

European Standardization Organizations

Cyber Resilience Act and the horizontal standards

Workshop in Copenhagen

8 April 2025



Welcome

Anne Holm Sjøberg
Danish Standards



Danish Standards – a strong player in a European and global standardization network



A standard is a solid basis for achieving compliance, safety, development and efficiency.



A standard is your basis for:

Compliance

Standards help comply with national and international legislation and requirements for documentation, quality, and best practice. This builds trust among customers and other stakeholders.



A standard is your basis for:

Safety

Standards help ensure that your products and practices meet the safety requirements of the outside world. This provides peace of mind for employees, customers and consumers.



A standard is your basis for:

Development

Standards help ensure that your innovation and development is built on recognised principles. This gives you a lead when developing your organization and products.



A standard is your basis for:

Efficiency

Standards help optimise your work through well-defined guidelines and methods. It gives you a common language for efficient collaboration with both internal and external stakeholders.

Meet your moderator

Giovanni Collot

CEN and CENELEC



The STAN4CR project



- ▶ Funded by EISMEA (European Innovation Council and SMEs Executive Agency)
- ▶ Aims to accelerate EU standardization efforts, fostering collaboration and coherence in the evolving cybersecurity landscape.
- ▶ Strives to enhance cyber resilience across the EU Single Market while promoting broader societal engagement in standardization, including participation from SMEs, Open-Source Communities, Academia, and other key actors within the digital ecosystem.



Agenda – before lunch

- ▶ **10.20:** A brief overview of the Cyber Resilience Act (CRA), key elements, requirements, and the significance of standardization
Filipe Jones Mourão, DG CNECT, European Commission
- ▶ **10.40:** A short introduction to standardization and the objective of the workshop
Lucia Lanfri, CEN & CENELEC
- ▶ **11.00:** Coffee break
- ▶ **11.20:** Workshop round 1: Principles for cyber resilience
Simon Steendam, CEN/CLC JTC13/WG9 representative and rapporteur on the standard for Principles for cyber resilience
- ▶ **13.05:** Lunch

Agenda – after lunch

- ▶ **14.05:** Workshop round 2: Vulnerability handling
Michael Schuster, CEN/CLC JTC13/WG9 representative on the standard for Vulnerability handling
- ▶ **15.50:** Coffee break
- ▶ **16.10:** Case presentation: Implementing standards - preparation for the CRA in a global company
Thomas Young Olesen, Grundfos
- ▶ **16.40:** Next steps for the standardization development
Lucia Lanfri, CEN & CENELEC
Berit Aadal, Danish Standards
- ▶ **17.00:** Networking and drinks
- ▶ **17.30:** Goodbye



Filipe Jones Mourão

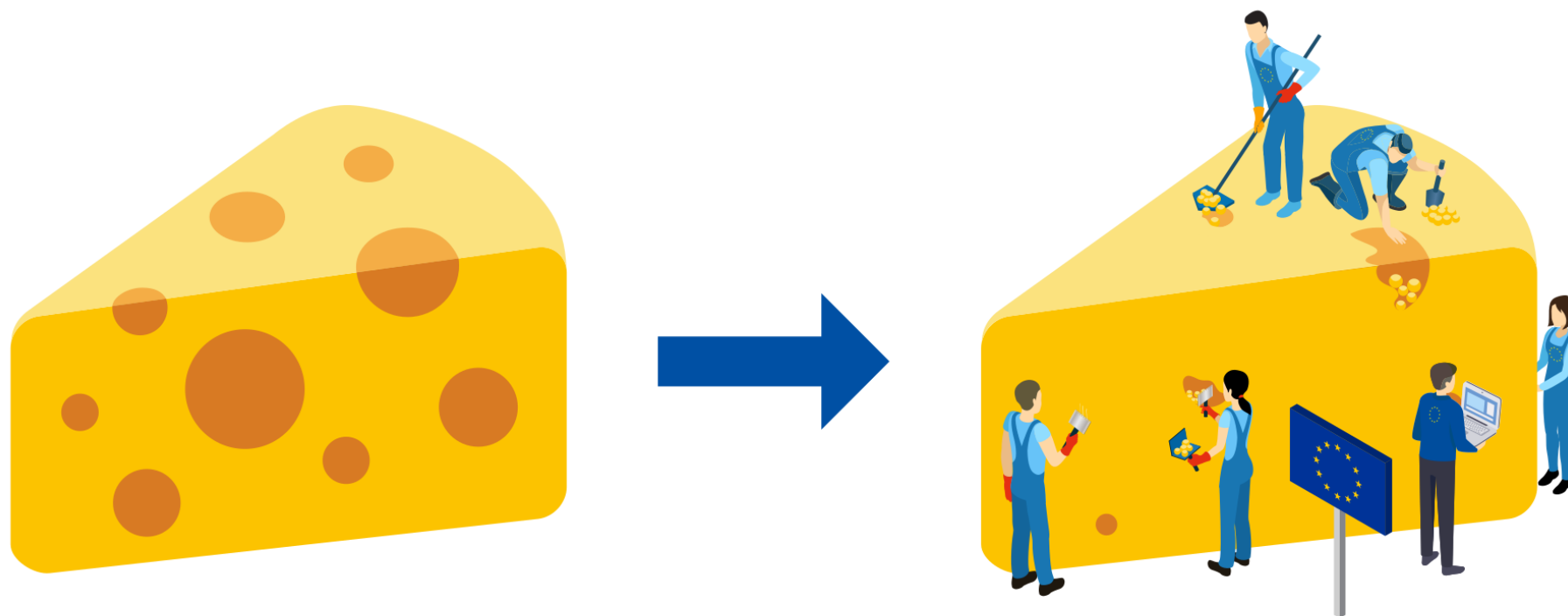
DG CNECT, European Commission

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...)

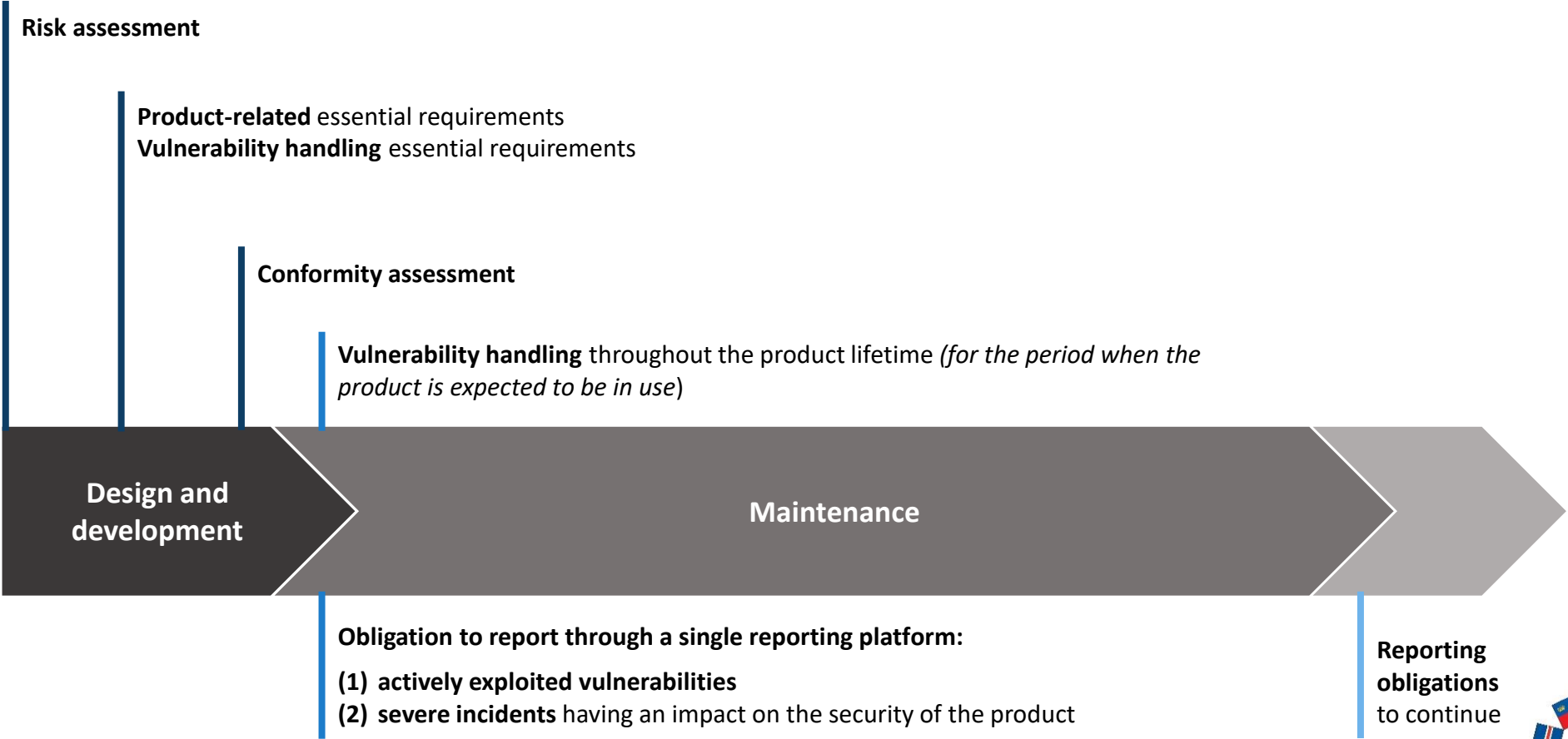


Outright exclusions

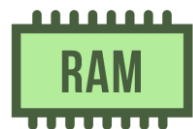
(cars, medical devices, in vitro, certified aeronautical equipment, marine equipment)



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*



► 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

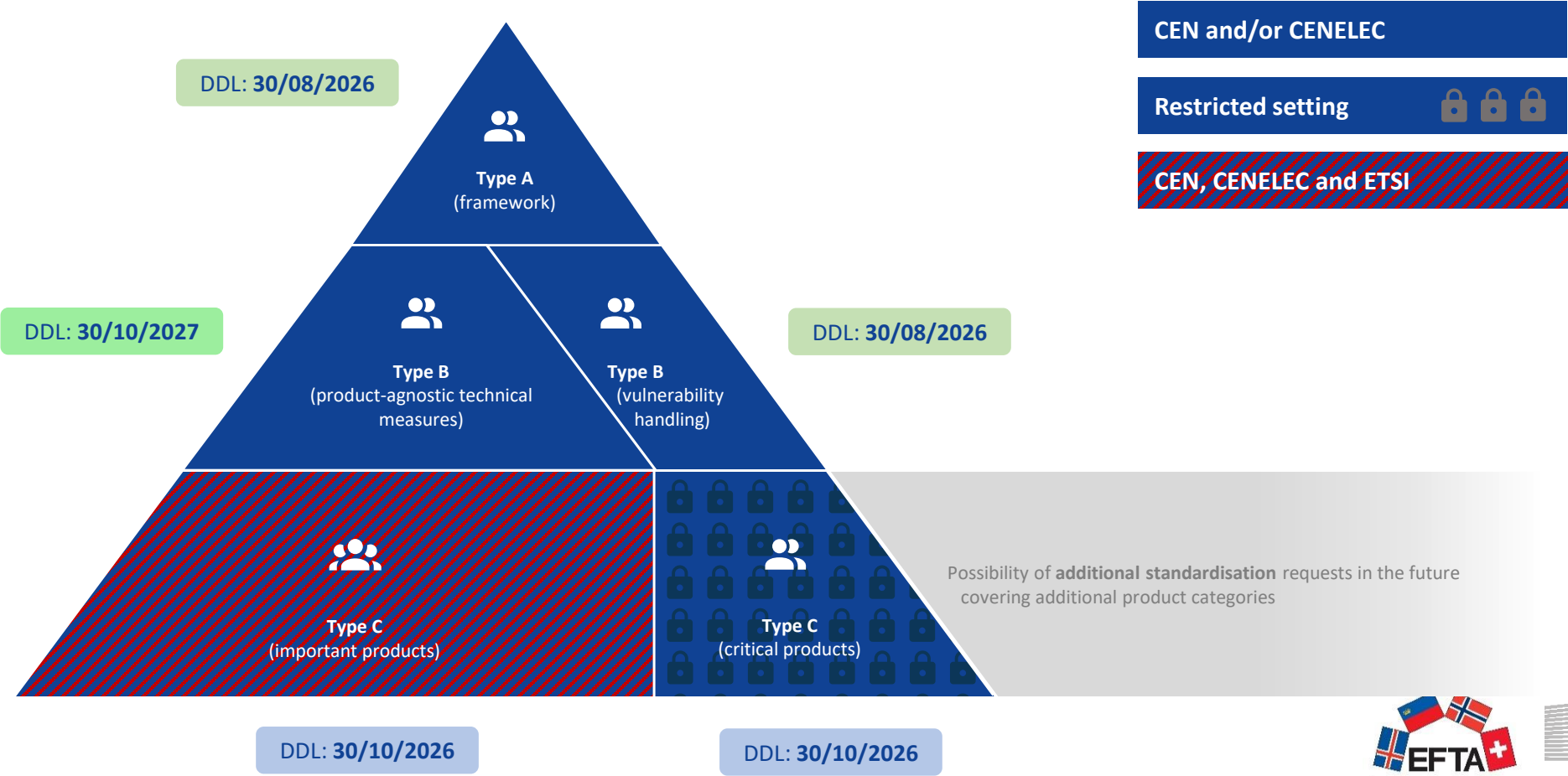
► **Horizontal standards (1-15)**

- 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

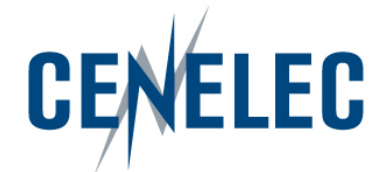


Thank you.



*Project Manager Electrotechnology
Standardization & Digital Solutions,
CCMC*





European Standardization Organizations

Cyber Resilience Standardization at CEN CENELEC

State of play



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 & CENELEC Business Sectors



ACCUMULATORS,
PRIMARY CELLS AND
PRIMARY BATTERIS



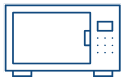
DEFENCE AND
SECURITY



DIGITAL SOCIETY



ELECTRIC EQUIPMENT
AND TRANSFORMERS



ELECTRIC EQUIPMENT
AND APPARATUS



ELECTRONIC,
ELECTROTECHNICAL
SUPPLIES



CONSTRUCTION



CHEMICALS



ELECTROTECHNOLOG
Y GENERAL



ENERGY AND
UTILITIES



HEALTHCARE



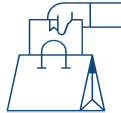
HOUSEHOLD
APPLIANCES
AND HVAC



INSULATED WIRE
AND CABLE



LIGHTING
EQUIPMENT AND
ELECTRIC LAMPS



CONSUMER



DEFENCE
AND
SECURITY



LOW VOLTAGE
ELECTRICAL
EQUIPMENT AND
INSTALLATIONS



MECHANICAL AND
MACHINES



OCCUPATIONAL
HEALTH AND SAFETY



TRANSPORT AND
PACKAGING



FOOD AND
AGRICULTURE



HEALTHCARE



SERVICES



MINING
AND
METALS



CEN and CENELEC Members in 34 countries

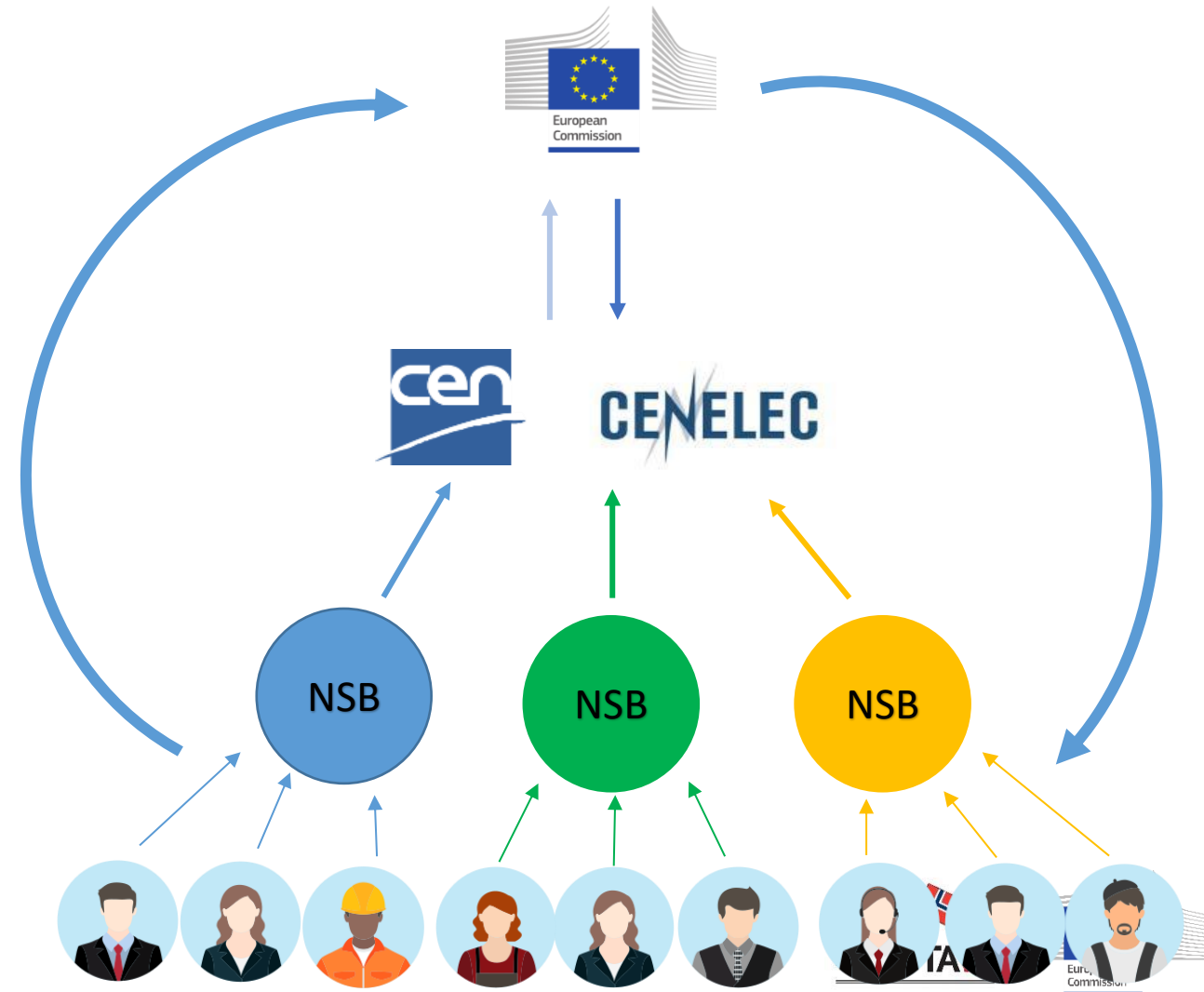


Austria 	Denmark 	Greece 	Latvia 	Poland 	Slovenia 
Belgium 	Estonia 	Hungary 	Lithuania 	Portugal 	Spain 
Bulgaria 	Finland 	Iceland 	Luxembourg 	Republic of North Macedonia 	Sweden 
Croatia 	France 	Ireland 	Malta 	Romania 	Switzerland 
Cyprus 	Germany 	Italy 	Netherlands 	Serbia 	Türkiye 
Czech Republic 	Norway 	Slovakia 	United Kingdom 		

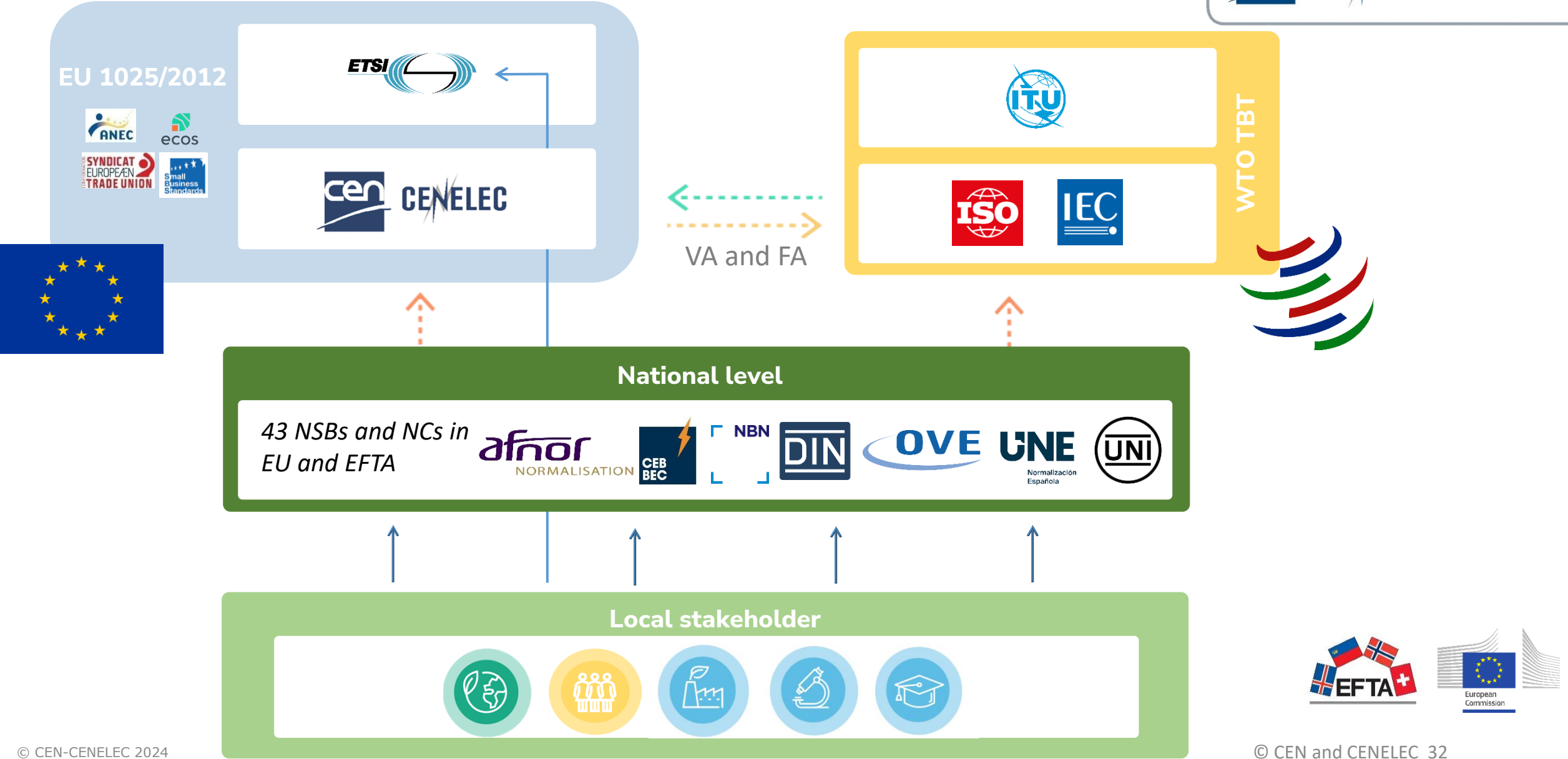


An inclusive system based on dialogue

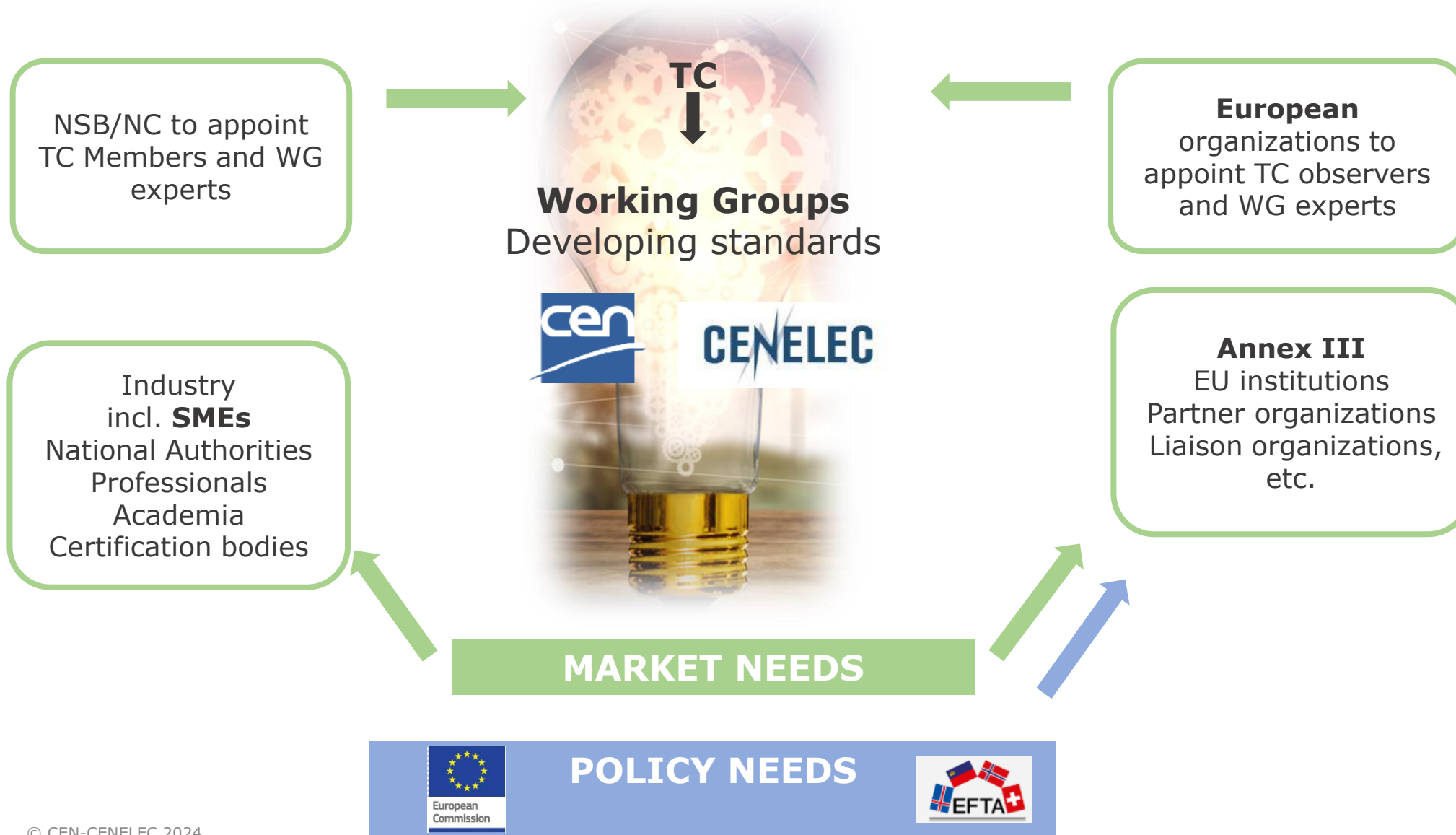
- ▶ Based on the national delegation principle
- ▶ Representing a consensus among all interested parties, including industry & SMEs and societal stakeholders
- ▶ Voluntary
- ▶ A continuous dialogue for a bottom-up + top-down approach



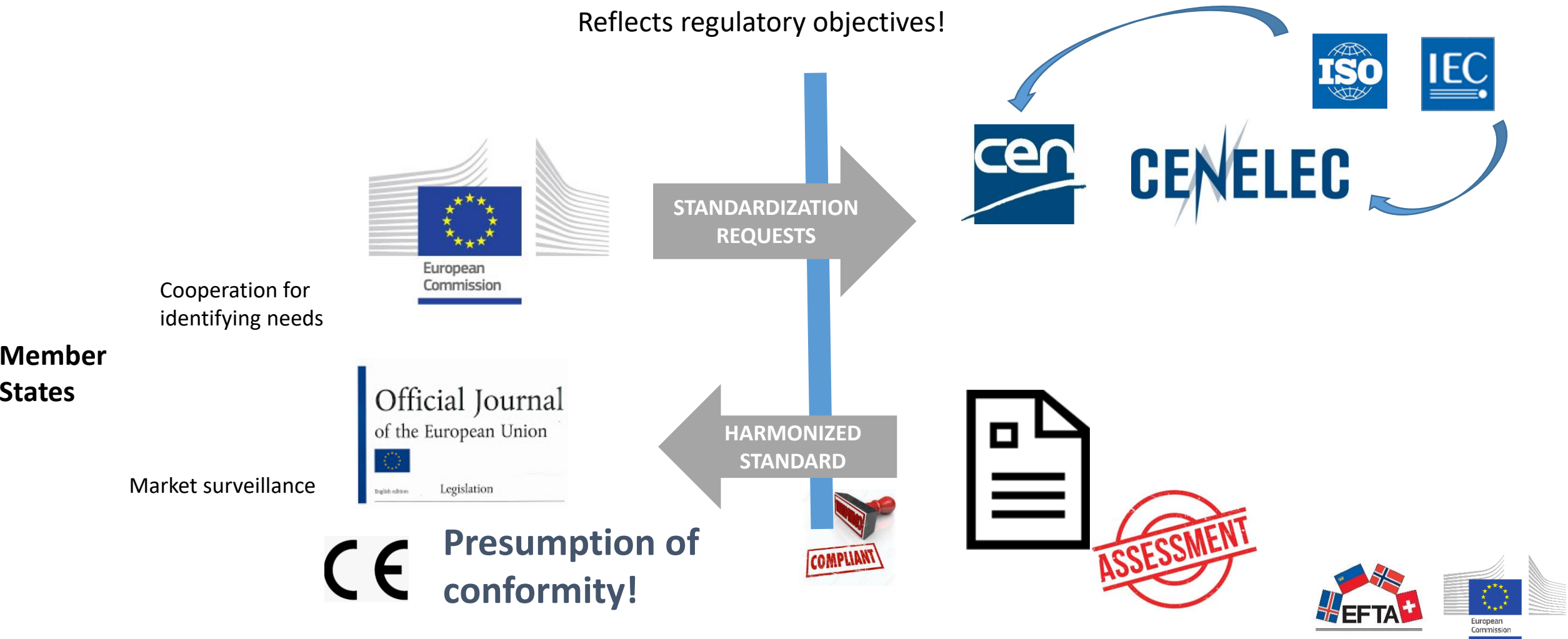
Stakeholder participation in technical work



Who drafts standards



Standardization Requests



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.



CRA Standardization Request

ANNEX I

List of new European Standards to be drafted

Reference information		Deadline for the adoption by the ESOs
Horizontal standards for security requirements relating to the properties of products with digital elements		
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 the risks	30/08/2026
2.	European standard(s) on making products with digital elements available on the market without known exploitable vulnerabilities	30/10/2027
3.	European standard(s) on making products with digital elements available on the market with a secure by default configuration	30/10/2027
4.	European standard(s) on ensuring that vulnerabilities in products with digital elements can be addressed through security updates	30/10/2027
5.	European standard(s) on ensuring protection of products with digital elements from unauthorised access and reporting on possible unauthorised access	30/10/2027
6.	European standard(s) on protecting the confidentiality of data stored, transmitted or otherwise processed by a product with digital elements	30/10/2027
7.	European standard(s) on protecting the	30/10/2027

► 41 topics, 3 'types' of deliverables:

► Category "A": horizontal framework

- Only CEN and CENELEC
- Topic #1 (JTC 13 WG9)
- deadline 2026-08-30

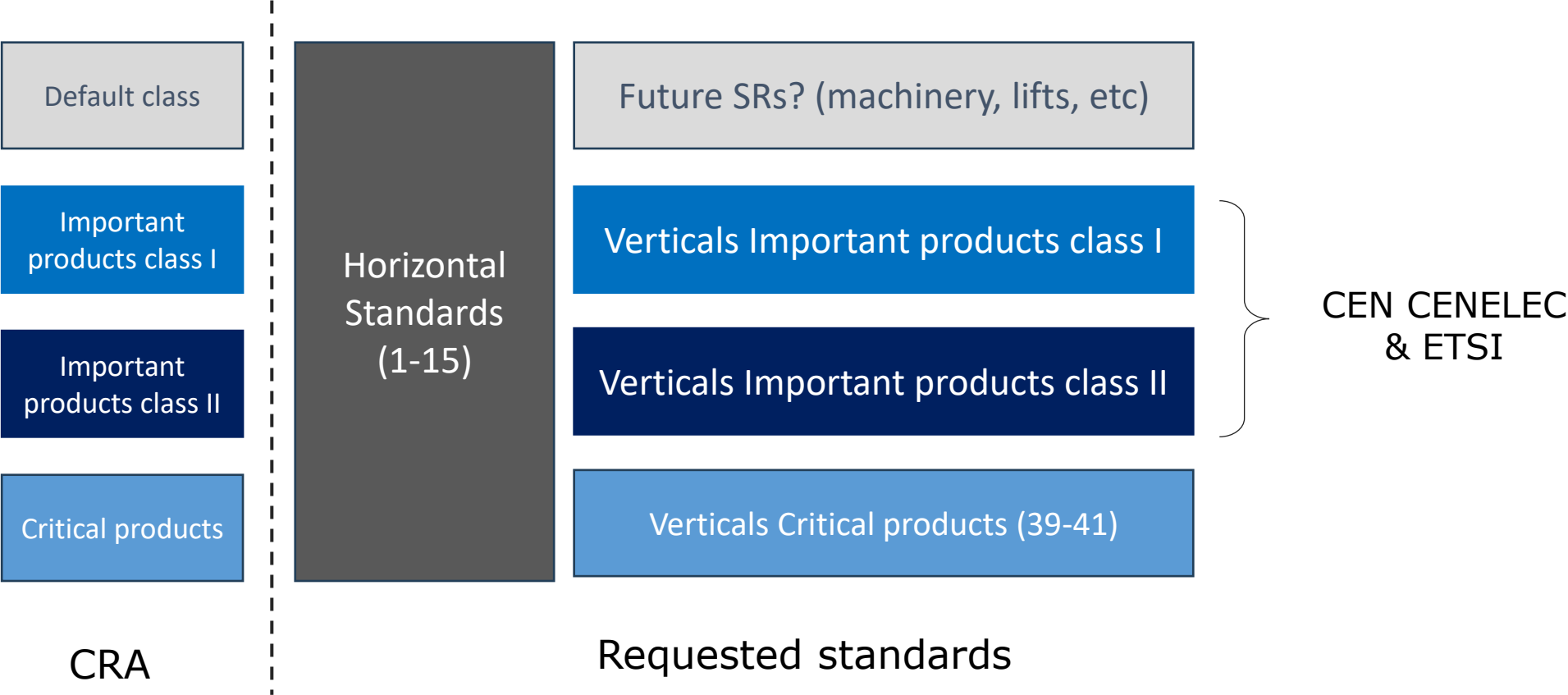
► Category "B": product-agnostic technical measures & vulnerability handling

- Only CEN and CENELEC
- Topic #2-15 (JTC 13 WG9)
- Deadline 2027-10-30 (except for line 15 - vulnerability handling - 2026-08-30)

► Category "C": Important and critical products

- Topic #16-38: CEN, CENELEC and ETSI
- deadline 2026-10-30
- Topic #39-41: CEN and CENELEC
- **Critical products**

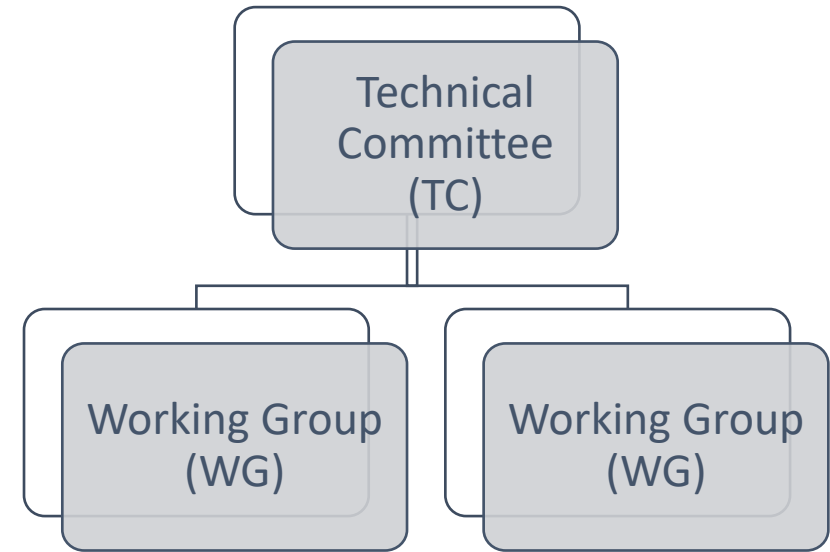
Requested standards



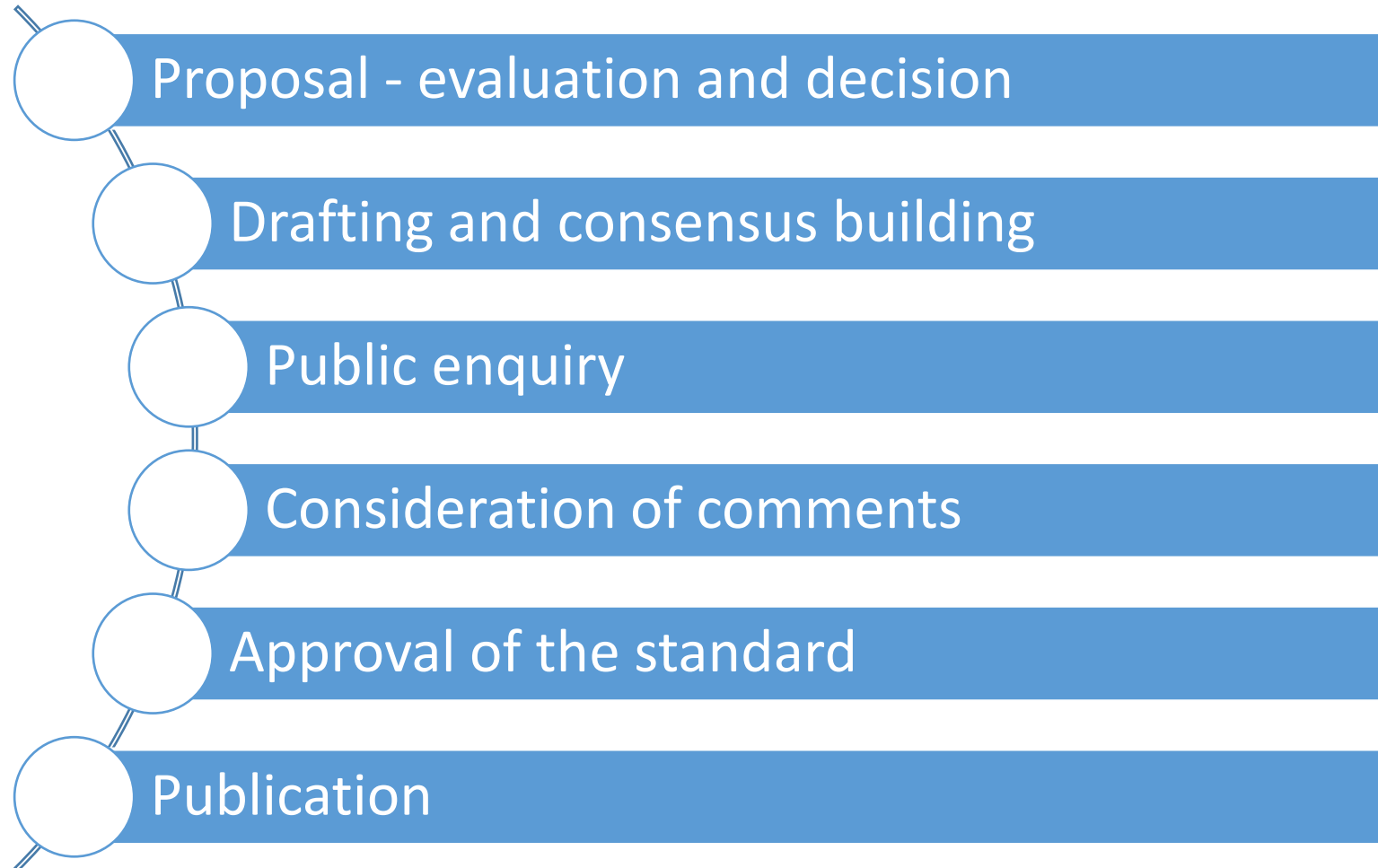
How is the work organized?



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



How are standards made?



- ▶ **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)
 - ▶ Smart card applications (Line 41)
- ▶ **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)



► CLC/TC 47X 'Semiconductors and Trusted Chips Implementation'

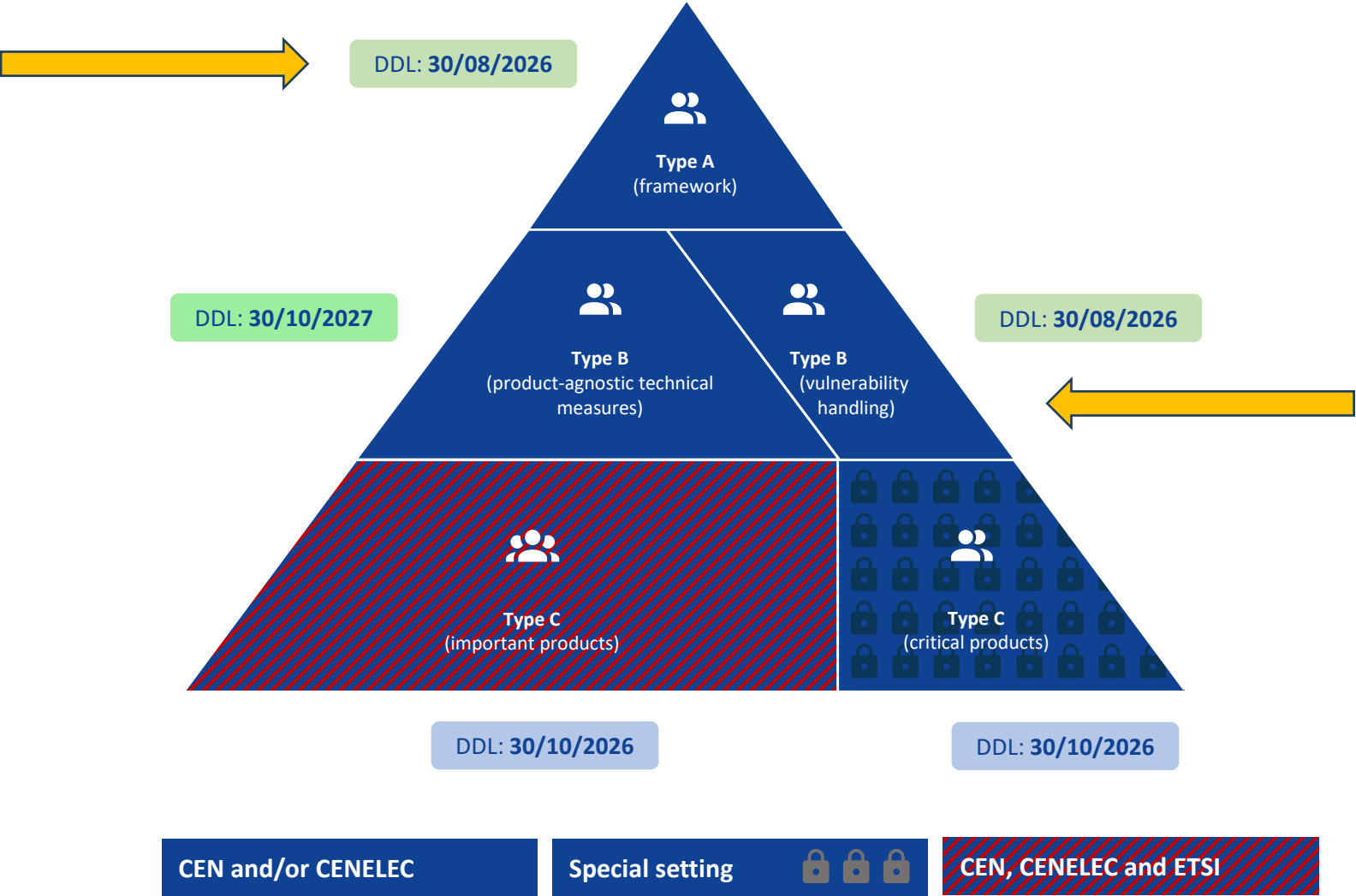
- European standard(s) on essential cybersecurity requirements for tamper-resistant microprocessors and microcontrollers (lines 37 & 38)
- European standard(s) on essential cybersecurity requirements for microprocessors and microcontrollers with security-related functionalities (lines 28 & 29)
- European 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



Focus of the workshop



Thank you!

www.cencenelec.eu

Follow us:    

Tag us [@Standards4EU](https://twitter.com/Standards4EU)

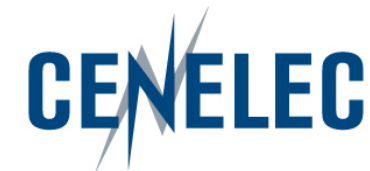
Lucia Lanfri

Project Manager CEN CENELEC Management Center



Simon Steendam

*CEN/CLC JTC13/WG9 representative
and rapporteur on the standard for
Principles for cyber resilience*



European Standardization Organizations

CRA - General Principles for Cyber Resilience Serious Game

Simon Steendam, PT1 Rapporteur



Introduction - Who am I

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

Introduction – CRA

- ▶ Cybersecurity is a key challenge for the union.
- ▶ Connectivity demands responsibility.
- ▶ The CRA is meant to tackle two major issues:
 - ▶ The low level of cybersecurity in products with digital elements;
 - ▶ The lack of understanding and access to information for users.
- ▶ It does this by providing a uniform legal framework setting the boundary conditions for the development of secure Products with Digital Elements (PwDE).
- ▶ It also aims to ensure users have access to information regarding cybersecurity to allow for informed purchases.

Introduction – The Request

- ▶ 41 total deliverables.
- ▶ 15 horizontal deliverables to be developed under CEN/CLC.
- ▶ 26 vertical deliverables to be developed in relevant technical committees in CEN/CLC or ETSI.
- ▶ PT1: General Principles for Cyber Resilience
 - ▶ 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
- ▶ PT3: Vulnerability Handling
 - ▶ European standard(s) on vulnerability handling for products with digital elements

Introduction – PT1 The Standard

- ▶ Dual purpose standard:
 - ▶ Cover the first essential requirement;
 - ▶ Provide a framework for the vertical standards.
- ▶ The standard sets the level for and provides the baseline of activities that enable compliance across the whole lifecycle of the product.
- ▶ The standard does not provide presumption of conformity.
- ▶ The process standard forms the basis on which the vertical standards are build.

Introduction – Principles

- ▶ The many principles of cybersecurity are condensed into four main principles based on the issues the CRA attempts to fix:
 - ▶ Risk based approach
 - ▶ Security by Design
 - ▶ Security by Default
 - ▶ Transparency
- ▶ These principles are fundamental to compliance with the essential requirements
- ▶ Activities are set up to enable compliance with these principles



Introduction – Risk based approach

- ▶ Products with digital elements must consider the risks.
- ▶ The standard does not enforce a specific method of measuring risk.
- ▶ The standard does contain horizontal elements of risk management needed in the context of the CRA.
- ▶ Based on the ISO 31000 but adjusted for the CRA.

Introduction – Elements of risk management

- ▶ Determine the product context
- ▶ Determine the product assets
- ▶ Identify threats to these assets and extrapolate the risks
- ▶ Evaluate and treat the risks with appropriate mitigation measures
- ▶ This standard cannot inform the manufacturer what degree of mitigation is sufficient, this is something the vertical standards can.
- ▶ Monitor and review the risks
- ▶ Communicate to relevant stakeholders where appropriate

- ▶ Activities are intended to be process agnostic state of the art elements that can be implemented in processes to enable a secure lifecycle for a product with digital elements.
- ▶ Names might differ, but the goals remain the same.
- ▶ The standard focusses on output.
- ▶ Some examples: product cybersecurity plan, (legal) requirement analysis, secure product architecture and design, secure implementation, security verification and validation, monitoring, security issue management, potential decommissioning, and third-party supply chain component security management.

Introduction – The workshop

- ▶ Two main goals:
 - ▶ Process preparation to enable CRA compliance;
 - ▶ Gather information around activities.
- ▶ A scenario using a fictional company will be used that seeks to bring its product to the Union market.
- ▶ You are to determine what activities this company needs to set up in order to be CRA complaint.
- ▶ No need to deep dive the specific product controls, stay high level.

Introduction – The setup

- ▶ Discuss what activities you deem needed for compliance with the Essential Requirements (ER) as provided by the material
- ▶ We will discuss this afterwards.
- ▶ This exercise is both for collection and dissemination of information.

Introduction – The Template

ACTIVITIES



Activity	Description	Link to the essential requirements in the CRA
Requirement Analysis	The goal of the requirement analysis activity is to determine what requirements from the CRA are applicable to the Product with Digital Elements	Not applicable

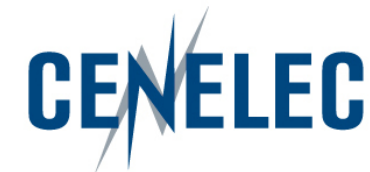
Introduction – The Scenario

- ▶ The TELO-pod is a one person capsule created by PODcorp.
- ▶ It can convert people into data and transport them over the internet to a different TELO-pod in the network where they then rematerialize.
- ▶ Your task is to ensure that the product with digital elements shall be designed, developed, produced and disposed in such a way that they ensure an appropriate level of cybersecurity based on the risks across the entire lifecycle of the product.
- ▶ Look at this for activities that you need to implement, not specific product controls.



Michael Schuster

*CEN/CLC JTC13/WG9 representative
on the standard for Vulnerability
handling*



European Standardization Organizations

CRA - General Principles for Cyber Resilience Serious Game

Michael Schuster, PT3 Representative



PT3 The Standard

- ▶ Focused on creating a harmonized horizontal standard on vulnerability handling for products with digital elements
- ▶ Covers the Essential Requirements of the CRA Annex I part II Vulnerability handling requirements (1) – (8)
- ▶ Processes shall allow the manufacturer to fulfil the vulnerability handling requirements
- ▶ Structure of the requirements in the standard will reflect the phases of the Coordinated Vulnerability disclosure (CVD) process to be in line with the ISO/IEC 29147:2018 and EN ISO/IEC 30111:2019

PT3 Standard – Table of Content

- ▶ 1 Scope
- ▶ 2 Normative Reference
- ▶ 3 Terms and Definitions
- ▶ 4 General
- ▶ 5 Vulnerability Handling Requirements
- ▶ Annex

PT3 Standard – VH Requirements

- ▶ Sharing
- ▶ Preparation
- ▶ Discovery
- ▶ Validation and Triage
- ▶ Remediation
- ▶ Gaining Awareness
- ▶ Promote Deployment
- ▶ Post Release

PT3 Standard - Sharing

- ▶ Activities of the manufacturer of the PwDE for sharing vulnerability information
- ▶ The manufacturer needs to take measures to facilitate the sharing of information about potential vulnerabilities in their PwDE
- ▶ **Annex I, Part 2, (6): take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;**

PT3 Standard - Preparation

- ▶ Activities regarding the preparation of the CVD process
- ▶ The manufacturer needs to have policies and processes in place before the CVD process starts
- ▶ **Annex I, Part 2, (1): identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;**
- ▶ **Annex I, Part 2, (5): put in place and enforce a policy on coordinated vulnerability disclosure;**

PT3 Standard - Discovery

- ▶ Activities regarding the discovery of vulnerabilities
- ▶ The manufacturer needs to have processes in place to receive vulnerability information from various sources
- ▶ **Annex I, Part 2, (1): identify and document vulnerabilities and components contained in products with digital elements**, ~~including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;~~
- ▶ **Annex I, Part 2, (3): apply effective and regular tests and reviews of the security of the product with digital elements;**

- ▶ Activities regarding the validation and assessment of the vulnerability
- ▶ The manufacturer needs to perform an initial assessment of the vulnerability to see if a vulnerability is applicable to the PwED
- ▶ The manufacturer needs to determine the risk created by the vulnerability
- ▶ **Annex I, Part 2, (2) in relation to the risks posed to products with digital elements, address** ~~and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;~~

PT3 Standard - Remediation

- ▶ Activities regarding the remediation of the vulnerability
- ▶ The manufacturer needs to determine what the best measure is, to neutralizing or fixing a vulnerability is
- ▶ Can include intermediary ways before a final remediation is provided
- ▶ **Annex I, Part 2, (2)** ~~in relation to the risks posed to products with digital elements, address and~~ **remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;**

PT3 Standard – Gaining Awareness

- ▶ Activities regarding the dissemination of security updates addressing the identified security issue
- ▶ The manufacturer needs to have processes in place to distribute available updates to ensure the continuity of the PwDE's security
- ▶ **Annex I, Part 2, (8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.**

PT3 Standard – Promote Deployment

- ▶ Activities regarding the making publicly available of the information regarding the fixed vulnerability
- ▶ The manufacturer needs to have processes in place to inform about a vulnerability and its treatment through advisories
- ▶ **Annex I, Part 2, (4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;**
- ▶ **Annex I, Part 2, (7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;**

PT3 Standard – Post Release

- Activities regarding the post release action plan for the PwDE
- The manufacturer needs to monitor the effects of the remediation to the PwDE after deployment
- The manufacturer might need to update the secure development lifecycle

The workshop


- ▶ Two main goals:
 - ▶ Process preparation to enable CRA compliance;
 - ▶ Gather information around activities.
- ▶ A scenario using a fictional company will be used that seeks to bring its product to the Union market.
- ▶ You are to determine what vulnerability handling activities this company needs to set up in order to be CRA complaint.
- ▶ No need to deep dive the specific product controls, stay high level.

The Scenario

- ▶ Two months after the TELO-pod was launched a security researcher discovered a vulnerability
- ▶ During the transmission of the users data across the internet, it is possible to manipulate the data via a man-in-the-middle attack.
- ▶ Your task is to check whether all activities are in place to handle that vulnerability.



ACTIVITIES¶



Activity¶	Description¶	Link-to-vulnerability-handling-stages¶
Have a contact address in place¶ ¶ ¶ ¶	The manufacturer needs to have an easy-to-find contact address published for the reporting of vulnerabilities.¶	Sharing¶

Thomas Young Olesen

*Head of Product Compliance,
Grundfos*



Preparation for the CRA in a global company

8 April 2025

Workshop: Cyber Resilience Act and the horizontal standards

Thomas Young Olesen
Head of Product Compliance

GRUNDFOS 

Possibility in every drop

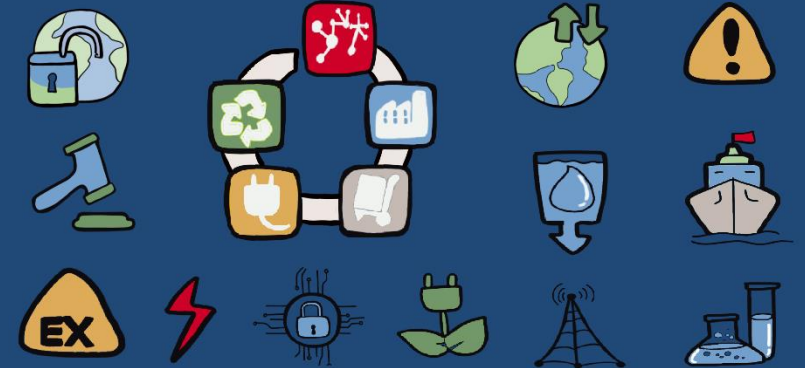
Thomas Young Olesen




Head of Product Compliance

20 years in product quality and -compliance

**>10 years in Dependability standardization, DS
S-556, IEC TC56, Convenor of TC56-WG4
Information Systems**



- Product Compliance
- Electro technical
- Materials and Environmental
- Global Market Access
- 15M / 1.5M / 3k products
- >200 countries
- Yearly 1.000 obligations



GRUNDFOS is One of
the world's leading
pump and water
solutions companies



19,937

employees

87.5%

owned by the
Poul Due Jensen Foundation

**EUR
4.6bn**

revenue
in 2023

1945

when it all
started

15,000,000

units produced
per year

5.4%

of revenue
reinvested

Domestic Building Service

A home is a place of comfort and sustainability

The Domestic Building Services (DBS) Division within Grundfos serves OEMs, distributors, installers, and homeowners with some of the world's most energy-efficient pumps and solutions for domestic homes.

We develop, produce, and sell smaller domestic pumps and solutions for single-family housing and residential buildings. We have an opportunity and responsibility to enable homeowners to reduce their climate impact and increase comfort. This inspires our aspiration to offer homeowners the most attractive choices for sustainable homes and comfortable lives.

A domestic pump solution for every application

- HVAC Trade
- HVAC OEM
- Hot Water Recirculation
- Boosting
- Drainage
- Wastewater

Water Utility

Transforming water, together

Meeting the growing demand for clean and safe water requires a transformation of the way we manage the entire water cycle, from drinking water to wastewater, from communities to irrigation.

In Water Utility, we work in partnership with stakeholders from our entire ecosystem: customers, designers, consultants, value chain partners as well as suppliers. Together, we create intelligent, sustainable pumping and solar powered solutions to optimise water management all over the world.

Together, we are on a journey towards a sustainable water future within:

- Ground water and irrigation
- Clean water distribution
- Wastewater collection and transport
- Water intake solutions

Commercial Building Service

High performance buildings ensuring comfort and safety

From hotels and hospitals to office towers and airports, every commercial building has its own special requirements.

When Grundfos is part of the solution, you get smarter and more sustainable workplaces and places to live with increasing comfort and energy efficiency.

A commercial system solution for every application

- Commercial air conditioning
- Commercial hot water recirculation
- Commercial wastewater
- Commercial fire protection
- Commercial water pressure boosting
- Commercial heating
- Commercial water disinfection

Industry

Helping industrial end-users and OEMs reach their water and climate ambitions – globally

Grundfos Industry delivers a wide range of premium quality products, solutions, and services based on pumping and water treatment systems to help our industrial customers and end-users globally to reach their water and climate ambitions while maximising their output. We enhance and optimise industrial utilities, and industrial processes, covering areas such as water treatment or water reuse, system integration, energy and process optimisation, and liquid composition, as well as delivering value-adding digital solutions. Our employees are passionate to help our customers solve their water and energy challenges.

An industrial solution from Grundfos is designed, selected, and built to perform and last. It can be used in a wide range of industrial processes, an industrial pump and water treatment solution for every application:

- Industrial water treatment and water transport
- Industrial temperature control: cooling, and heating
- Industrial processes: wash and clean, machine tool, general processes



ONE
GRUNDFOS
organized into four
Divisions



Close to you,
wherever
you are

Domestic Building Service

A home is a place of comfort and sustainability

The Domestic Building Services (DBS) Division within Grundfos serves OEMs, distributors, installers, and homeowners with some of the world's most energy-efficient pumps and solutions for domestic homes.

We develop, produce, and sell smaller domestic pumps and solutions for single-family housing and residential buildings. We have an opportunity and responsibility to enable homeowners to reduce their climate impact and increase comfort. This inspires our aspiration to offer homeowners the most attractive choices for sustainable homes and comfortable lives.

A domestic pump solution for every application

- HVAC Trade
- HVAC OEM
- Hot Water Recirculation
- Boosting
- Drainage
- Wastewater



Commercial Building Service

High performance buildings ensuring comfort and safety

From hotels and hospitals to office towers and airports, every commercial building has its own special requirements.

When Grundfos is part of the solution, you get smarter and more sustainable workplaces and places to live with increasing comfort and energy efficiency.

A commercial system solution for every application

- Commercial air conditioning
- Commercial hot water recirculation
- Commercial wastewater
- Commercial fire protection
- Commercial water pressure boosting
- Commercial heating
- Commercial water disinfection

Water Utility

Transforming water, together

Meeting the growing demand for clean and safe water requires a transformation of the way we manage the entire water cycle, from drinking water to wastewater, from communities to irrigation.

In Water Utility, we work in partnership with stakeholders from our entire ecosystem: customers, designers, consultants, value chain partners as well as suppliers. Together, we create intelligent, sustainable pumping and solar powered solutions to optimise water management all over the world.

Together, we are on a journey towards a sustainable water future within:

- Ground water and irrigation
- Clean water distribution
- Wastewater collection and transport
- Water intake solutions



Industry

Helping industrial end-users and OEMs reach their water and climate ambitions – globally

Grundfos Industry delivers a wide range of premium quality products, solutions, and services based on pumping and water treatment systems to help our industrial customers and end-users globally to reach their water and climate ambitions while maximising their output. We enhance and optimise industrial utilities, and industrial processes, covering areas such as water treatment or water reuse, system integration, energy and process optimisation, and liquid composition, as well as delivering value-adding digital solutions. Our employees are passionate to help our customers solve their water and energy challenges.

An industrial solution from Grundfos is designed, selected, and built to perform and last. It can be used in a wide range of industrial processes, an industrial pump and water treatment solution for every application:

- Industrial water treatment and water transport
- Industrial temperature control: cooling, and heating
- Industrial processes: wash and clean, machine tool, general processes

Our Product Cyber Compliance Journey

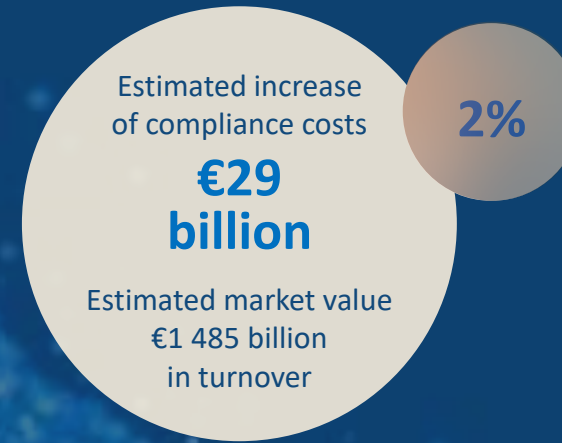


Possibility in every drop

Upcoming Cyber Regulations



Zoom on Europe - it's not going away



ISMS/ISO 27001, IEC 62443-4-1, IEC 62443-4-2

- cyber compliance ready

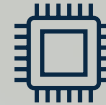


PEOPLE



- Organizational alignment and collaboration
- Training & awareness
- Skills & certifications
- Cyber maturity

TECHNOLOGY



- Secure product design
- Security level (SL)
- Software update
- Security testing
- Intrusion detection
- Security event logging

PROCESS



- Incident management (detect, respond, fix)
- Reporting
- Whole lifecycle
- Maturity level (ML)
- SDLC (development process)
- SW supportability

REDDA is on the path towards CRA, December 2027, It is critical that we keep the pace!



✓ ISO 27001



✓ IEC 62443-4-1



► ISMS, SDL, 2024

► 1. August 2025

► 11. December 2027

Where to start?



1. LEADERSHIP



- Acceptance
- External Board
- Top Management

2. FUNDING



- Secure funding and Budgets
- Roadmap
- Adjust business plans
- Setup a security program

3. START NOW!



- Secure Development Lifecycle (SDL)
- Vulnerability Handling
- Incident Management
- Security testing capabilities
- Prepare technology and product platforms
- Supplier management

CRA path forward



Possibility in every drop

CRA is going to be a difficult journey

- > New processes and organizational alignment
- > Skill and maturity gap – Shortage of talent
- > Short time to upgrade existing products





Take responsibility,
Be practical – not idealistic



Clarity, certainty and leadership
is needed from the Commission
and Standardization

- > Scope, Terms and Definitions
- > Guidance on standards and requirements
- > Help create direction and certainty



Possibility in every drop

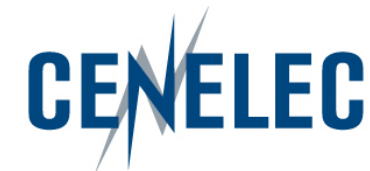
Next steps and thank you

Lucia Lanfri

*Project Manager Electrotechnology
Standardization & Digital Solutions,
CCMC*

Berit Aadal

Chief Consultant, Danish Standards



European Standardization Organizations

Cyber Resilience Standardization at CEN CENELEC

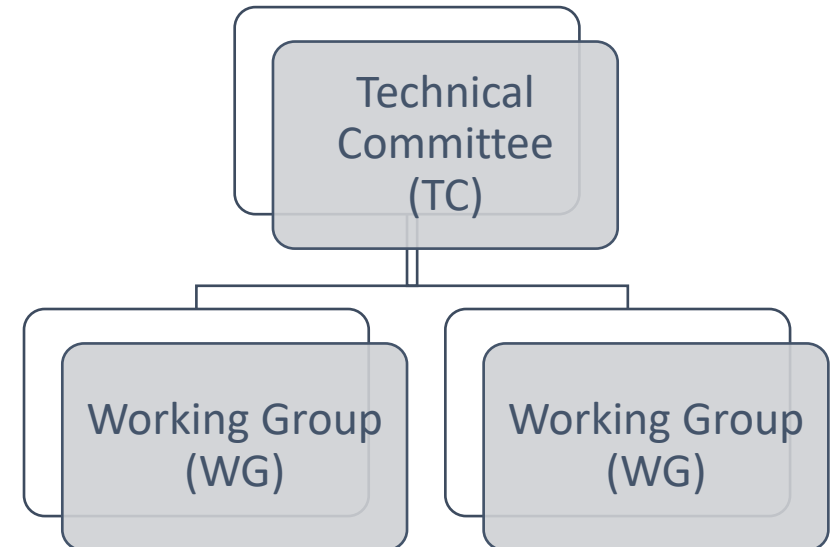
State of play



How is the work organized?



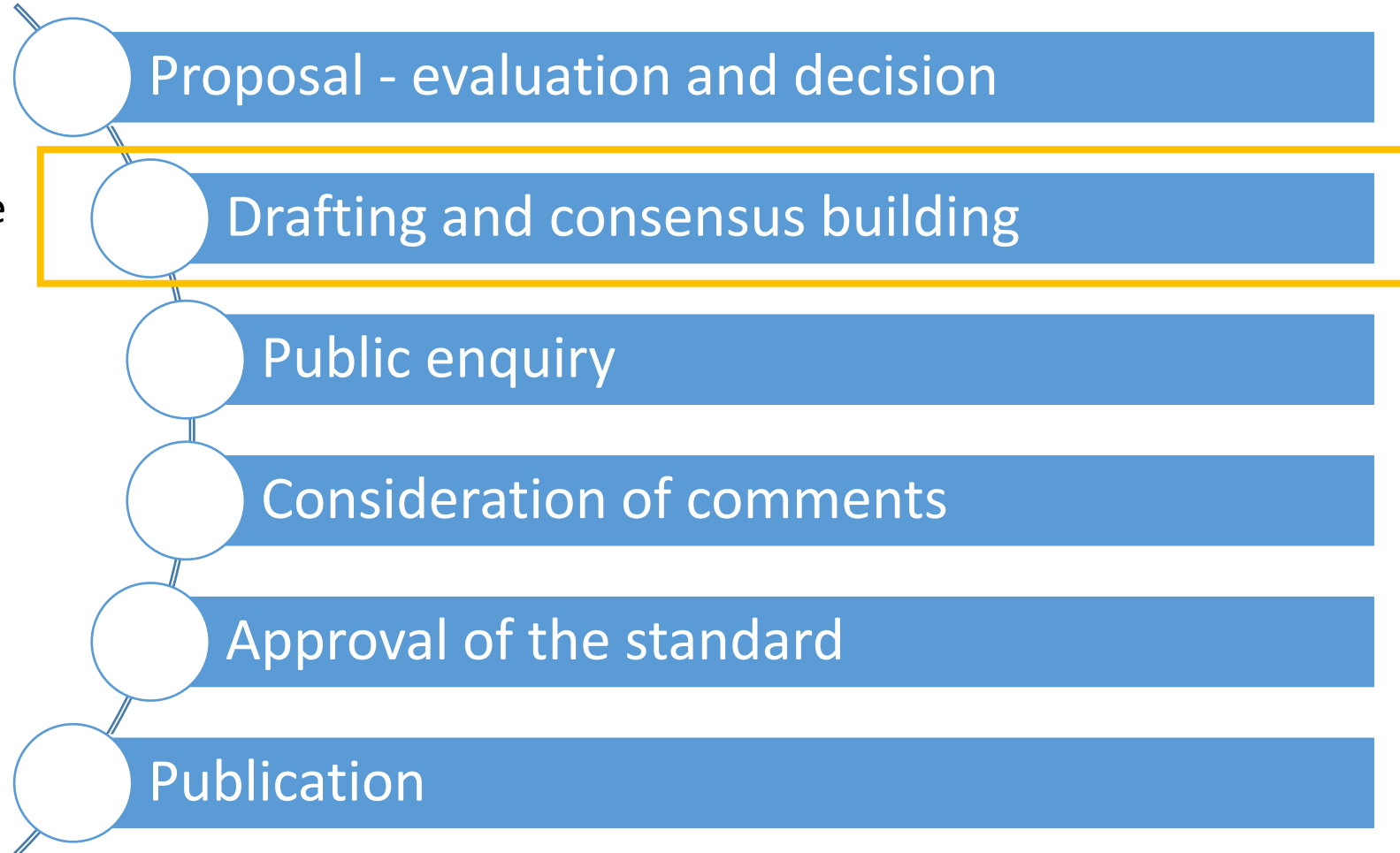
- ▶ The standards are developed in Technical Committees (TC)
- ▶ Each TC has Working Groups (WGs)
- ▶ Each WG has a dedicated scope



How are standards made?

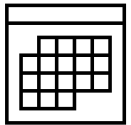


We are here



► 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)



The WG 9 meets every 2 weeks, project teams meet weekly.



Over 250 experts registered!



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)
 - ▶ Smart card applications (Line 41)

- ▶ **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)



► 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)



Open call for tender

Table 2 Distribution of deliverables per Rapporteur as per the present Call for Tender

Rapporteur 1 CEN/TC 224	16. 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
Rapporteur 2 CEN-CLC/JTC 13 WG 6	24. European standard(s) on essential cybersecurity requirements for public key infrastructure and digital certificate issuance software
Rapporteur 3 CLC/TC 65X	<p>*20. European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)</p> <p>*21. European standard(s) on essential cybersecurity requirements for network management systems</p> <p>*22. European standard(s) on essential cybersecurity requirements for Security information and event management (SIEM) systems</p> <p>*25. European standard(s) on essential cybersecurity requirements for physical and virtual network interfaces</p> <p>*27. European standard(s) on essential cybersecurity requirements for routers, modems intended for the connection to the internet, and switches</p>
Rapporteur 4 TBD	<p>23. European standard(s) on essential cybersecurity requirements for boot managers</p> <p>26. European standard(s) on essential cybersecurity requirements for operating systems</p>

*Only focused on the OT part of the deliverables and deriving from OT broad vertical EN IEC 62443-4-2 which will be handled by CLC/TC 65X. The rest of the scope is outside of this call for tender.

[Call for Tender for Rapporteurs in the field of 'Cybersecurity' - CEN-CENELEC](#)

No need to be CEN CENELEC ETSI member

Applications open until 11/04/2025



5th Specific Service Procedure

[Home](#)



CYBERSTAND.eu

Apply for Funding to Develop Standards for the Cyber Resilience Act

ENCOURAGED CONTRIBUTIONS

Drafting and consensus on horizontal standards

5th SSP

OPEN 10th Mar

CLOSE 11th Apr 17:00 CEST

APPLY NOW

  Co-funded by the European Union

CYBERSTAND.eu provides € 1,500,000 to support contributions to the development of harmonised standards for the Cyber Resilience Act.

This fifth funding cycle or Specific Service Procedure (SSP) **cybersecurity specialists, Open Source contributors and representatives from Small and Medium Enterprises (SME)** to contribute to the drafting and consensus building of the CRA horizontal standards.

The 5th SSP opens on the 10th of March and will close on the 11th of April.

[Apply Now To The 5th SSP](#)

We look for projects that will contribute to the CRA standards developments in any of the 41 deliverables

Next coming → 6th SSP opens 14/04

Future stakeholder events under the STAN4CR project



- ▶ Workshops and events considering the vertical requirements through 2025
- ▶ Workshop on the 'Generic Security Requirements' (horizontal lines 2-14 'in the CRA Standardization request) will be held in Spain in September 2025
- ▶ Final workshop will be held in Cyprus in 2026



Normalización
Española



Second workshop on CRA and the horizontal standards

- ▶ In Madrid, Spain in September 2025.
- ▶ Focus on lines 2-14 in the standardization request
- ▶ Full-day hybrid event with structured feedback collection
- ▶ Objectives: Gather stakeholder input on draft standards, identify implementation challenges, ensure practical applicability, collect diverse perspectives from industry
- ▶ Target audience: Manufacturers, industry associations, SMEs, certification bodies, national authorities (expected 50-100 participants)



Want to join standardization?

- If you want to contribute to the development of the standards supporting the Cyber Resilience Act, please contact your National Standardization Body to join.



THANK YOU

www.cencenelec.eu

Follow us:    

Tag us [@Standards4EU](https://twitter.com/Standards4EU)

