



European Standardization Organizations

The Cyber Resilience Act: Preparing for new requirements and emerging standards

CEN – CENELEC Sectoral Project Manager
Electro & Digital Technologies- Standardization

CRA REGULATION – A MAJOR STANDARDISATION AND COORDINATION EFFORT

CRA REGULATION— A MAJOR STANDARDISATION AND COORDINATION EFFORT

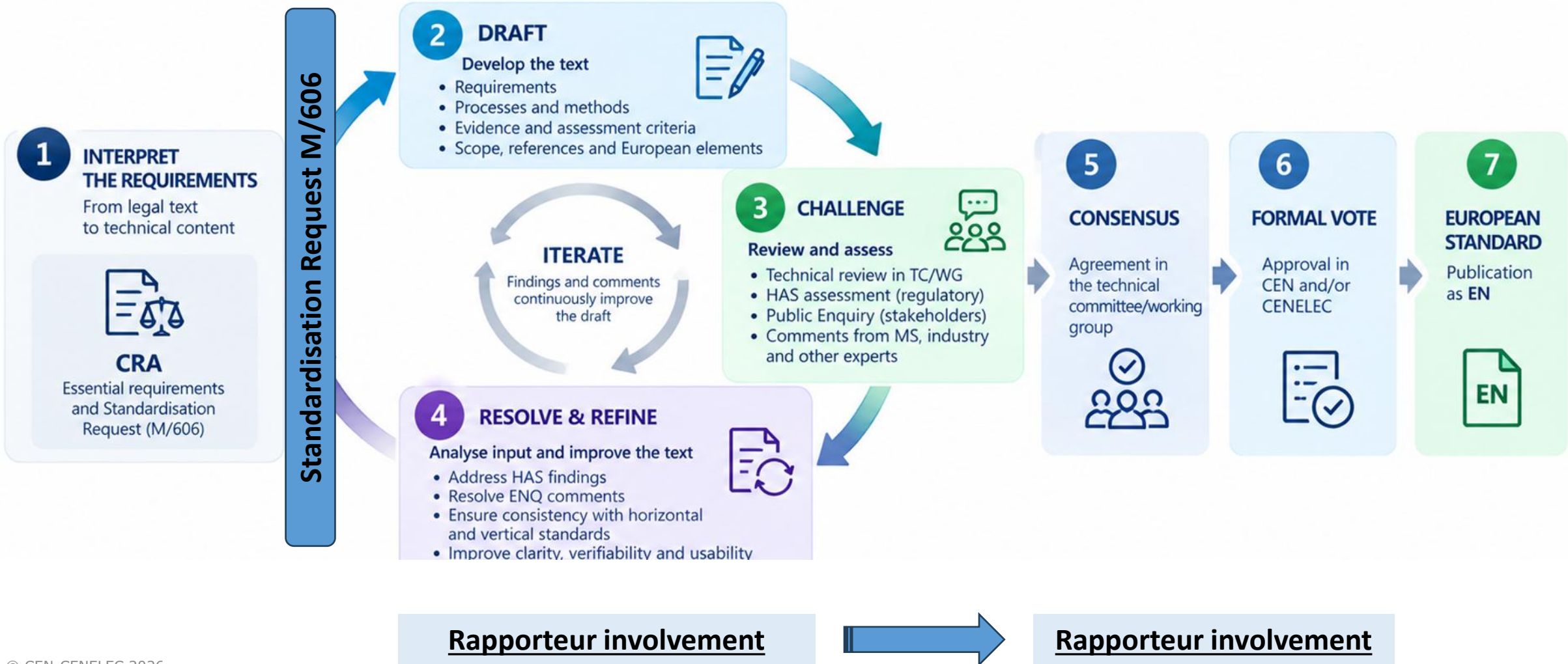


The challenge is not only
WHAT to standardise —
but **HOW** to deliver it.

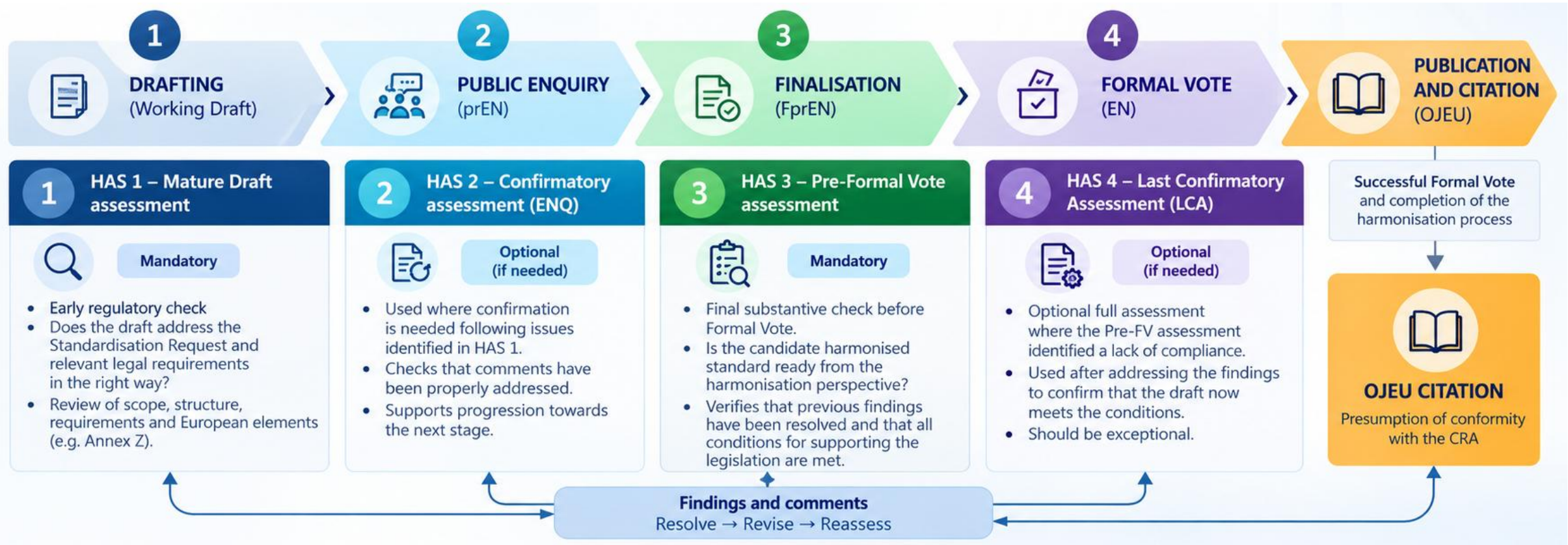


CRA – Drafting is an iterative process and Coordination Effort

Technical drafting, assessment and consensus continuously shape the text



Before Citation HAS Assessment Process – a necessary step



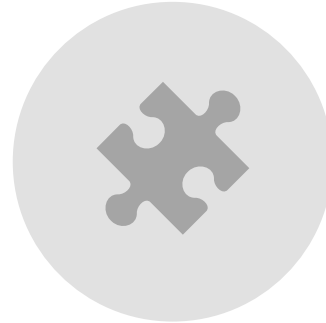
CRA standards – Lessons learned



01 — TRANSLATION

Legal language ≠ standards language

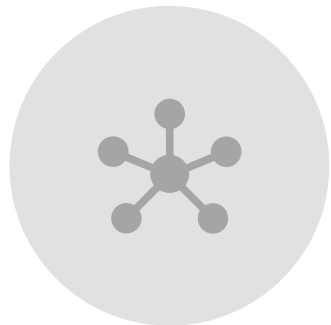
Turn regulatory outcomes into implementable technical requirements without changing their meaning.



02 — COHERENCE

41 deliverables cannot become 41 interpretations

Horizontals and verticals need common concepts, methods and terminology, need for cross vertical alignment



03 — COORDINATION

The work is distributed — the framework must not be

CEN, CENELEC and ETSI work across different technical communities, but the resulting standards need to fit together.



04 — ITERATION

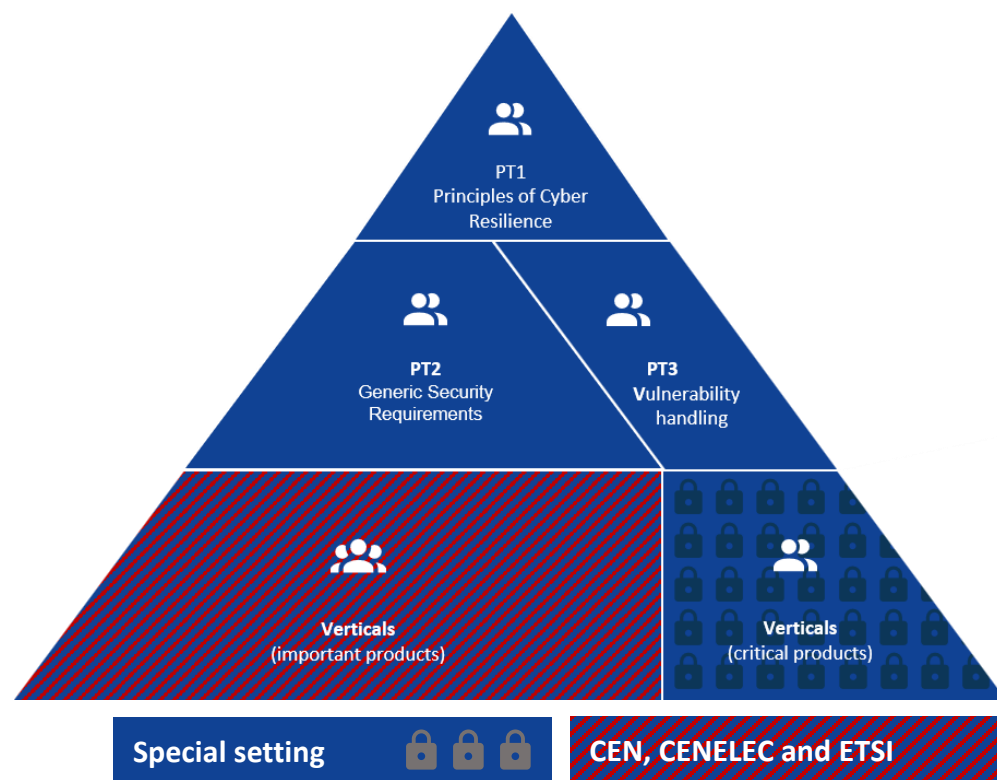
Consensus improves the technical result

Assessment, enquiry and comment resolution are part of developing a usable standard.

CRA Standard Framework

M/606

- 41 requested deliverables
- including 32 product-specific harmonised standards with harmonised standards developed to support OJEU citation and CRA presumption of conformity



-  Important products class I
-  Important products class II
-  Critical products

HORIZONTAL — THE COMMON FRAMEWORK

JTC 13/WG9 Horizontal Cybersecurity for Products with Digital Elements

4 horizontal work items

- PT 1: Principles & Product Risk Management
- **PT 3: Vulnerability Handling - Citation**
- PT 2: Generic security requirements



Horizontal standards are important because they can guide manufacturers in their self-assessment process, supporting them to cover the essential requirements of the CRA

Main objectives and interplay of the deliverables



FprEN 40000-1-1 Vocabulary

Common language for the horizontal standards

- Contains the **terms and definitions** of the horizontal standards
- The terms and definitions of the **legal text are leading**; some have been copied for clarity as some terms deviate
- Example: “hardware” is limited to hardware in scope of the CRA, thus resistors and screws do not need to be included



FprEN 40000-1-2 Principles, product risk management, and lifecycle activities

Common principles and a risk-based approach across the product lifecycle

- Covers CRA Annex I, Part 1, Requirement 1
- **Process standard** to ensure products are developed and maintained with a risk-based approach to cover **any** security risks
- Implementation demonstrated via documented process outputs
- Covers all lifecycle activities, with non-normative references to 40000-1-3 and 40000-1-4



FprEN 40000-1-3 Vulnerability handling

Managing vulnerabilities throughout the product lifecycle

- Covers CRA Annex I, Part 2
- **Process standard** to ensure products are maintained in a secure state using a risk-based approach
- Implementation demonstrated via documented process outputs and actions in the market updates, notifications, recalls, etc.
- Augments 40000-1-2 activities with specific requirements and assessment criteria for post-market activities



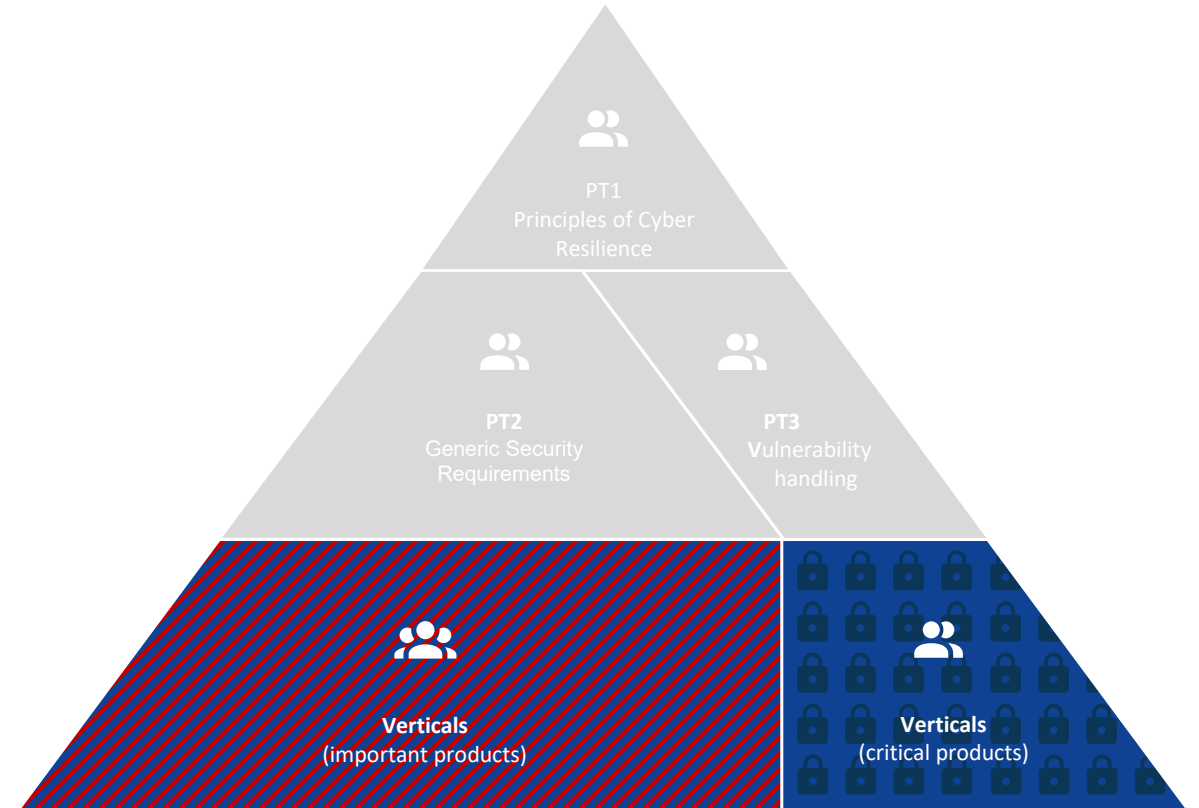
FprEN 40000-1-4 Generic security requirements

Common product security requirements

- Covers CRA Annex I, Part 1, Requirement 2(a) – 2(m)
- **Product standard** addressing a specific set of security requirements by mapping security objectives to a catalogue of possible security controls
- Implementation demonstrated via the product itself and/or supported by technical documentation

CRA “Vertical” standards – applicable to specific product categories

- Vertical standards cover product categories defined in the **Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements**
- They are developed jointly and in a coordinated manner in ETSI, CEN and CLC technical groups
- 32 harmonised standards are requested, to provide presumption of conformity with the essential requirements of the CRA
- Project teams, experts and rapporteurs are supported by EU and EFTA funded projects STAN4CR and CYBESTAND.eu



CEN, CENELEC and ETSI

Special setting

- Important products class I
- Important products class II
- Critical products



ETSI TC Cyber WG EUSR

Leads the development of 18 CRA product standards

- EN 304 617 – Browsers
- EN 304 618 – Password Managers
- EN 304 619 – Software that searches, removes, or quarantines malicious software (Antivirus)
- EN 304 620 – Virtual Private Networks (VPNs)
- EN 304 621 – Network Management Systems (NMS)
- EN 304 622 – Security Information and Management Systems (SIEM)
- EN 304 623 – Boot Managers
- EN 304 624 – Public Key Infrastructures (PKI) and digital certificate issuance software
- EN 304 625 – Physical and virtual network interfaces
- EN 304 626 – Operating Systems (OS)
- EN 304 627 – Routers, modems intended for the connection to the internet and switches
- EN 304 631 – Smart home general purpose virtual assistants
- EN 304 632 – Smart home products with security functionalities
- EN 304 633 – Internet connected toys
- EN 304 634 – Personal wearable products
- EN 304 635 – Hypervisors and container runtime systems
- EN 304 636 – Firewalls, intrusion detection and/or prevention systems
- EN 304 642 – Network functions of telecommunications systems

-  Important products class I
-  Important products class II
-  Critical products



CEN/TC 224 'Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment'

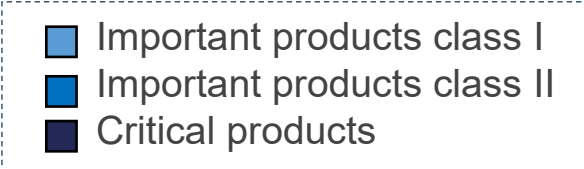
- Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
 - **ENQ Comment resolution > FV**
 - **OJEU citation**
- Hardware Devices with Security Boxes
 - **ENQ Comment resolution > FV**
 - **OJEU citation**
- Smart Card applications
 - **ENQ Comment resolution > FV**
 - **OJEU citation**

- Important products class I
- Important products class II
- Critical products



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

-  microprocessors and microcontrollers with security-related functionalities
 - **HAS Assessment & FV**
 - **OJEU citation**
-  application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) security-related functionalities
 - **ENQ**
 - **OJEU citation**
-  tamper-resistant microprocessors and microcontrollers
 - **HAS Resolution & FV**
 - **OJEU citation**
-  Platforms of Smart Cards and Similar Devices Including Secure Elements
 - **HAS Resolution & FV**
 - **OJEU citation**

- 
-  Important products class I
 -  Important products class II
 -  Critical products

Vertical standards development



CLC/TC 65X 'Industrial-process measurement, control and automation'

EN IEC 62443-4-1/-4-2 provide the common OT requirements from which the CRA product-specific vertical standards intended for OJEU citation are derived. Both standards are not foreseen for citation in the OJEU.

products with digital elements with the function of virtual private network (VPN)
network management systems
Security information and event management (SIEM) systems
physical and virtual network interfaces
routers, modems intended for the connection to the internet, and switches

- **All under FWD**
- **OJEU citation**

■ firewalls, intrusion, detection and/or prevention systems, including specifically those intended for industrial use

- **ENQ**
- **OJEU citation**

- Important products class I
- Important products class II
- Critical products

Vertical standards



CEN-CLC/JTC 13 WG 6: 'Product Security'

- smart meter gateways within smart metering systems
 - **FWD**
 - **OJEU citation**

- Important products class I
- Important products class II
- Critical products

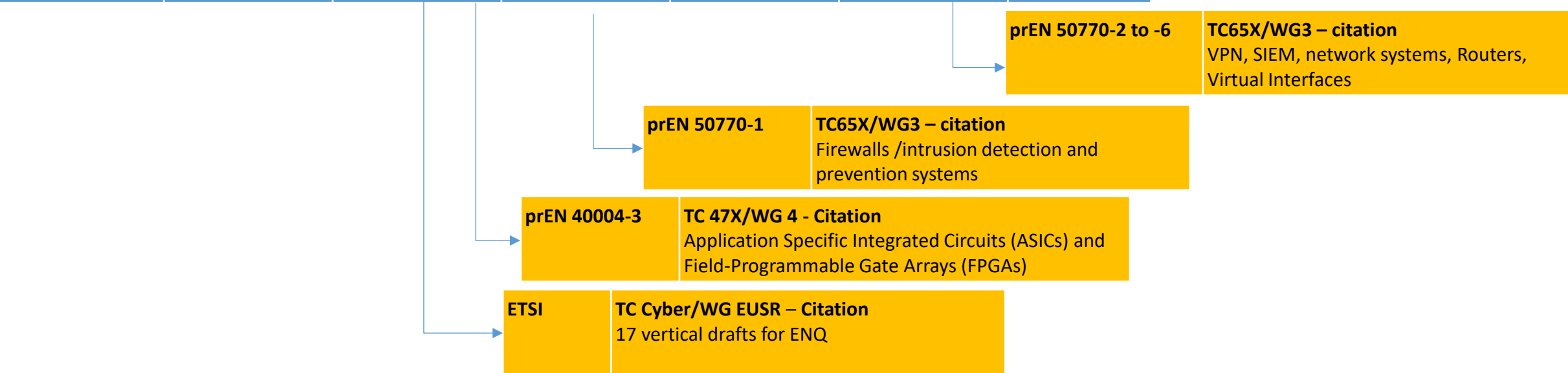
Overview Public Enquiry – Contribution and national participation



2026

2027

July	August	September	October	November	December	January
------	--------	-----------	---------	----------	----------	---------



How to contribute:

Under FWD	prEN 40000-1-4 Generic security prEN XXX Smart Meter Gateway - Citation
-----------	--

Public Enquiry: Consolidated versions subject to national vote and public commenting through the national members of CEN, CENELEC and ETSI.

Overview Formal Vote – bringing to Publication

2026

2027

July	August	September	October	November	December	January
------	--------	-----------	---------	----------	----------	---------



Formal Vote period:
shortened to 4 weeks
(instead of 8 weeks)

FprEN 40000-1
FprEN 40000-2

JTC 19/WG 9:
Part 1-1: Vocabulary
Part 1-2: Principles, product risk management

prEN EN IEC 62443-4-1:2018/prAA:2026
prEN EN IEC 62443-4-2:2018/prAA:2026

TC 65X/WG3:
• Part 4-1: Secure product development lifecycle requirements
• Part 4-2: Technical security requirements for ACS components

prEN 40001-3
prEN 40002-3

TC47XX/WG 1-2 - Citation
• Microprocessors and microcontrollers with security-related functionalities
• Tamper-resistant microprocessors and microcontrollers

FprEN 40003-3

TC 47X/WG 3 - Citation
Smartcards and similar devices including secure elements

prEN 40000-1-3

JTC 19/WG 9 - Citation
Part 1-3: Vulnerability handling

prEN 40000-10
prEN 40000-11
prEN 18330

TC 224/WG 17 - Citation
• Part 10: Products with digital elements used in identity management systems
• Part 11: Hardware Devices with Security Boxes
• Smartcards or similar devices, including secure elements - Application layer

CRA STANDARDS: MOVING FROM DRAFTING TO APPROVAL

CEN–CENELEC

11 projects at or before FV/
moving into finalization

**2 First
Working
Draft**

7 ENQUIRY

ETSI

17 vertical standards
published to ENQ

Product-specific standards spanning:

For IT: Browsers • Operating systems • VPNs • Routers
SIEM • Consumer connected products • Security products

National Standardisation Organisations and stakeholders can
now comment through the Public Enquiry process.

The CRA standards programme is shifting from drafting to consultation and final approval — with multiple deliverables now close to completion.

*Thank you
for your attention!*



YVES LEBOUCHER

CEN – CENELEC Sectoral Project Manager
Electro & Digital Technologies- Standardization

yleboucher@cencenelec.eu

www.cencenelec.eu

Follow us:



Tag us @standards4EU