

European Standardization Organizations

Webinar 'Standards supporting the Cyber Resilience Act'

*We start at
10:00 CET*

Webinar moderator



Els SOMERS

Project Manager

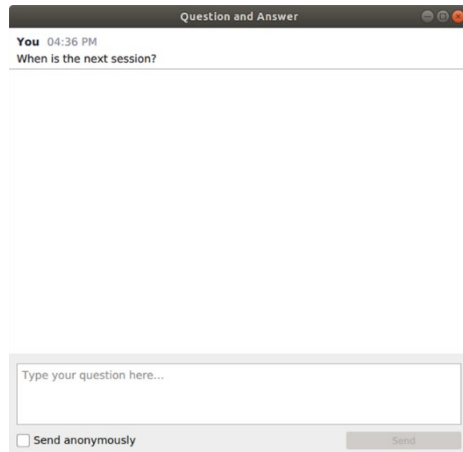
Public Relations

CEN-CENELEC

esomers@cencenelec.eu

Get the most out of the webinar today

- ▶ You are muted
- ▶ Use the Q&A panel to submit your questions



The screenshot shows a 'Question and Answer' panel. At the top, it says 'You 04:36 PM' and 'When is the next session?'. Below this is a large empty text area for typing a question. At the bottom, there is a text input field with the placeholder 'Type your question here...', a checkbox labeled 'Send anonymously', and a 'Send' button.

- ▶ Talk about us with [#training4standards](#)
 - ▶ On X [@Standards4EU](#)
 - ▶ On Bluesky [@cen-cenelec.bsky.social](#)
 - ▶ On LinkedIn www.linkedin.com/company/cen-and-cenelec

- Welcome – house keeping rules
- Introduction to the CRA Standardization Request, by Filipe Jones Mourão - DG CNECT
- CEN and CENELEC work on the CRA standards, by Lucia Lanfri – CEN and CENELEC
- Horizontal standards development: Principles for cyber resilience and vulnerability handling, by Simon Steendam, CEN-CLC/JTC 13 WG 9 representative
- Industry's view: implementation of the CRA by manufacturers, by Steffen Zimmermann
- Closing remarks, Cyber Resilience Act and the horizontal standards workshop, by Berit Aadal

Your speakers today



Lucia LANFRI
Project Manager Electrotechnology
Standardization & Digital Solutions



Filipe JONES MOURÃO
DG CNECT
European Commission



Berit AADAL
Chief Consultant
Danish Standards



Simon STEENDAM
CEN-CLC/JTC 13 WG 9



Steffen ZIMMERMANN
Head of Industrial Security,
VDMA, Germany

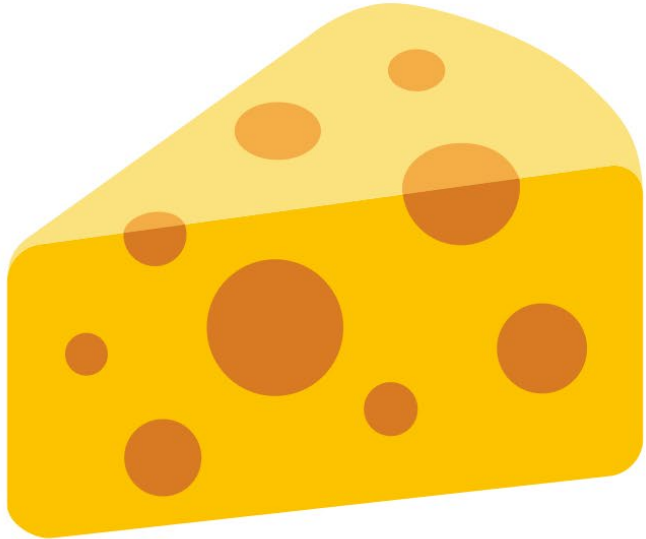


Cyber Resilience Act

CNECT.H2

European Commission, DG CONNECT

CRA in a nutshell



Main elements of the law

- ❖ **Cybersecurity rules** for the placing on the market of hardware and software
- ❖ **Obligations** for manufacturers, distributors and importers
- ❖ Cybersecurity **essential requirements** across the life cycle
- ❖ Harmonised **standards** to follow
- ❖ **Conformity assessment** – differentiated by product category
- ❖ **Reporting** obligations
- ❖ **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!**

Outside the scope



Non-commercial products

(hobby products)



Services, in particular standalone SaaS (covered by NIS2)

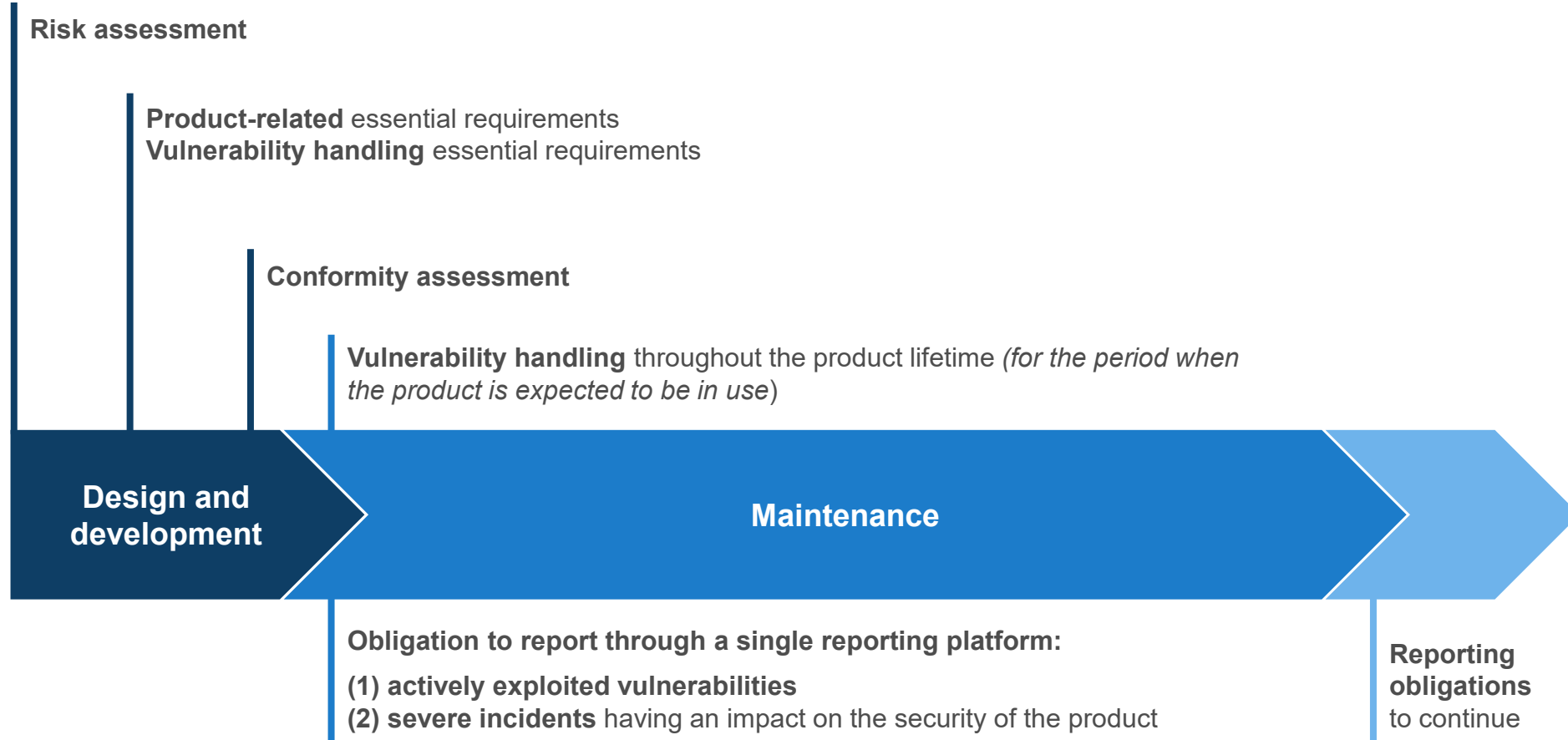
(websites, purely web-based offerings...)



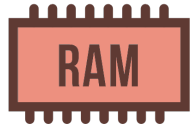
Outright exclusions

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

Obligations of manufacturers



Conformity assessment – product categorisation



Default category — self-assessment

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



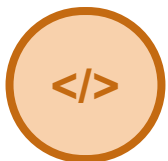
Important products — application of standards/third-party assessment

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



Critical products — 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...)

CRA implementation underway

- ❖ Development of harmonised standards
- ❖ Technical descriptions of important and critical products
 - ❖ *To be adopted by 11 December 2025*
- ❖ Terms and conditions for CSIRTs to withhold notifications
 - ❖ *To be adopted by 11 December 2025*
- ❖ Single Reporting Platform by ENISA
 - ❖ *To be operational by 11 September 2026*

CRA implementation underway - continued

- ❖ Guidance to support implementation
 - ❖ *Covering at least RDPS, OSS, support period, interplay with other Union legislation, substantial modification + targeting SMEs*
- ❖ Member States to set up notifying & market surveillance authorities
- ❖ CRA Expert Group
 - ❖ First meeting on 12 February; additional fora for involvement

CRA implementation – SME support

- ❖ Support measures in Art. 33 – may include:
 - ❖ Member States to organise awareness-raising & support testing and conformity assessment activities
 - ❖ Regulatory sandboxes
 - ❖ Empowerment for simplified technical documentation
- ❖ Support under Digital Europe Programme

Standardisation

- ❖ Standardisation request for harmonised standards adopted by COM and notified to ESOs
- ❖ 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

Deliverables requested

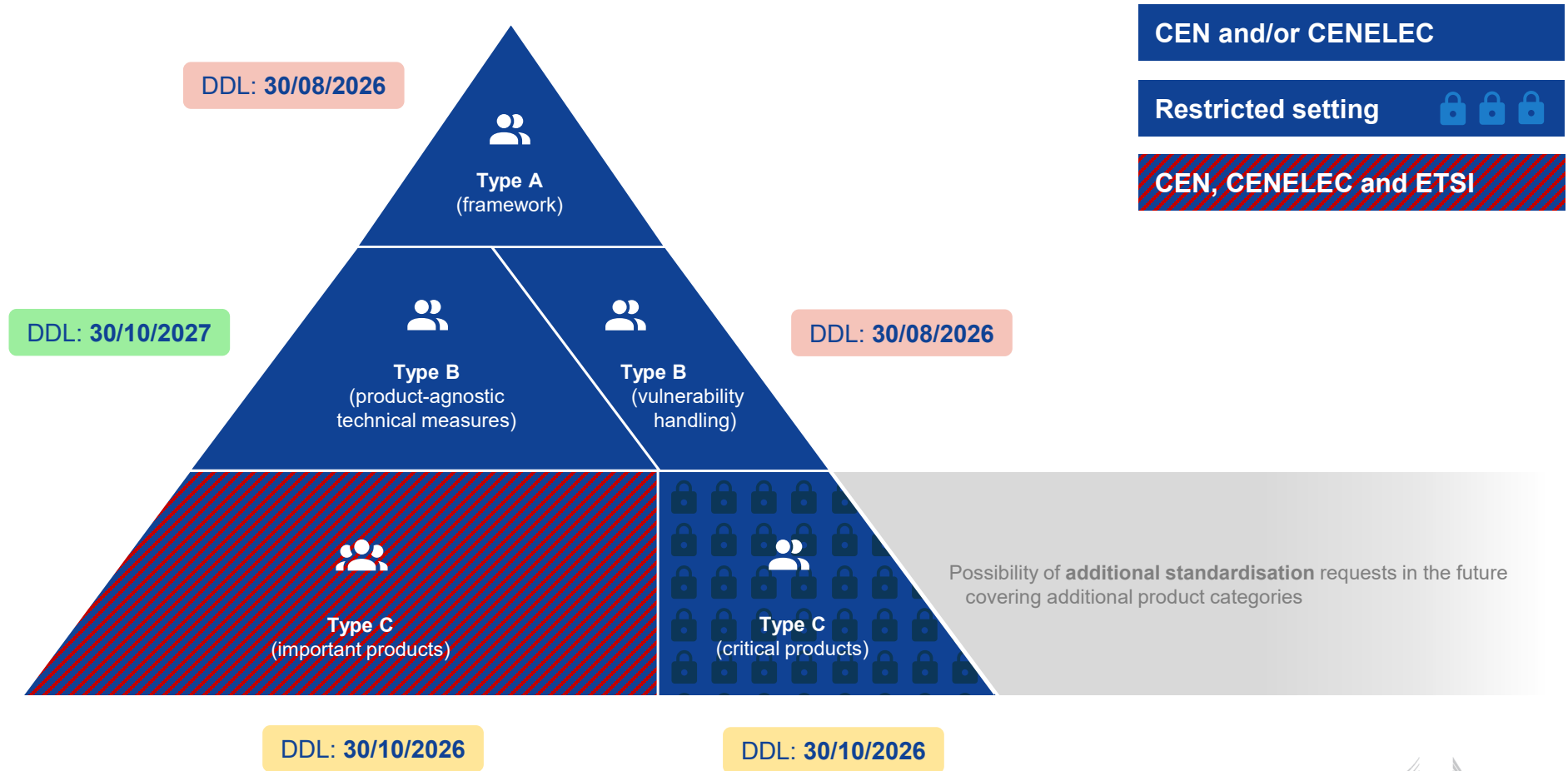
❖ **Horizontal standards (1-15)**

- ❖ Risk-based approach (CRA Annex I)
- ❖ Essential Requirements (CRA Annex I part 1)
- ❖ Vulnerability Handling (CRA Annex I part 2)

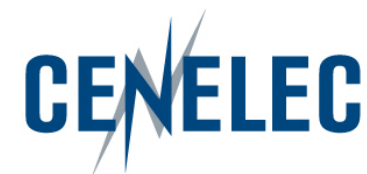
❖ **Vertical standards (16-41)**

- ❖ Important products class 1 (CRA Annex III)
- ❖ Important products class 2 (CRA Annex III)
- ❖ Critical products (CRA Annex IV)

CRA standardisation request in a nutshell



Thank you.



STAN4CR

European Standards
supporting the Cyber
Resilience Act

European Standardization Organizations

CRA Standardization Request

Lucia Lanfri, Project Manager CEN-CENELEC



Who we are?



- ▶ CEN and CENELEC are two out of the three European Standards Organizations (ESOs) together with ETSI
- ▶ CEN, CENELEC and ETSI officially **recognised** as European Standards Organizations ([Regulation EU 1025/2012](#))



Standardization in various business sectors



Standardization in the Electrotechnology sector



Telecommunications, broadcasting and other electronic communications networks and services

CEN and CENELEC members in 34 countries



Austria



Denmark



Greece



Latvia



Poland



Slovenia



Belgium



Estonia



Hungary



Lithuania



Portugal



Spain



Sweden



Bulgaria



Finland



Iceland



Malta



Republic of North Macedonia



Switzerland



Croatia



France



Ireland



Serbia



Türkiye



Czech Republic



Germany



Italy



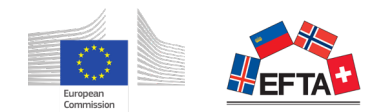
Norway



Slovakia



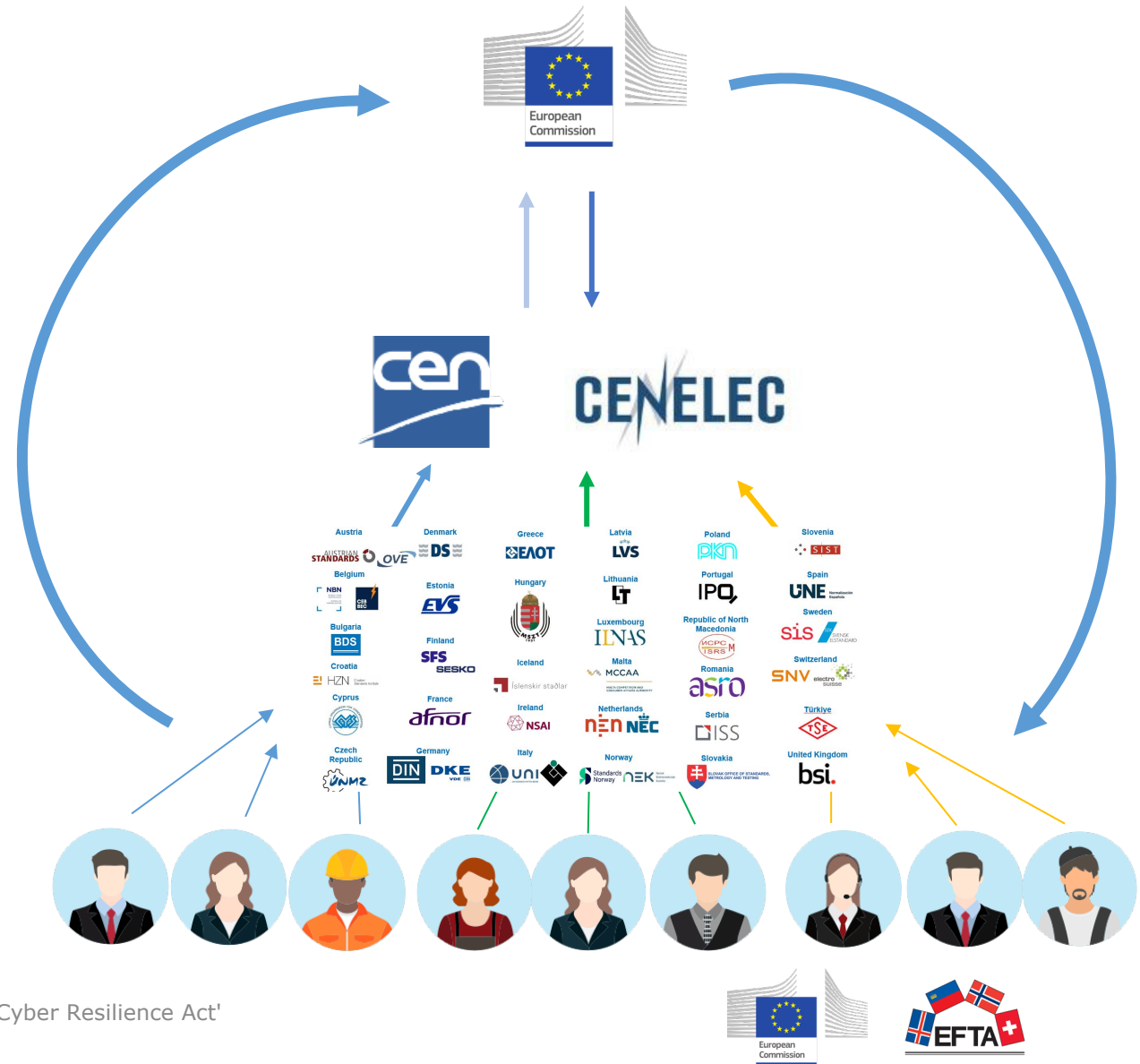
United Kingdom



An inclusive system based on dialogue



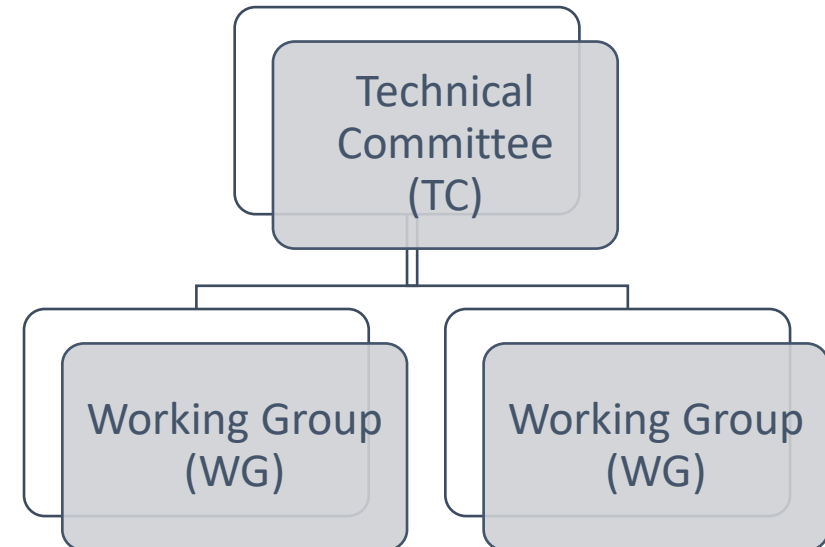
- ▶ Based on the national delegation principle
- ▶ Representing a consensus among all interested parties, including industry & SMEs and societal stakeholders
- ▶ Standards are voluntary
- ▶ 1 standard for all CEN & CENELEC members **'Stand Still Rule'!**



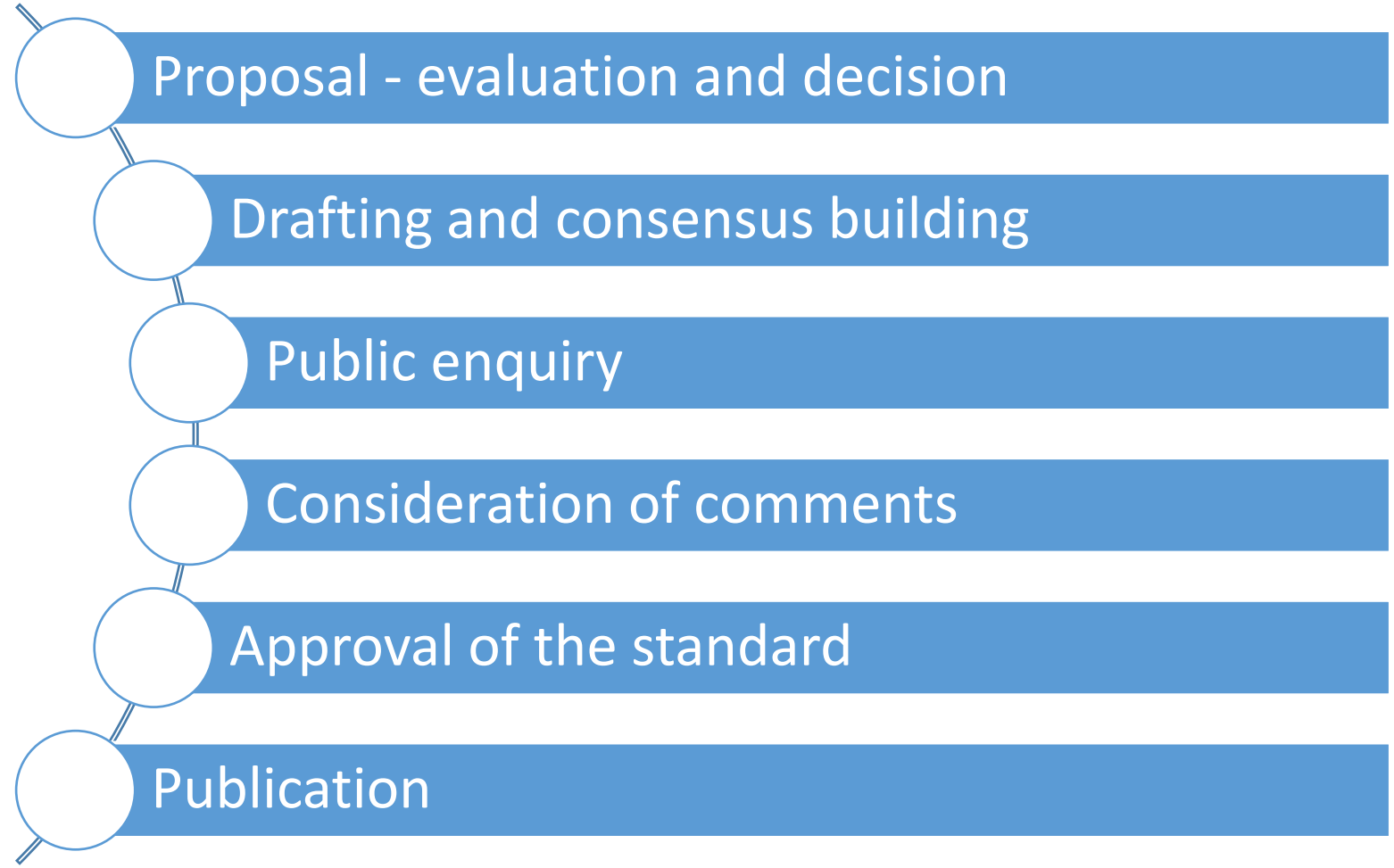
How is the work organized?



- ▶ The standards are developed in Technical Committees (TC)
- ▶ Each TC has Working Groups (WGs)
- ▶ Each WG has a dedicated scope



How are standards made?

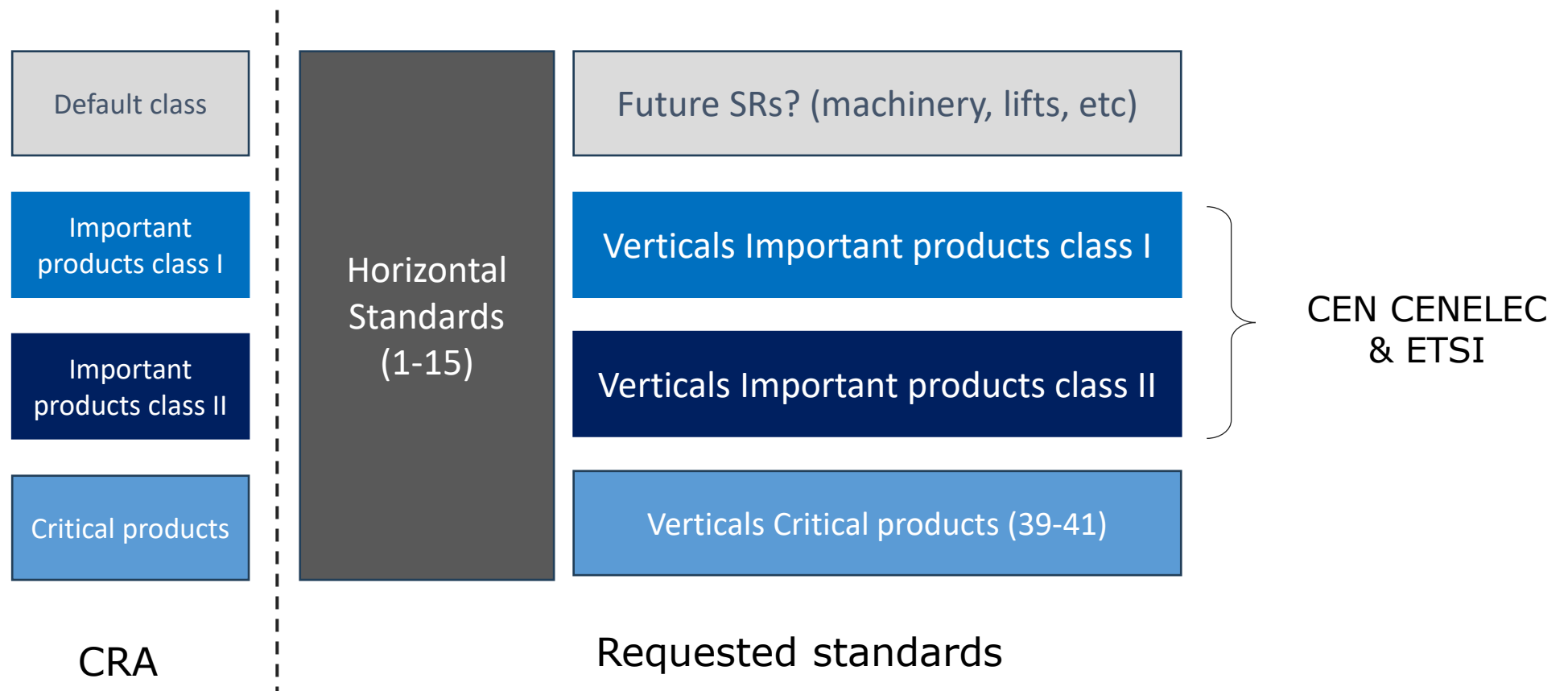


What is a harmonized standard?



- ▶ A harmonized standard is a European standard developed by recognized European Standards Organizations.
- ▶ It is created following a request from the European Commission to one of these organizations → Standardization Requests
- ▶ Their use is voluntary
- ▶ Manufacturers, other economic operators, or conformity assessment bodies can use harmonized standards to demonstrate that products, services, or processes comply with relevant EU legislation. They are free to choose another technical solution to demonstrate compliance with the mandatory legal requirements.
- ▶ The CRA is a first of its kind regulation, so no standards currently exist that specifically cover the CRA essential requirements.

Requested standards



CEN CENELEC and ETSI joint work

- ▶ Lines #16-38
- ▶ Ongoing exchanges between CEN CENELEC ETSI and the relevant technical bodies
- ▶ Collaboration mode-4 as a starting point to facilitate exchange between CEN CENELEC and ETSI
- ▶ Basis for the work programme (Article 3 SReq)

Horizontal developments CEN-CLC TCs



For discussion purposes only
DRAFT

- ▶ **CEN-CLC/JTC 13 WG 9 “Special Working Group on Cyber Resilience Act’**
 - ▶ Principles for cyber resilience (line 1)
 - ▶ Generic Security Requirements (line 2-14)
 - ▶ Vulnerability handling (line 15)

Vertical developments CEN-CLC TCs

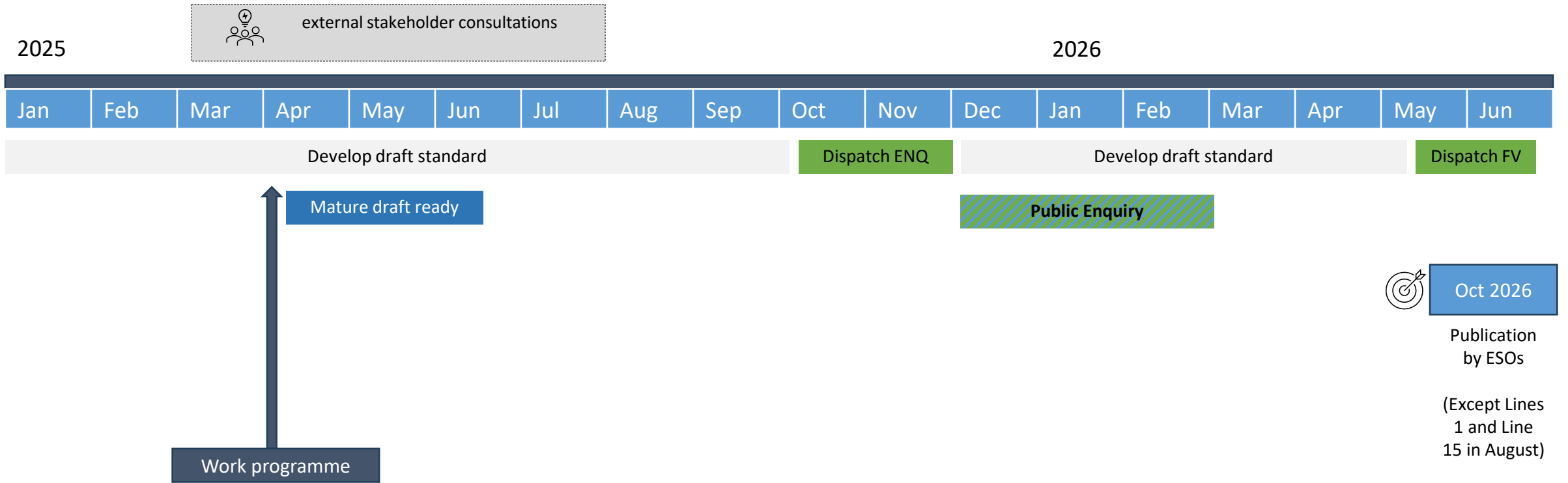
- ▶ **CEN/TC 224 'Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment'**
 - ▶ European standard(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers (line 16)
 - ▶ European standard(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes (line 39)
- ▶ **CLC/TC 65X 'Industrial-process measurement, control and automation'**
 - ▶ Developments based on EN IEC 62443-4-2
- ▶ **CEN-CLC/JTC 13 WG 6**
 - ▶ European standard(s) on essential cybersecurity requirements for smart meter gateways within smart metering systems (line 40)
 - ▶ European standard(s) on essential cybersecurity requirements for hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments (Line 35)


Vertical developments CEN-CLC TCs

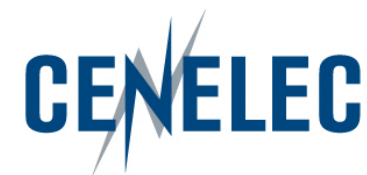
▶ **CLC/TC 47X 'Semiconductors and Trusted Chips Implementation'**

- ▶ European standard(s) on essential cybersecurity requirements for tamper-resistant microprocessors and microcontrollers (lines 37 & 38)
- ▶ European standard(s) on essential cybersecurity requirements for microprocessors and microcontrollers with security-related functionalities (lines 28 & 29)
- ▶ European standard(s) on essential cybersecurity requirements for application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) security-related functionalities (line 30)
- ▶ European standard(s) on essential cybersecurity requirements for smartcards or similar devices, including secure elements (shared with CEN/TC 224) (line 41)

High level expected timeline



 **Oct 2026**
Publication by ESOs
(Except Lines 1 and Line 15 in August)



STAN4CR

European Standards
supporting the Cyber
Resilience Act

European Standardization Organizations

CRA Standardization Request

Simon Steendam, STAN4CR Rapporteur



Introduction

-Who am I



Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken



- ▶ Dutch Authority for Digital Infrastructure
- ▶ Future Market Surveillance Authority for the CRA in the Netherlands
- ▶ Rapporteur under the STAN4CR project for the standard: General Principles for Cyber Resilience

Introduction – The work

- ▶ **Horizontal standards**
 - ▶ Developed under CEN/CLC JTC13 WG9
 - ▶ Applicable to the full scope of the CRA
 - ▶ Provide elements for the vertical standards
- ▶ **Vertical standards**
 - ▶ Developed under applicable CEN/CLC working groups
 - ▶ Developed under applicable ETSI working groups
 - ▶ Applicable to only specific product categories (CRA Annex III/IV)
 - ▶ Grant presumption of conformity

Introduction – Working Group 9

- ▶ Special Working Group for the CRA.
- ▶ Building horizontal standards as a basis for future standards
- ▶ One Project Team (PT) for each requested standard
- ▶ PT1: General Principles for Cyber Resilience
- ▶ PT2: Generic Security Requirements
- ▶ PT3: Vulnerability Handling
- ▶ Coordinate with ETSI CYBER for a coherent approach

The horizontals

- ▶ European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks
- ▶ European standard(s) on vulnerability handling for products with digital elements

Introduction – Products with Digital Elements (PwDE)

- ▶ A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately



Introduction – Design Develop and Producing



- ▶ The standardization request requests that cybersecurity risks are addressed across the planning, design, development, production, delivery and maintenance phases of the product
- ▶ The standard is to cover the lifecycle as a whole to enable appropriate cybersecurity for all phases of the lifecycle of a Product with Digital Elements
- ▶ The lifecycle is important as the threat landscape of a product with digital elements changes

Introduction – Appropriate level of cybersecurity based on Risk

- ▶ The need for the risk-based approach
- ▶ Mitigate proportionally and appropriately
- ▶ The standardization request specifically requests the state of the art is reflected in the standard
- ▶ This minimizes cybersecurity risks and impacts
- ▶ A process standard focused on basic hygiene

General Principles for Cyber Resilience

- ▶ High level principles of cybersecurity
 - ▶ Risk based approach
 - ▶ Security by Design
 - ▶ Security by Default
 - ▶ Transparency
- ▶ Risk management is key
- ▶ Activities as indicators, Clean kitchen clean product
- ▶ Provide a framework to support the creation of (future) vertical standards

Vulnerability Handling

- ▶ Critical part of a risk-based approach
- ▶ A process standard focused on the changing threat landscape
- ▶ Interplay with the General Principles for Cyber Resilience
- ▶ Vulnerability handling:
 - ▶ Detect
 - ▶ Determine
 - ▶ Deal with
 - ▶ Deploy

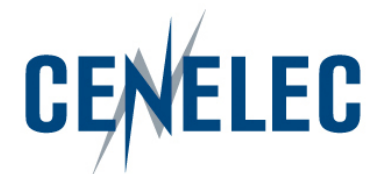
Timeline

- ▶ Horizontal deadlines for 30-08-2026
- ▶ Vertical deadlines for 30-10-2026
- ▶ Enquiry end of Q3 2025
- ▶ Formal vote medio 2026

Workshop: Cyber Resilience Act and the horizontal standards



- ▶ 8 April 2025
- ▶ Online/Tivoli Hotel Copenhagen
- ▶ Join us for a more in-depth overview of the CRA and standardization
- ▶ Workshop a Product with Digital Elements under the CRA
- ▶ Explore case-based Vulnerability Handling



European Standardization Organizations

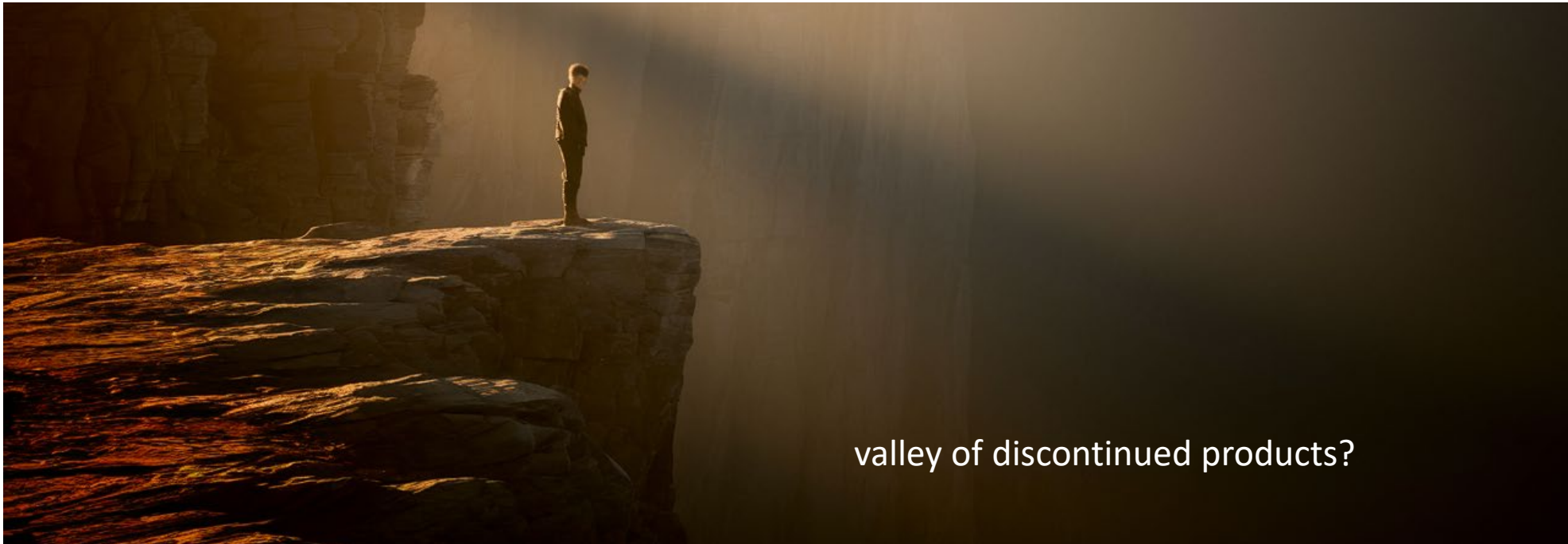
Manufacturer's View on CRA & Standards

Steffen Zimmermann, VDMA (vertical / machinery)



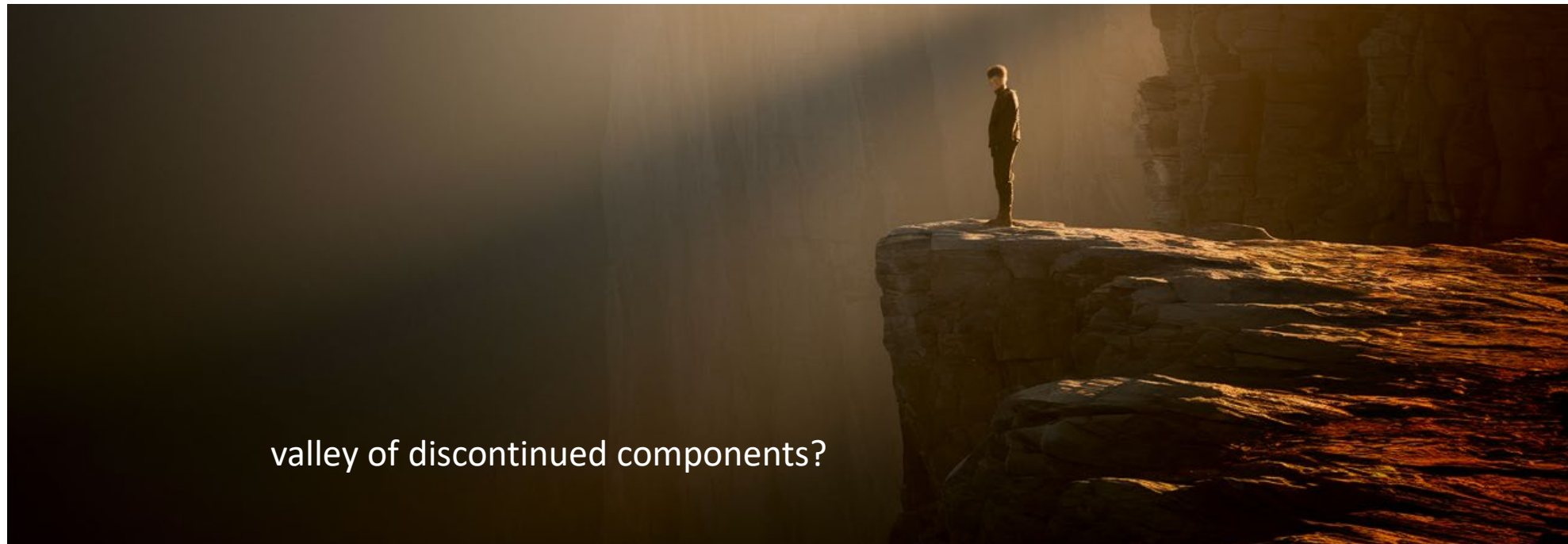
Supplier: component view

- ▶ Can I still sell my fully developed product series in 2028?
- ▶ Is my in-development product compliant in 2028?



Machinery: system integrator view

- ▶ Is my in-development product compliant in 2028?
- ▶ Can I still buy components for contracted systems in 2028?



How to fill this gap?



Important products and hEN



Why to engage?

▶ Time

- ▶ 41 standards – 15 horizontal and 26 vertical standards
- ▶ Broad vertical standards “improvement” (OT)

▶ Context

- ▶ Multiple purposes (e.g. MR, NIS2)
- ▶ Product-specific for Annex III/IV

▶ Content

- ▶ Participate via your National Standardization Body/EU Funding
- ▶ Early access

How to engage?

- ▶ We need experts in products
- ▶ Find your CEN/CLC national mirror committee
 - ▶ Germany: „DIN/DKE Gemeinschaftsgremium Cybersecurity“
 - ▶ France: „AFNOR/CN CYBERSECURITE“
 - ▶ Ask Lucia 😊 or look at cencenelec.eu
- ▶ Ask ETSI directly via cybersupport@etsi.org
- ▶ Apply for funding via cyberstand.eu
- ▶ Attend the upcoming webinars and workshops
- ▶ Meetings are always hybrid – no need to travel

Cyber Resilience Act and the horizontal standards

Berit Aadal, Chief Consultant, Danish Standards

Workshop on 8 April 2025 Copenhagen/online

The workshop is part of the STAN4CR project, funded by EISMEA (European Innovation Council and SMEs Executive Agency), The STAN4CR plays a pivotal role in the drafting process of harmonised standards to support CRA compliance.

The STAN4CR project aims to raise public awareness and actively involve key stakeholders in the standardization process.

The workshop and the STAN4CR project are funded by the European Union through the European Innovation Council and SMEs Executive Agency (EISMEA), under Grant Agreement No. 101196779.



Workshop on 8 April 2025

Copenhagen/online



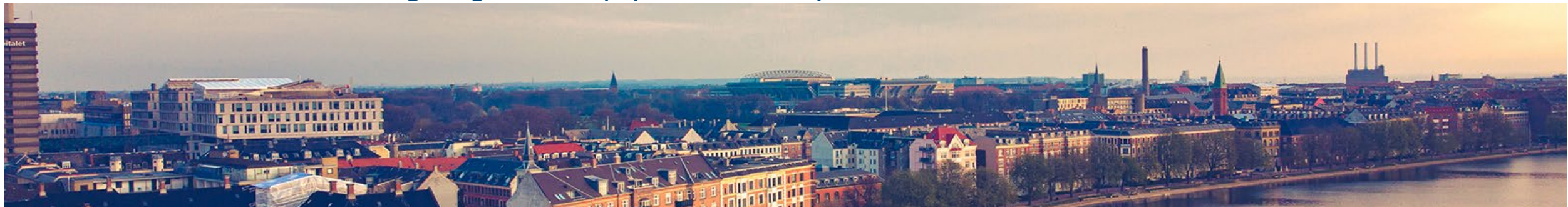
Focus

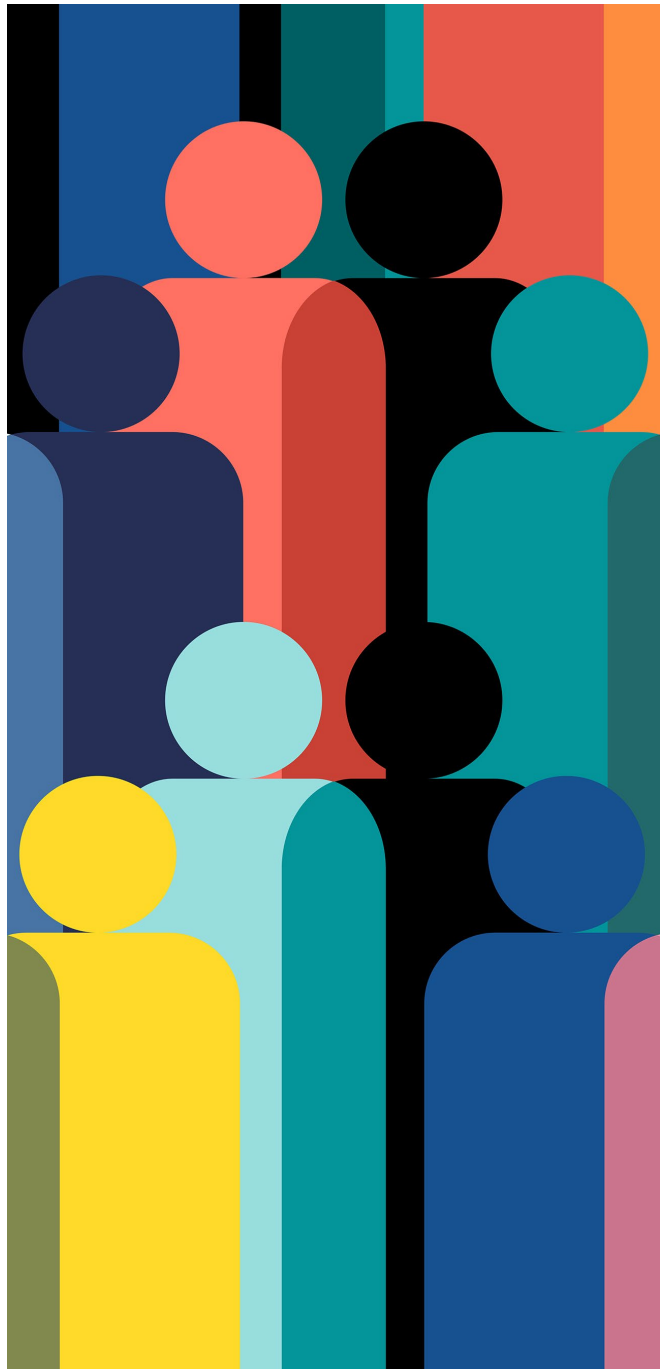
The workshop will address lines 1 and 15 in the Standardization Request:

- Line 1: European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on risks
- Line 15: European standard(s) on vulnerability handling for products with digital elements

Main objective

Present the preliminary content of the horizontal standards being developed to comply with lines 1 and 15 in the Standardization Request. And to receive feedback and input from stakeholders that are going to comply with the Cyber Resilience Act.





Workshop on 8 April 2025 Copenhagen/online

Target group

Manufacturers and distributors of products with digital elements covered by the CRA, and other stakeholders eager to share their expertise to help shape the future CRA standards.

Why should you participate?

The workshop provides a unique platform for you to influence the development of the horizontal CRA standards and share your expertise, insights, and experiences. By participating, you will have the opportunity to shape the future of cybersecurity practices and ensure that the standards developed are comprehensive, practical, and effective.

Workshop on 8 April 2025

Copenhagen/online

Draft agenda

10.00 Welcome

10.10 A brief overview of the Cyber Resilience Act (CRA), key elements, requirements, and the significance of standardization

10.30 A short introduction to standardization

10.45 Coffee break

11.05 Presentation of the workshop's goal

11.15 **Workshop round 1: Principles for cyber resilience**

13.00 Lunch

14.00 **Workshop round 2: Vulnerability handling**

15.45 Coffee break

16.05 Case presentation: Implementing standards – preparation for the CRA in a global company

16.35 Next steps for the standardization development

16.55 Goodbye and thank you - networking and drinks

Workshop on 8 April 2025 Copenhagen/online

Date

8 April 2025 from 9.30 AM to 5.30 PM

Location

Tivoli Hotel, Copenhagen, Denmark / online

Registration (Required)

<https://www.ds.dk/en/our-services/workshop-cyber-resilience-act>

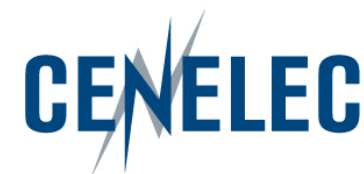
Questions?

Please contact Berit Aadal, baa@ds.dk





DANSK STANDARD



European Standardization Organizations

Thank you for your participation!

Upcoming webinars/events

2025-03-12 - Webinar [`How can CEN/TC 442 support digitalization of data in design & product standards`](#)

2025-03-18 - [`Cyber Resilience Act : deep dive session`](#)

2025-03-20 - Conference [`European standardization supporting new legislative cybersecurity landscape`](#)

2025-04-08 - Hybrid event [`Cyber Resilience Act and the horizontal standards - CEN-CENELEC`](#)