 2025	OPEN AUG 2025
CLOSE OCT 2024	CLOSE DEC 2024	CLOSE MAR 2025	CLOSE MAY 2025	CLOSE JUL 2025	CLOSE OCT 2025

Calling SSP Evaluators

- Individuals with expertise in standardisation, vertical sectors and the market.
- Selected evaluators will review SSP proposals.
- Apply here

CYBERSTAND.eu
Apply for Funding to Develop Standards for the Cyber Resilience Act
1st SSP
TOTAL FUNDING AVAILABLE € 250,000
DEADLINE 5th Oct 2024
APPLY NOW!
Funded by the European Union

*Applicants **individuals or natural persons** residing **in European Member States and Associate countries**.

CRA Working Group

SMEs

Start-ups

Consumers

Open-Source Community

DEP & HE EU Projects

Multi-stakeholder dialogue around the CRA

- Identify and provide **recommendations** on key priority areas for standardisation activities;
- **Awareness and outreach**, making sure that work done on standardisation is well understood as well as aligned with the market;
- Supporting the drafting of **guidelines and recommendations.**

What to expect

- Contribute to the challenges on standards and implementation of the CRA;
- Have your say on CRA implementation
- Gain expertise and visibility as a subject matter expert
- Become part of a long-term body of expertise with peer-to-peer synergies and opportunities of networking

CYBERSTAND.eu
Cyber Resilience Act Working Groups (CRAWGs)
Funded by the European Union

Registration now open

Guidance and dialogue with SMEs

WHY

- Address key areas where SMEs may struggle with CRA compliance.
- Navigate CRA requirements and manage their products and services cybersecurity risks.

WHAT

- Support and resources tailored specifically for SMEs to:
  - Help them comply with the CRA requirements.
  - Provide them with the knowledge needed to implement the CRA cybersecurity requirements.

HOW

- 2 SMEs Public consultations to understand their specific challenges and needs.
- Feedback from the SMEs will be used to tailor the guidance and make it even more relevant for them.

Thank you!

Nicholas Ferguson (Coordinator) - n.ferguson@trust-itservices.com

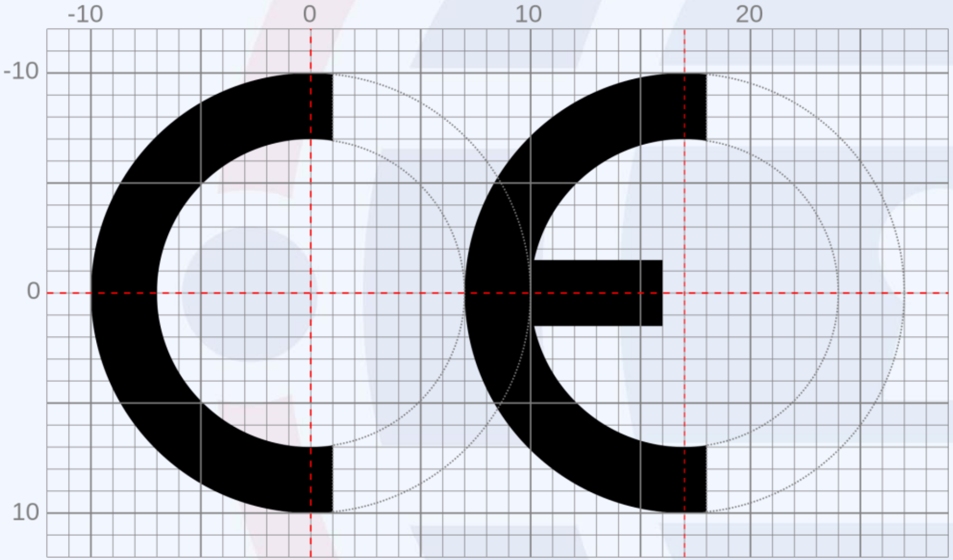
www.cyberstand.eu

Funded by
the European Union

Cyber Resilience Act

Filipe Jones Mourao, policy officer
European Commission, DG CONNECT

CE marking



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**

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:

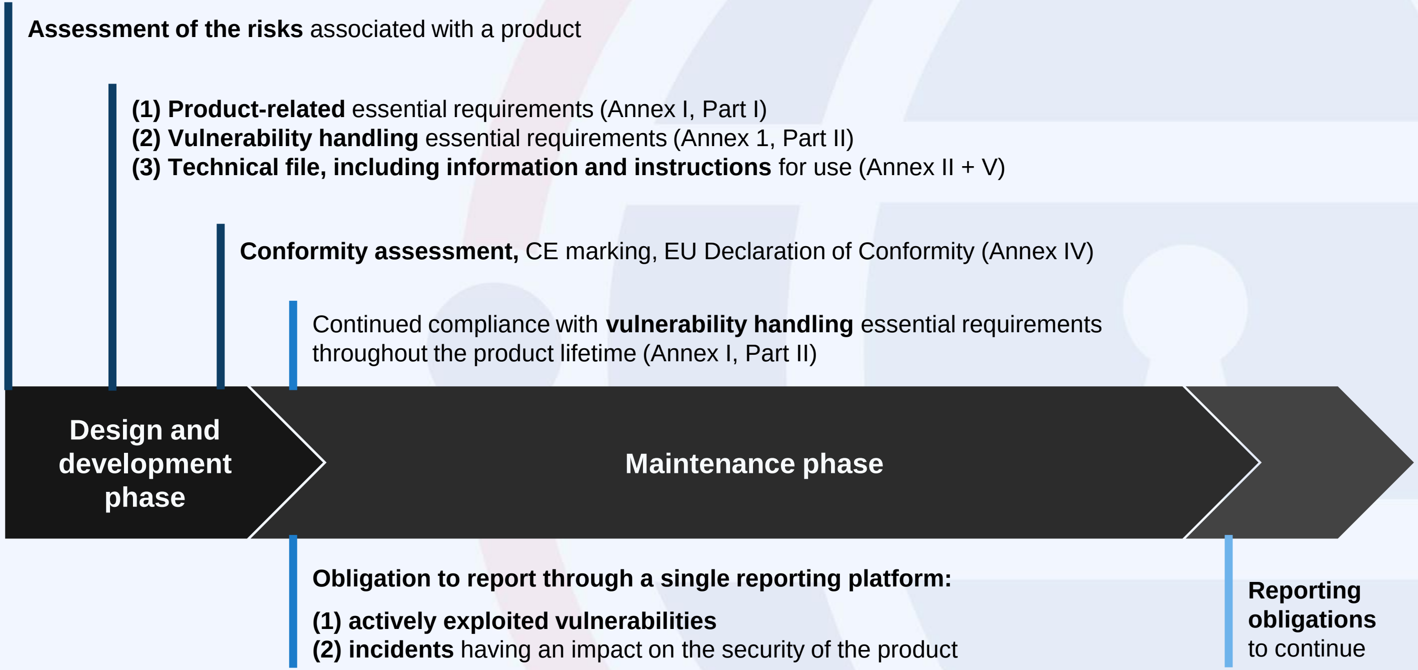
- ✖ **Certain products sufficiently regulated on cybersecurity** (cars, medical devices, *in vitro*, certified aeronautical equipment, marine equipment)

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)

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

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

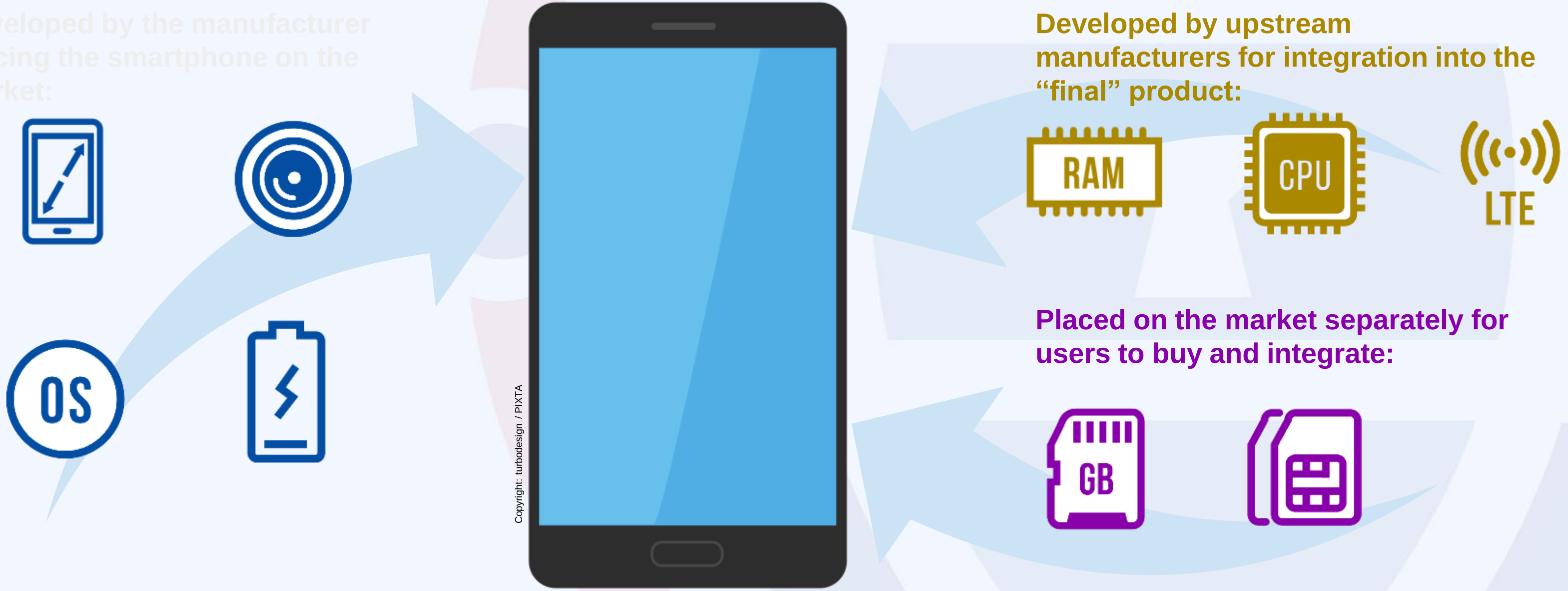
- **Manufacturers to draw up a SBOM** in a commonly used format covering at the very least the top-level dependencies of the product
- **No requirement** to make the SBOM publicly available
- SBOM to be included in the **technical documentation** and, upon request, to be provided to **market surveillance 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:

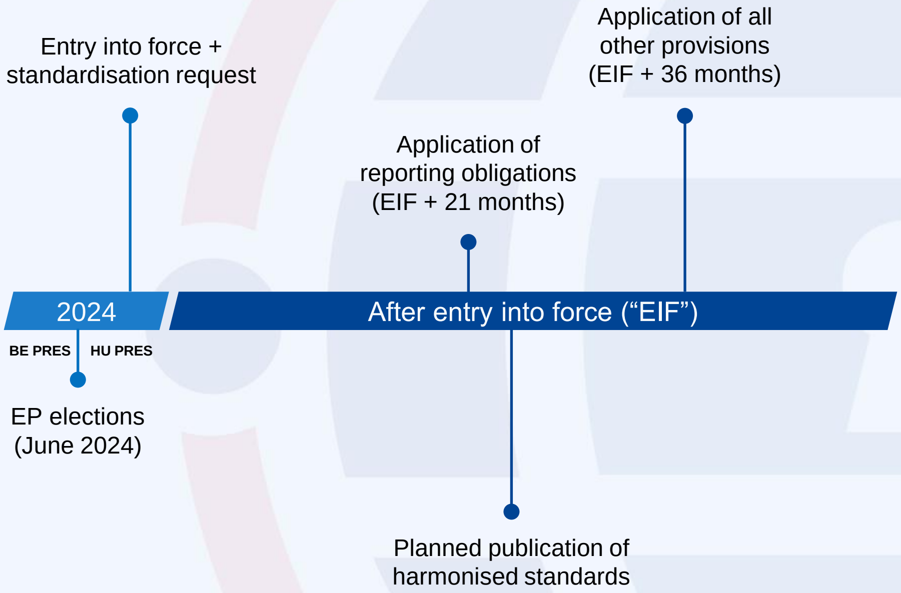
Placed on the market separately for users to buy and integrate:

Copyright: turbodesign / PIXTA

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



Entry into force + standardisation request

Application of all other provisions (EIF + 36 months)

Application of reporting obligations (EIF + 21 months)

2024

After entry into force ("EIF")

BE PRES

HU PRES

EP elections (June 2024)

Planned publication of harmonised standards

CRA implementation underway

- Technical descriptions of important and critical products
- Harmonised European standards

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

Thank you.

Our Panellists

Chair: Ultan Mulligan (ETSI)

Nooshin Amirifar (CEN-CENELEC)

Matteo Molé (ECSO)

Filipe Jones Mourão (European Commission)

Teresa Ridolfi (Trust-IT)

James Philpot (DIGITAL SME)