



Cyber Resilience Act

CNECT.H2

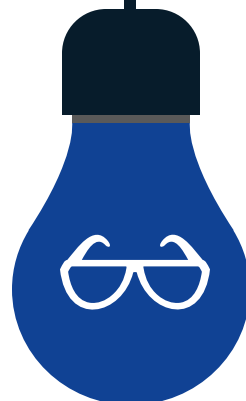
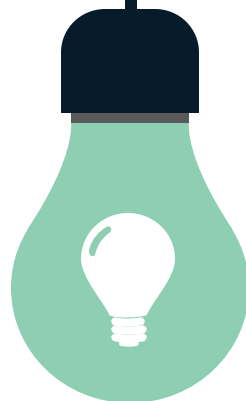
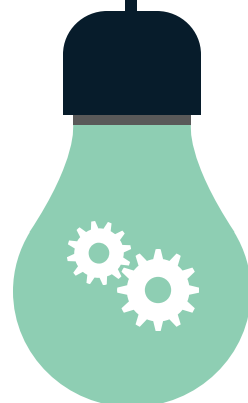
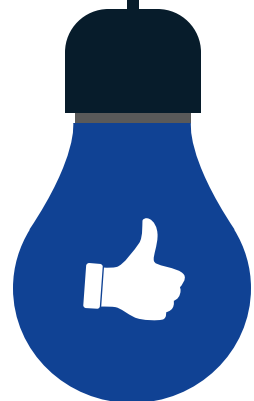
European Commission, DG CONNECT

Housekeeping rules

- ❖ Engage on sli.Do
- ❖ Selected questions will be answered



AGENDA



10:00 – 10:10 Welcome Remarks by
Christiane Kirketerp de Viron

1

10:10 – 10:50 Presentations by
the European Commission

2

10:50 – 11:20 state of the play of
the standardisation work supporting the CRA

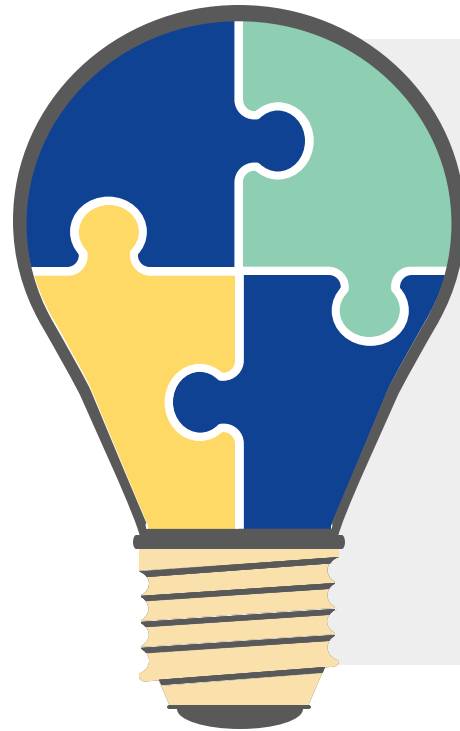
3

11:20 – 11:50 Making the CRA fit for SMEs

4

WELCOME!

Get ready for your Slido poll

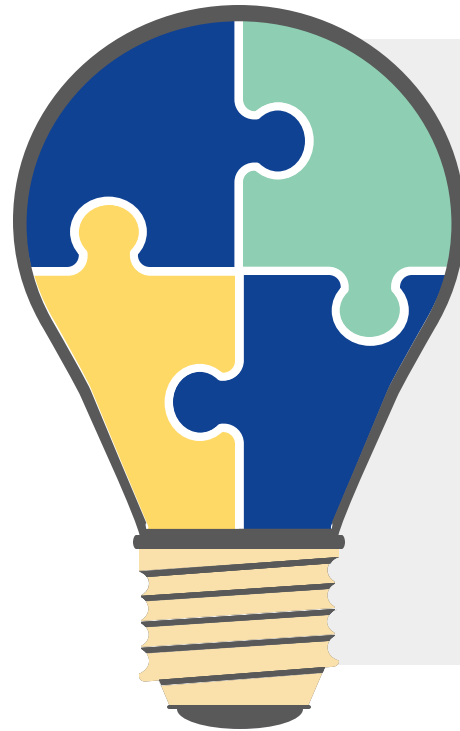


**What
organisation do
you represent?**

- 1) SME
- 2) Big company
- 3) Public sector
- 4) Trade association
- 5) Other

WELCOME!

Get ready for your Slido poll



**Do you work in
the area of
cybersecurity?**

1) Yes

2) No

WELCOME!

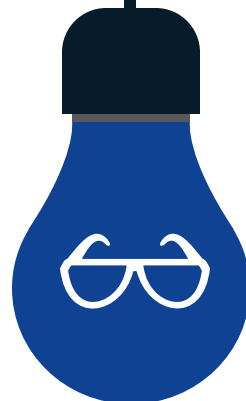
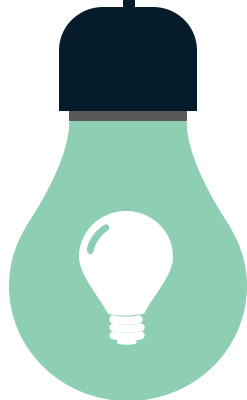
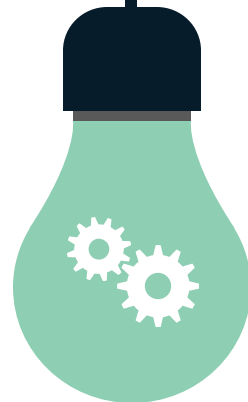
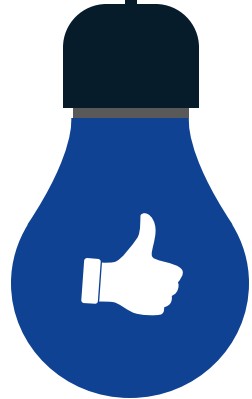
Get ready for your Slido poll



**How much do
you know about
the CRA?**

- 1) I am here to learn
- 2) I have some knowledge
but want to dig deeper
- 3) I consider myself an
expert

AGENDA



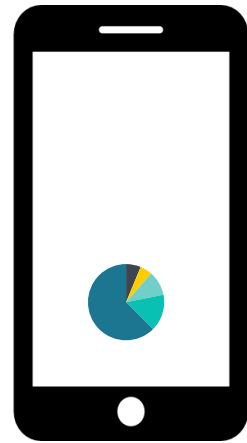
10:00 – 10:10 Welcome Remarks by
Christiane Kirketerp de Viron

1

Christiane Kirketerp de Viron,
Acting Director for Cybersecurity
and Trust, DG CONNECT,
European Commission

Launch of CRA Website and FAQ

[Cyber Resilience Act - Implementation | Shaping Europe's digital future](#)



Cyber Resilience Act - Implementation

Introducing the Cyber Resilience Act: the EU's new plan to make sure all digital products on the EU market are safe from cyber threats. This important rulebook covers the security of products considering their lifecycle. It requires that devices and software are designed, updated, and maintained to protect users in our increasingly digital world.

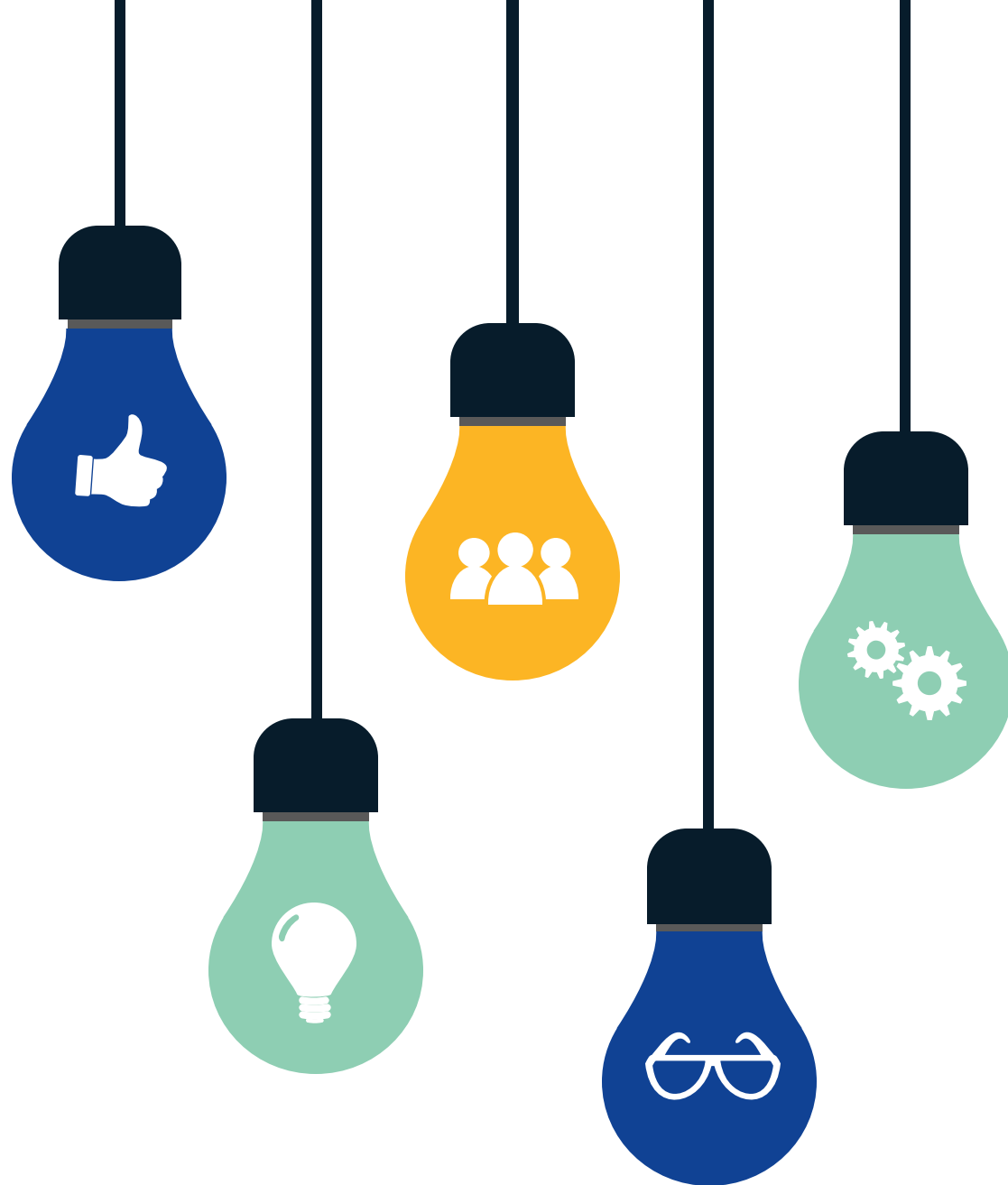
CYBER RESILIENCE ACT

#EU #Cybersecurity

Overview

Cybersecurity is a collective effort. The European Commission is closely working with the industry, Member States, and the [European Union Agency for Cybersecurity \(ENISA\)](https://www.enisa.europa.eu/) on the implementation of the Cyber Resilience Act (CRA).

AGENDA



10:10 – 10:50 Presentations by the
European Commission

2

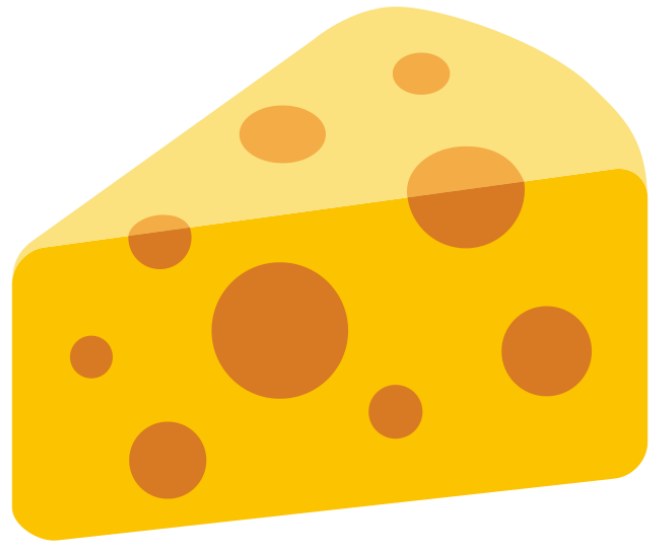
- **The CRA explained: objectives, scope, and practical implications**

- Cooperation across institutions, industry and Member States: who does what

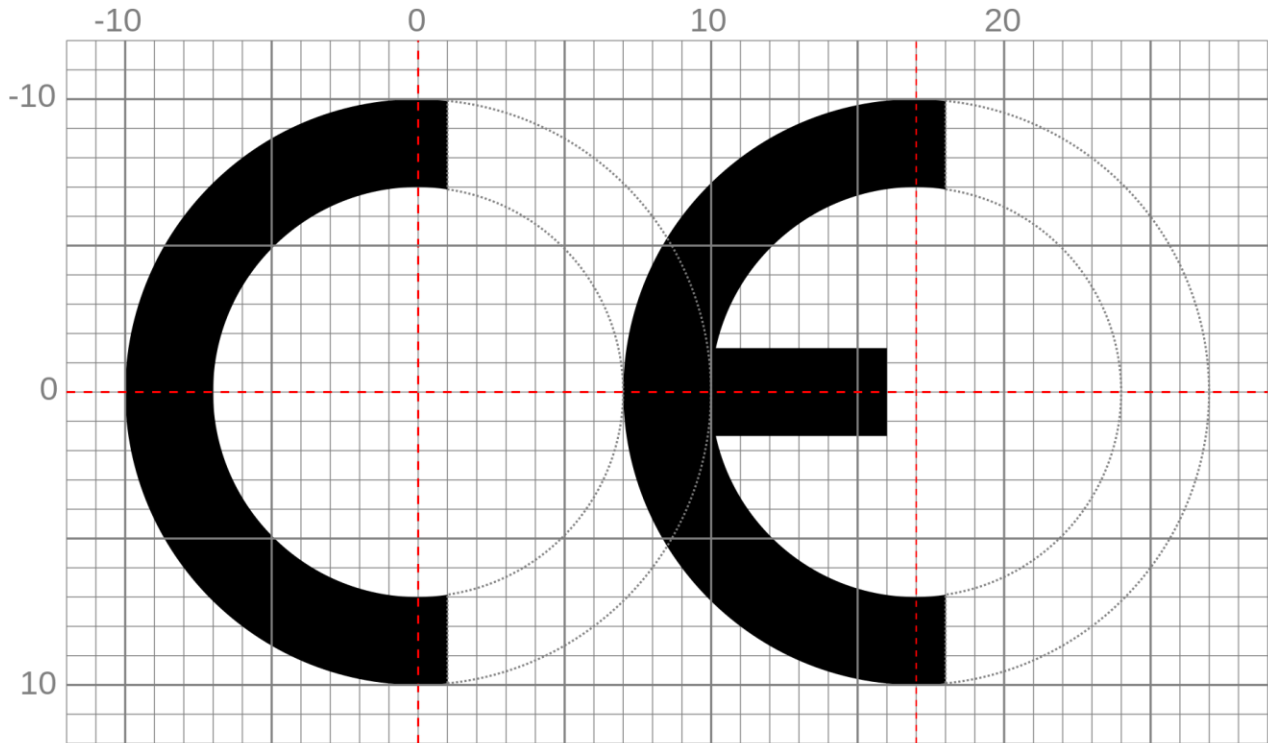
- Turning CRA into reality: key phases of the implementation phase, guidance, and ongoing regulatory efforts

- Q&A (15 min)

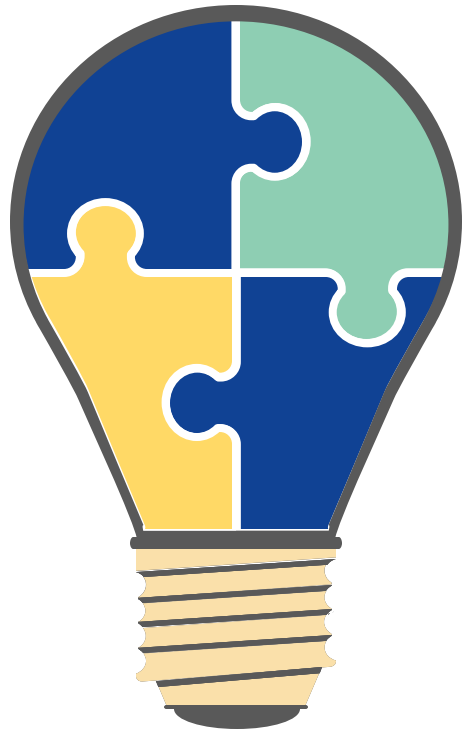
The CRA in a nutshell



CE marking



Main elements of the law



**Obligations for manufacturers,
distributors and importers**

**Cybersecurity rules for placing
products on the market and
during lifecycle**

Conformity assessment

Market surveillance and enforcement

In scope: “products with digital elements”



Hardware products (including components placed on the market)
(laptops, smart appliances, mobile phones, network equipment or CPUs...)



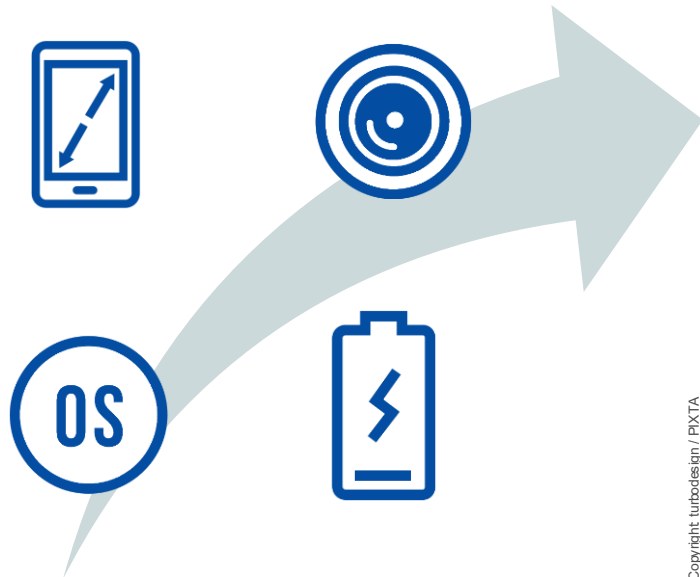
Software products (including components placed on the market)
(operating systems, word processing, games or mobile apps, software libraries...)

...including their **remote data processing solutions!**

Supply chain cooperation

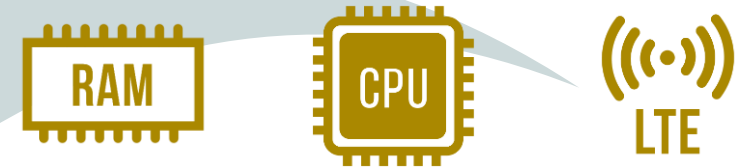
As a rule, whoever places on the market a “final” product or a component is required to comply with the essential requirements, undergo conformity assessment and affix the CE marking.

Developed by the manufacturer placing the smartphone on the market:



Copyright turbodesign / PIXTA

Developed by upstream manufacturers for integration into the “final” product:



Outside the scope



Non-commercial products

(hobby products)



Services, including standalone SaaS (i.e. not associated to a product with digital elements) (websites, purely web-based offerings...)



Outright exclusions

(cars, medical devices, in vitro, certified aeronautical equipment, marine equipment)

Reporting obligations

Manufacturers to report to the CSIRTs via a **single reporting platform** using national electronic notification end-points:



Actively exploited **vulnerabilities**



Severe **incidents** having an impact on the security of the product

Conformity assessment classes – not exhaustive!



Default category — self-assessment

(memory chips, mobile apps, smart speakers, computer games...)



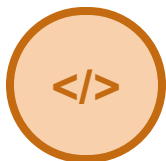
Important products — application of standards/third-party assessment

(operating systems, anti-virus, routers, firewalls...)



Critical products — third party assessment (in the future potentially certification)

(smart cards, secure elements, smart meter gateways...)



FOSS — self-assessment (unless categorized as “critical products”)

(web development frameworks, operating systems, database management systems...)

Market surveillance activities



Enforcement is key to ensure the credibility of the CRA



Market surveillance is a national competence > **market surveillance authorities (MSA)**

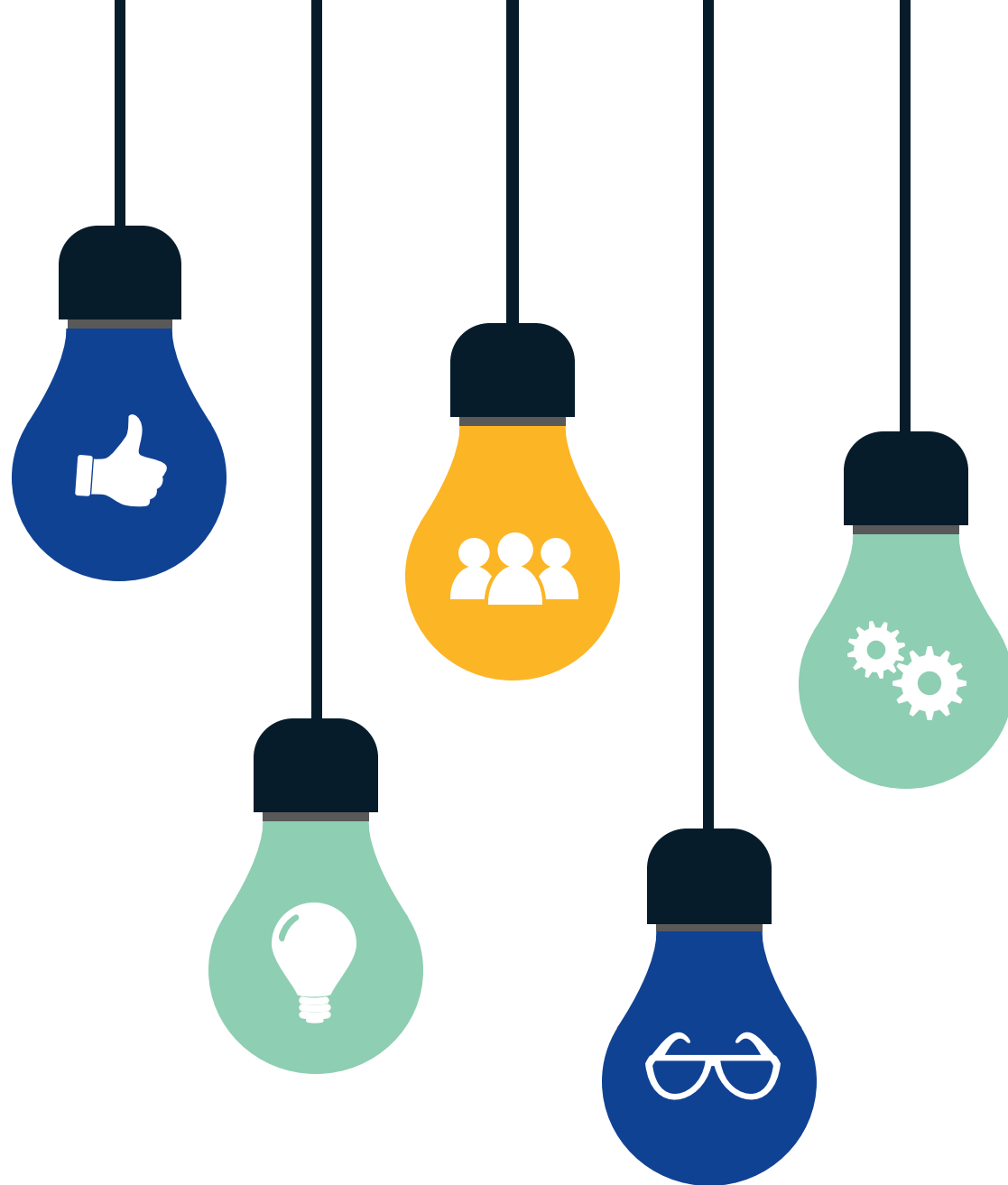


The Commission will propose a **strategic, objective and evidence-based approach** to ensure an efficient enforcement of the CRA



Cybersecurity, being a borderless field, requires strong **cooperation** among Member States

AGENDA



10:10 – 10:50 Presentations by the
European Commission

2

- The CRA explained: objectives, scope, and practical implications

- Cooperation across institutions, industry and Member States: who does what**

- Turning CRA into reality: key phases of the implementation phase, guidance, and ongoing regulatory efforts

- Q&A (15 min)

CRA implementation underway

European Commission



**European Cybersecurity
Competence Center**



Member States



**European Standardisation
Organisations**



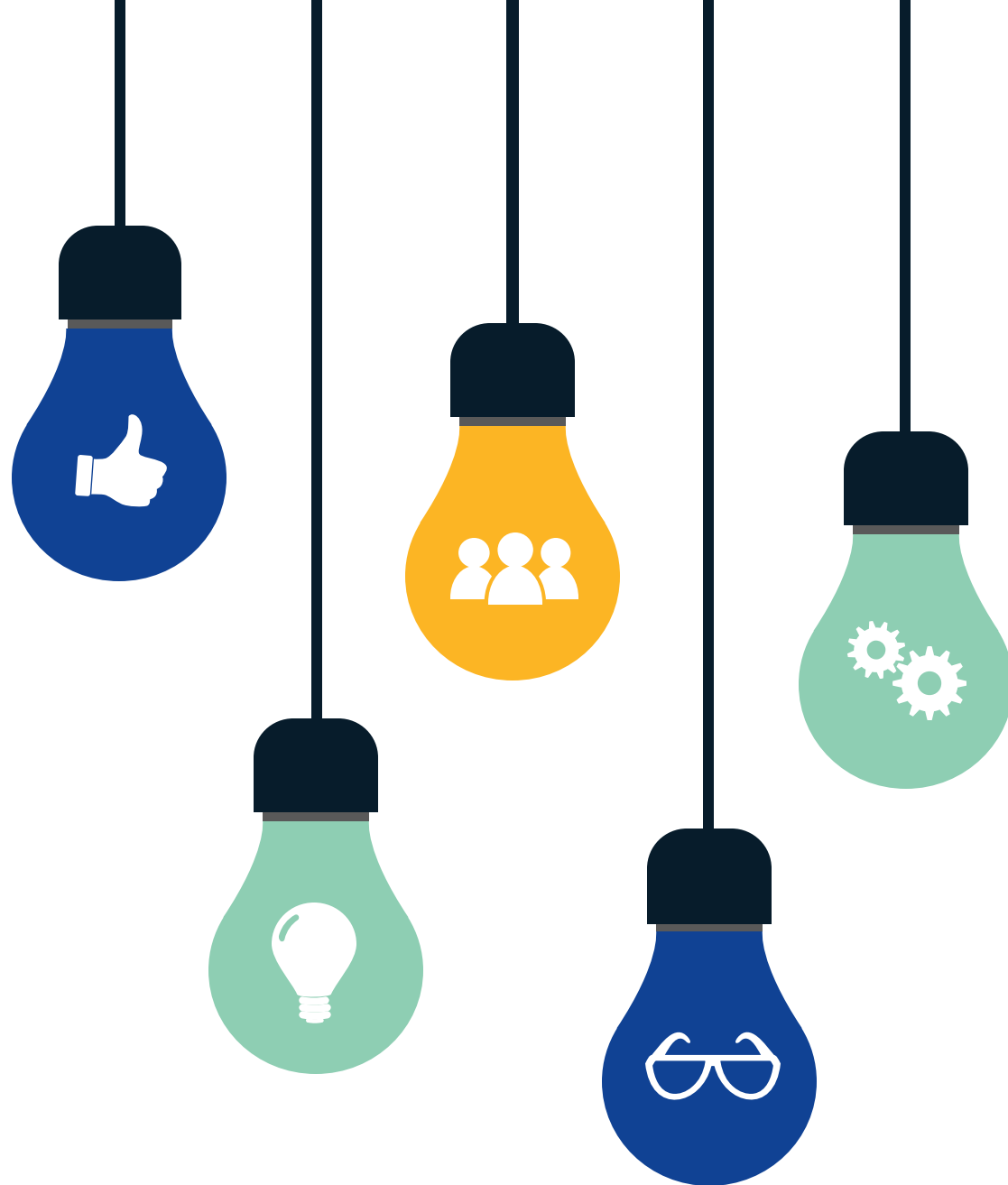
**ENISA – EU Agency for
Cybersecurity**



Businesses



AGENDA



10:10 – 10:50 Presentations by the
European Commission

2

- The CRA explained: objectives, scope, and practical implications
- Cooperation across institutions, industry and Member States: who does what
- Turning CRA into reality: key phases of the implementation phase, guidance, and ongoing regulatory efforts**
- Q&A (15 min)

CRA implementation underway

- ❖ Guidance (COM)
- ❖ Implementing & delegated acts (COM & Member States)
- ❖ Standardisation (COM, Member States & industry)
- ❖ Single Reporting Platform (ENISA & Member States)
- ❖ Projects funded by the EU (COM, ECCCC, MS & industry...)
- ❖ Stakeholder consultations & CRA Expert Group (industry)

Upcoming milestones (tentative)

2025

Standardisation request
Launch of CRA expert group
First MS meetings

- Legal acts on CRA product categories & reporting obligations

2026

First set of CRA guidelines
First standards
Single Reporting Platform
First notified bodies

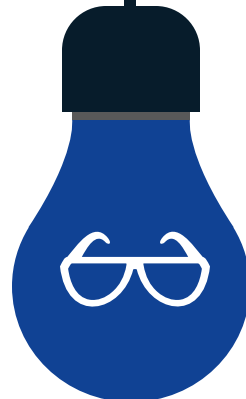
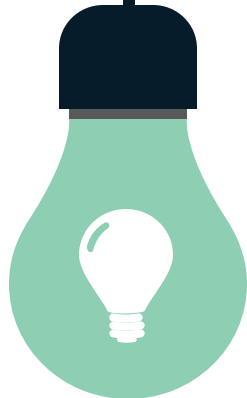
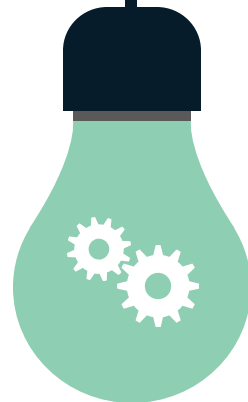
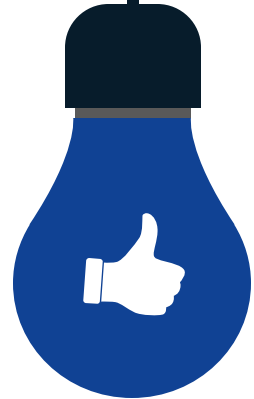
- More legal acts & guideline

2027

11 Dec.:
Full Application

- More legal acts, guidelines & Standards

AGENDA



10:00 – 10:10 Welcome Remarks by
Christiane Kirketerp de Viron

1

10:10 – 10:50 Presentations by
the European Commission

2

**10:50 – 11:20 State of the play of
the standardisation work supporting the CRA**

3

11:20 – 11:50 Making the CRA fit for SMEs

4

Slido Poll

Get ready for your Slido poll



**Do you feel well-
informed about the
CRA standardisation
process work on the
CRA?**

- 1) Yes
- 2) No

Slido Poll

Get ready for your Slido poll



**Is your organisation
involved in the drafting
of CRA standards?**

- 1) Yes
- 2) No

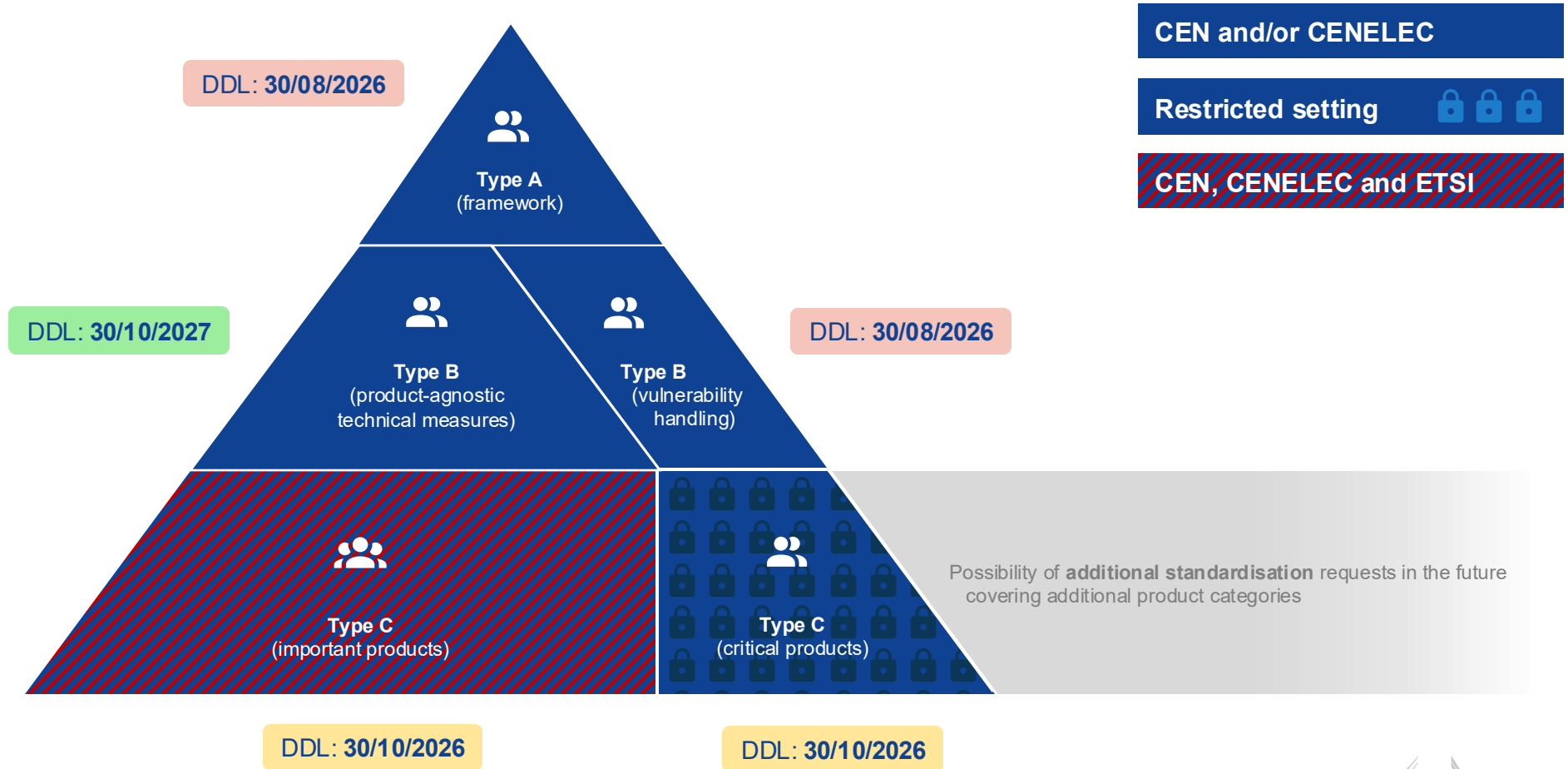
The role of standards in the CRA

- ❖ NLF approach: essential requirements in the legislation, technical aspects further detailed in harmonised standards
- ❖ Benefit of the use of harmonised standards for manufacturers: presumption of conformity with the CRA essential requirements
- ❖ Additional benefit for products listed in Annex III Class I: self-assessment possible

CRA standardisation request

- ❖ Standardisation request for harmonised standards addressed to three European Standardisation Organisations (CEN, CENELEC, ETSI)
- ❖ Building on existing international and European standards
- ❖ 2-tiered approach: horizontal and vertical standards
- ❖ Prioritising important/critical products (CRA Annex III/IV)
- ❖ First building blocks for product security ecosystem of standards

CRA standardisation request (2)



AGENDA



11:20 – 11:50 Making the CRA fit for SMEs

4

•Introduction by European Commission

- Presentation by European projects: CYBERSTAND.eu (Nicolas Ferguson) & SECURE (Danilo D'elia)
- Q&A (15 min)

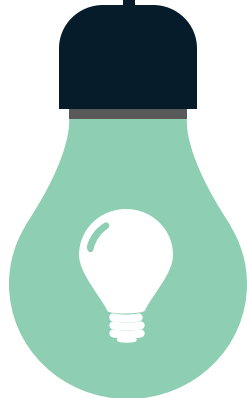
Support measures for MSMEs

**Risk-based and
proportionate
approach in
CRA**

**Role of ENISA,
Member States,
the Commission
(Article 33 CRA)**

**Guidance,
Trainings,
Awareness
raising**

For further information



Introducing the Cyber Resilience Act: the EU's new plan to make sure all digital products on the EU market are safe from cyber threats. This important rulebook covers the security of products considering their lifecycle. It requires that devices and software are designed, updated, and maintained to protect users in our increasingly digital world.



CRA website

[Cyber Resilience Act - Implementation | Shaping Europe's digital future](#)

[Summary of legal text](#)

[FAQ on CRA implementation](#)

How to stay in touch:

<https://ec.europa.eu/eusurvey/runner/CRA-implementation>

Thank you.