



CENTRE TECNOLÒGIC DE TELECOMUNICACIONS DE CATALUNYA (CTTC)

PACKET OPTICAL NETWORKS AND SERVICES RESEARCH UNIT

RAUL MUÑOZ,
RESEARCH DIRECTOR (R4),
HEAD OF THE PACKET OPTICAL NETWORKS AND SERVICES



Centre Tecnològic de
Telecomunicacions de Catalunya



INTRODUCTION TO CENTRE TECNOLÒGIC DE TELECOMUNICACIONS DE CATALUNYA (CTTC)

MISSION & VISION

CTTC's core activity is the conception, design and implementation of **research and development projects in telecommunications and geomatics**, which must produce **innovative results** in all their development phases, in both **scientific and engineering terms**.

- To establish durable **links** with the **industrial and business** sectors, reinforcing CTTC's position as a player of innovation process through its research with industry.
- To be an **Excellence flagship Center** that serves as a bridge between academia and industry.
- A center that influences the future paths of **communication technologies, systems, networks, and geomatics**.



WHO WE ARE



Non-profit research center, founded in 2001 from public initiative.



Structural funds from “Generalitat de Catalunya”.



Self-funded: approximately 60 of our running cost (competitive funds & industrial projects).



Cutting-edge laboratories, state-of-the-art testbeds (own developments).



Fundamental and Applied Research. International Collaboration Network.



Innovations and Inventions.

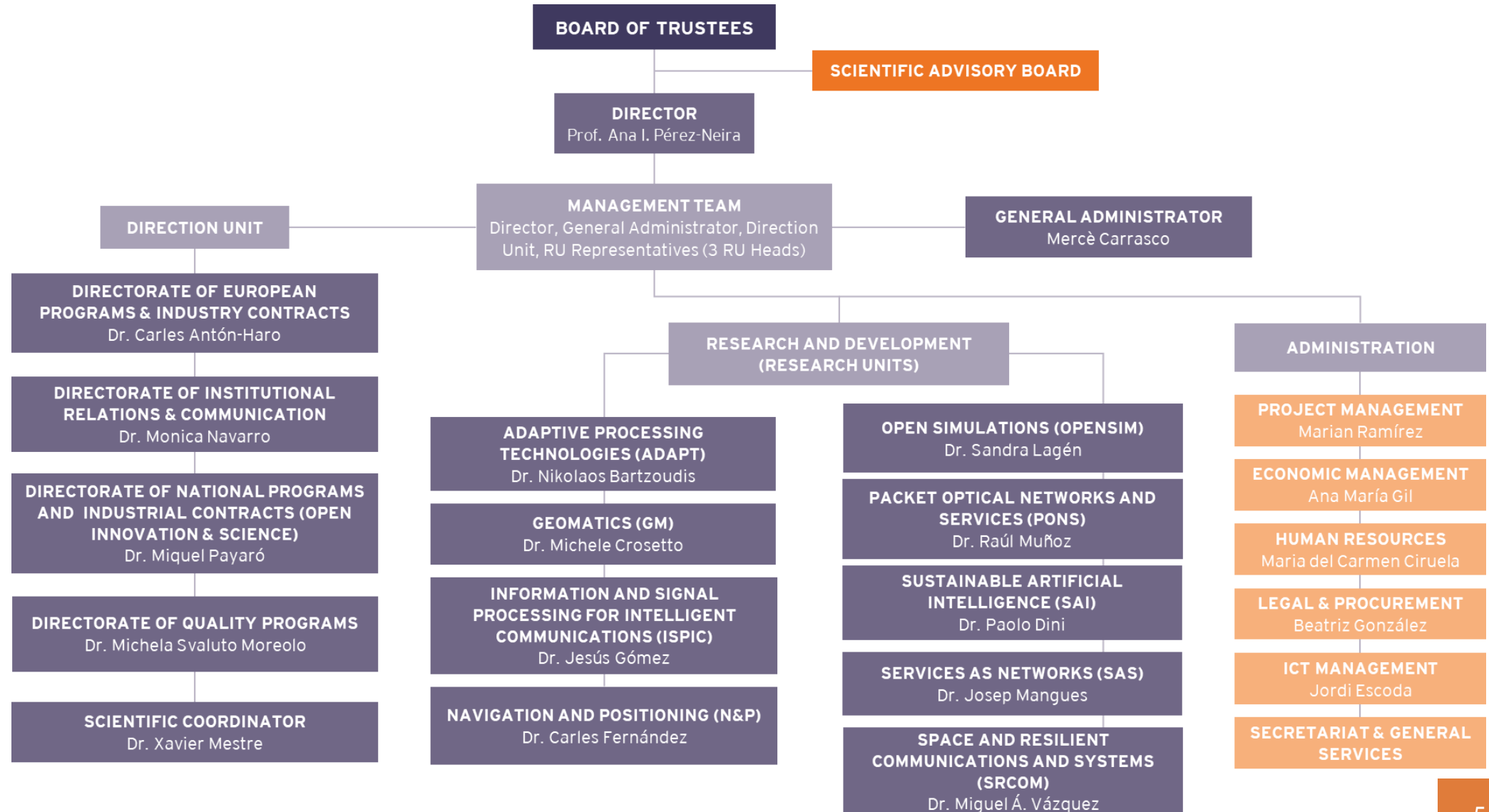


Contributes with more than 80 journals and 125 conference publications per year.



We contribute to training: host PhD candidates, + schools + master and undergraduate thesis.

ORGANIZATION

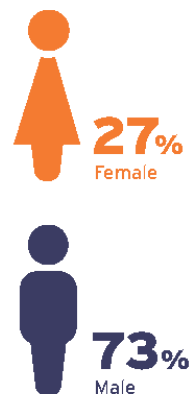
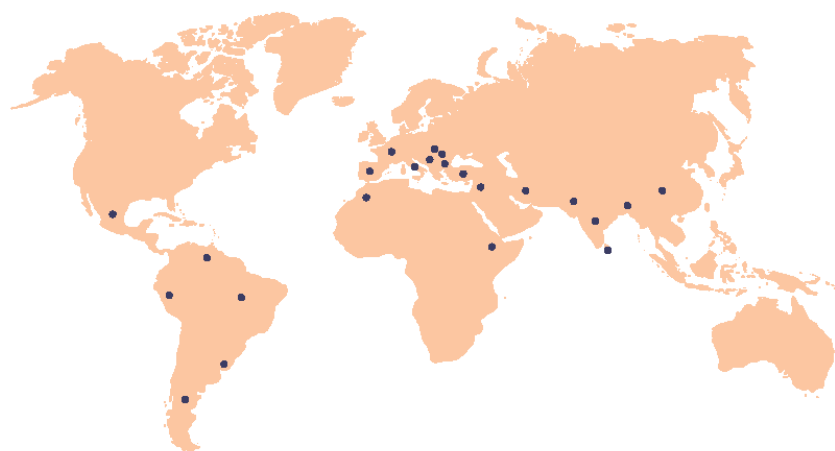


KEY FIGURES

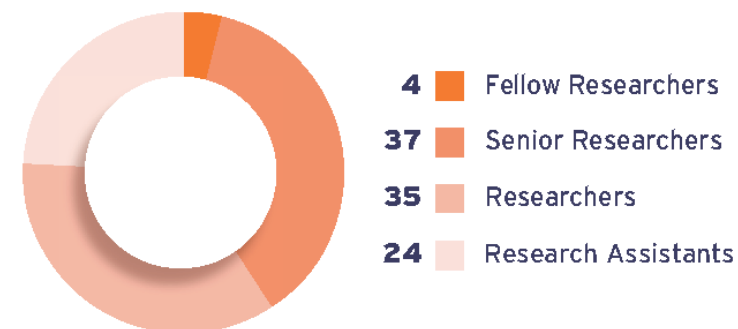
STAFF

133

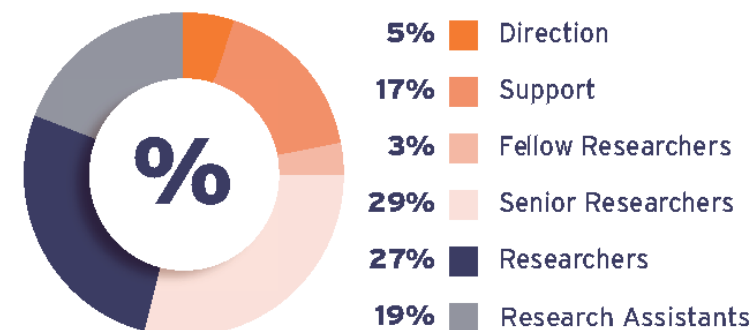
TEAM MEMBERS



R&D Personnel



Staff





INTRODUCTION TO PACKET OPTICAL NETWORKS AND SERVICES RESEARCH UNIT

PONS TEAM

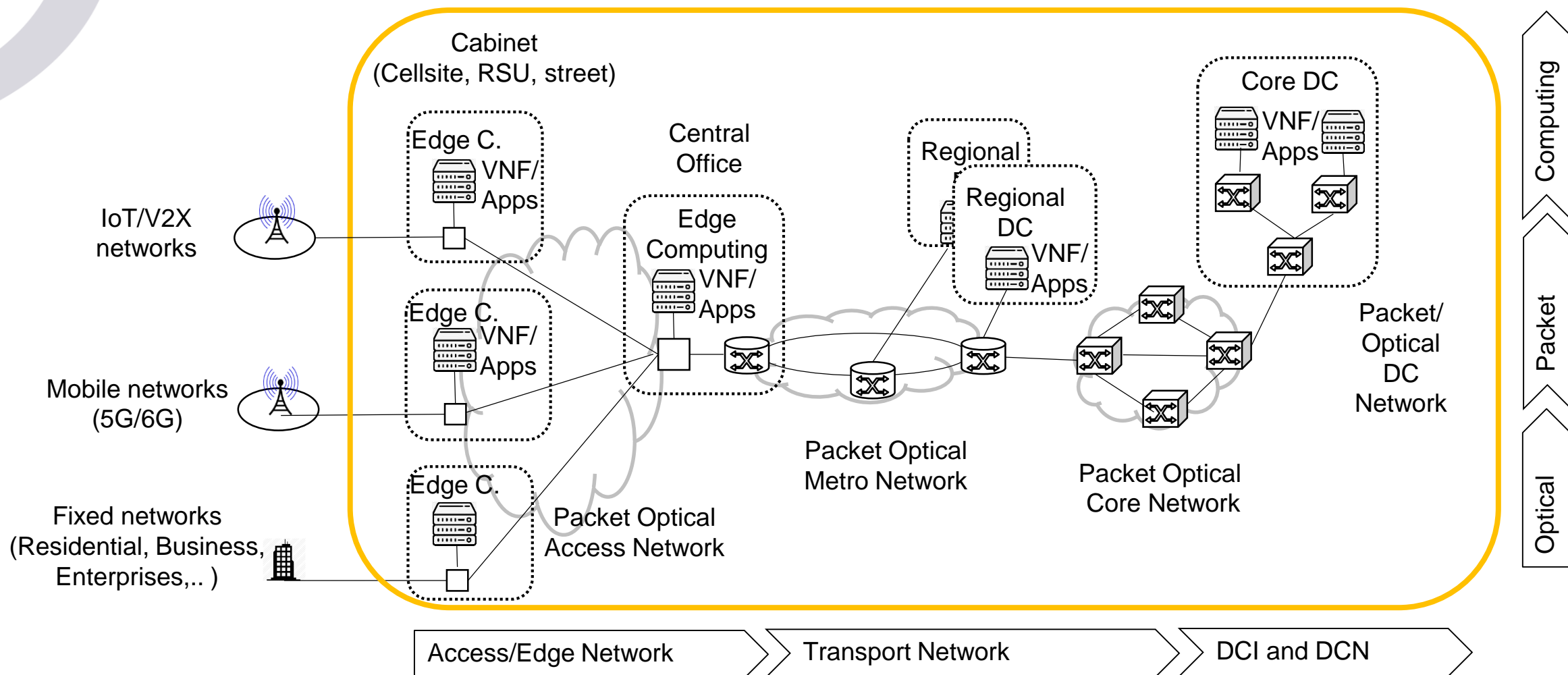
- Inter-disciplinary and international research team, covering from optical (and quantum) communications to optical network control, service management, and security



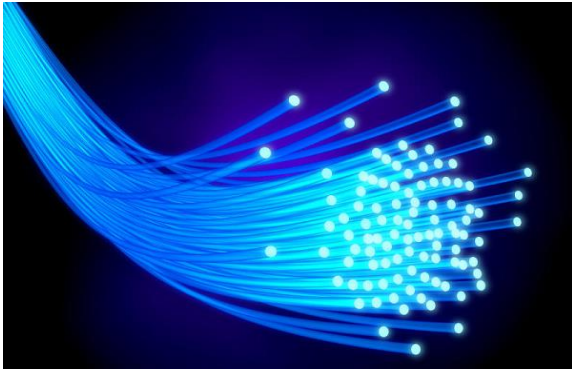
 12 Permanent Researchers

 7 Temporal Researchers

SCOPE: FIXED NETWORKS FOR 6G AND AI



RESEARCH LINES



Photonic and quantum communication technologies

- High-performance optical transmission and network telemetry systems
- Photonic technologies and transceiver solutions
- Quantum communications



Control and Telemetry of Autonomous Packet/Optical Networks

- Network Control and (Streaming) Telemetry
- Configuration and Control of Programmable Forwarding Pipelines and Open Devices
- Generalized Resource Allocation
- Autonomous Networks



Zero-touch management and secured network service orchestration

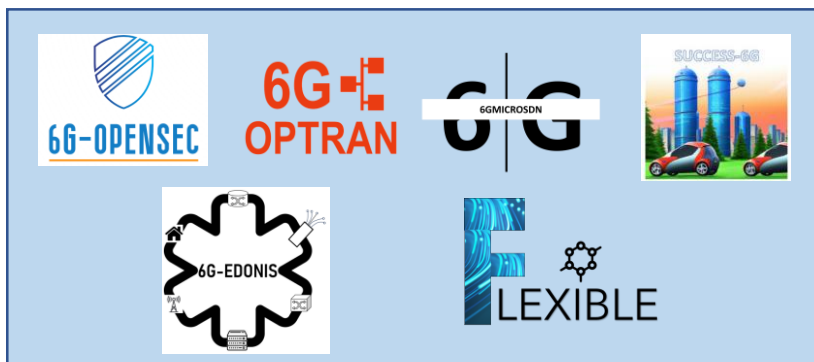
- Cloud-Edge Continuum integration
- End-to-end zero-touch management of network services
- Security and trust mechanisms for network service operations

PARTICIPATION IN LARGE EUROPEAN AND SPANISH R&D PROJECTS

Horizon Europe (SNS/CL3/CL4):
11 Projects – 2 TM



Spanish UNICO-5G (6 Projects – 5 PM)



Horizon 2020 (5GPP) Projects:
13 Projects – 1 PM



Photonics KET



Marie Skłodowska-Curie
Innovative Training Network
(ITN) (1 PM)



CONTRIBUTIONS TO MAJOR OPEN-SOURCE PROJECTS

ETSI TeraFlowSDN
(TFS)

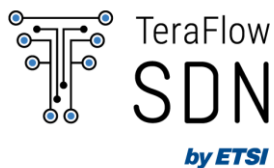
ONF Open
Networking ONOS
(ODTN)

ETSI
OpenSourcEMANO
(OSM)

ETSI OpenSlice
(OSL)

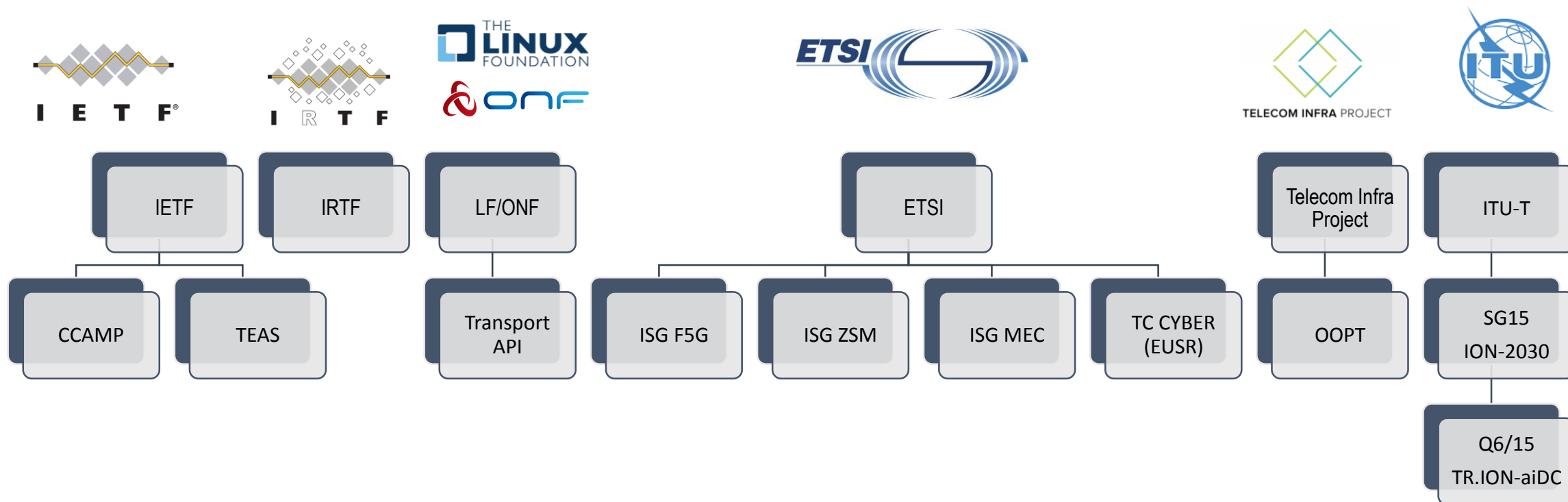
ETSI OpenCAPIF

5GPPP Sonata NFV.



Led by
CTTC

PARTICIPATION IN STANDARD DEFINING ORGANIZATIONS (SDO) AND INDUSTRIAL ASSOCIATIONS



INDUSTRY COLLABORATION NETWORK

- Network operators:



- System Vendors:

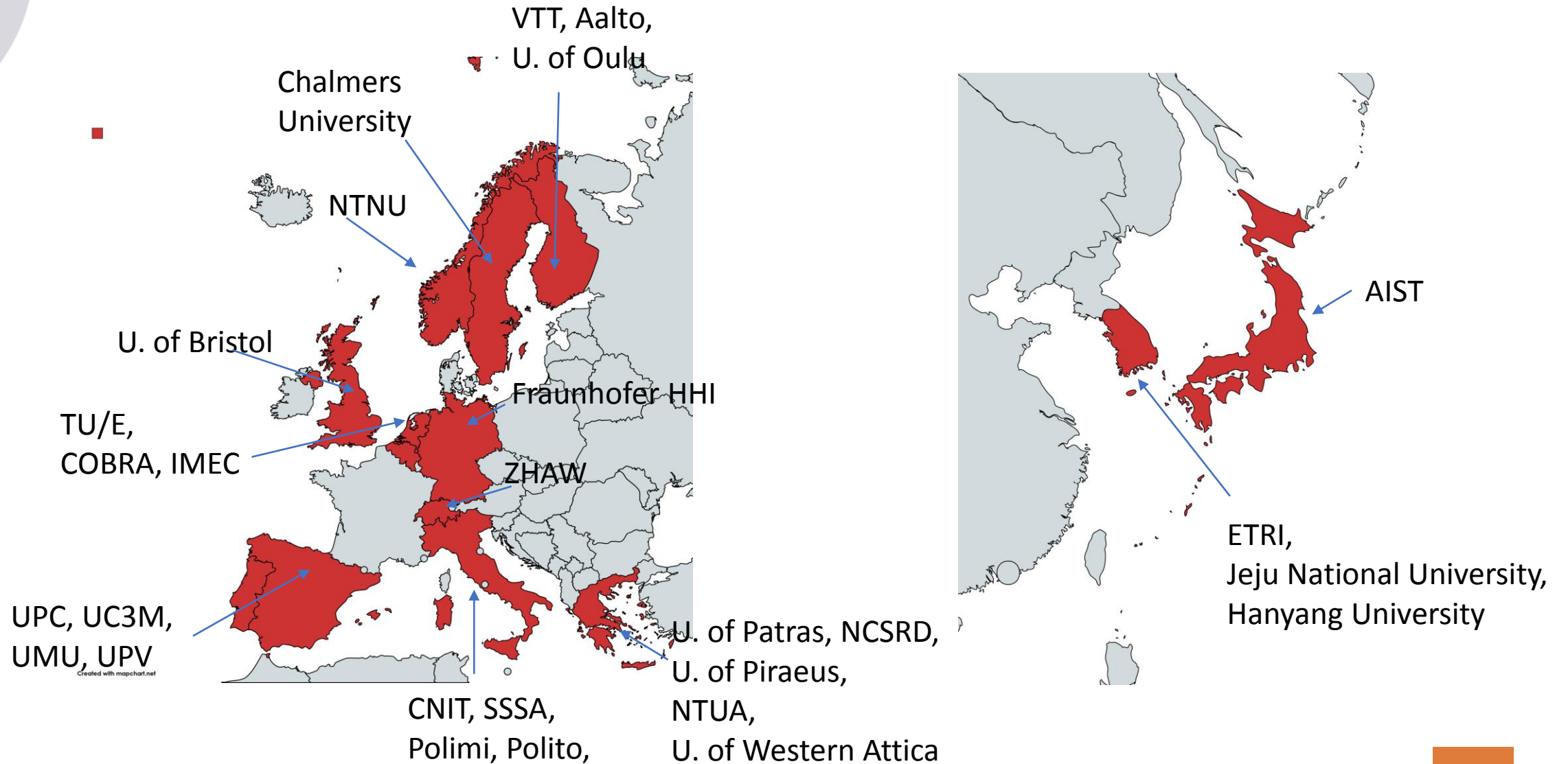


- System/Cloud Integrators:



- +20 SME form local and European ecosystem

ACADEMY COLLABORATION NETWORK



LABORATORIES: OPTICAL NETWORKING LAB

- 110m² distributed in two rooms (60m² + 50m²) in different buildings connected with 48 single mode fibers.



Transport network



Access network

LABORATORIES: OPTICAL TRANSMISSION AND SYSTEMS LAB

- 90m² distributed in two rooms (40m² + 50m²) in different buildings connected with 48 single mode fibers.

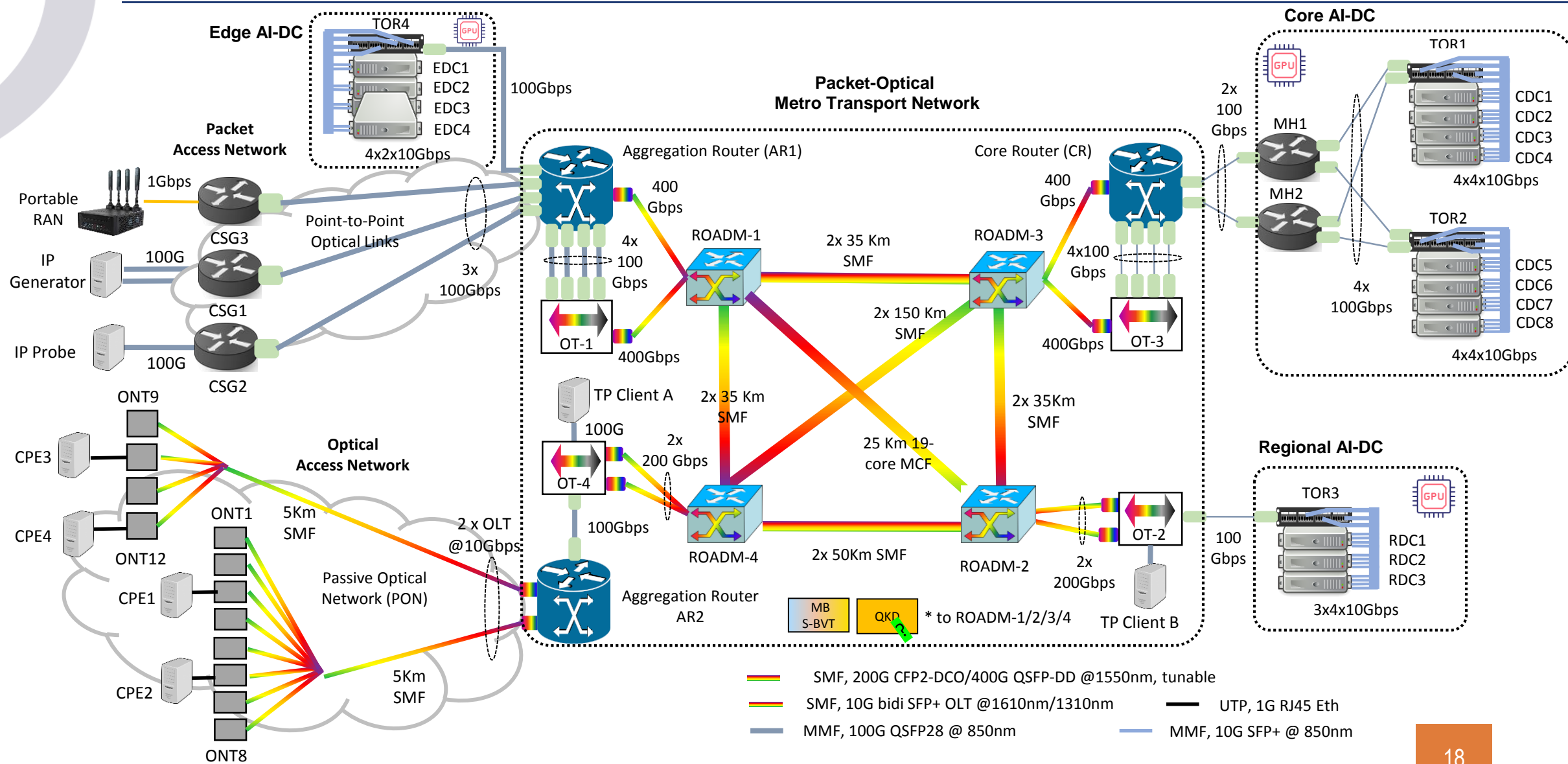


Optical communications



Access and quantum communications

ADRENALINE TESTBED: NETWORKING LAB





Advanced research for everyday life



HR EXCELLENCE IN RESEARCH



CENELEC



CYBERSTAND.eu



Centre Tecnològic de
Telecomunicacions de Catalunya

CRA Standards Unlocked

EU Tour in Barcelona

26 March 2026, 09:00-17:00 CET
Avinguda Carl Friedrich Gauss 7,
Castelldefels, 08860, Barcelona, Spain



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
CONFERENCE CENTRE





European Standardization Organizations

CRA STANDARDS UNLOCKED – EU TOUR in Barcelona – 26 March 2026

ESOs Role in CRA standardisation – How to engage

STAN4CR, STAN4CR2, CYBERSTAND.eu projects



Who we are?

- CEN, CENELEC and ETSI are the three European Standards Organizations (ESOs) officially recognised in [Regulation EU 1025/2012](#)



Standardization in various
business sectors



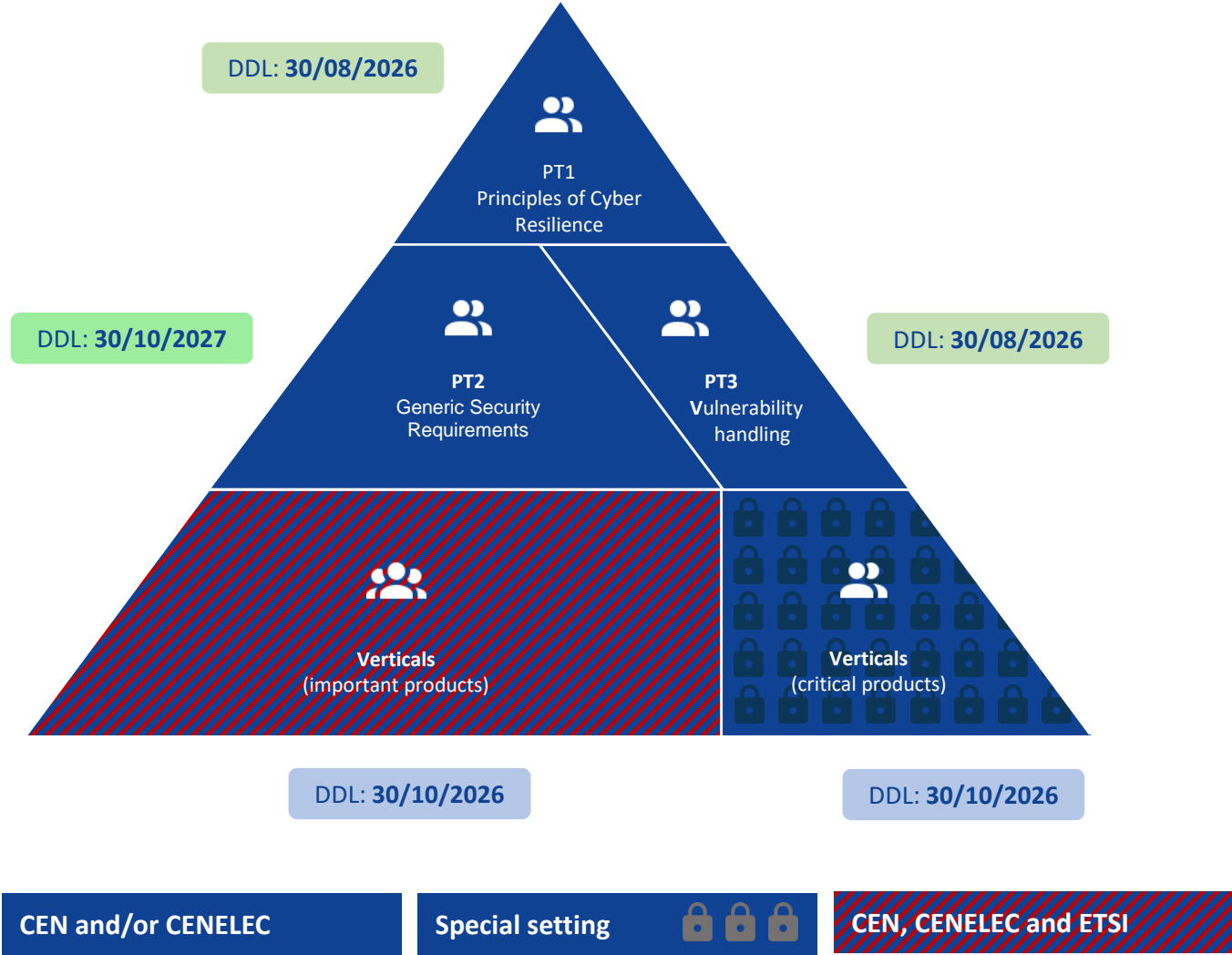
Standardization in the
Electrotechnology sector



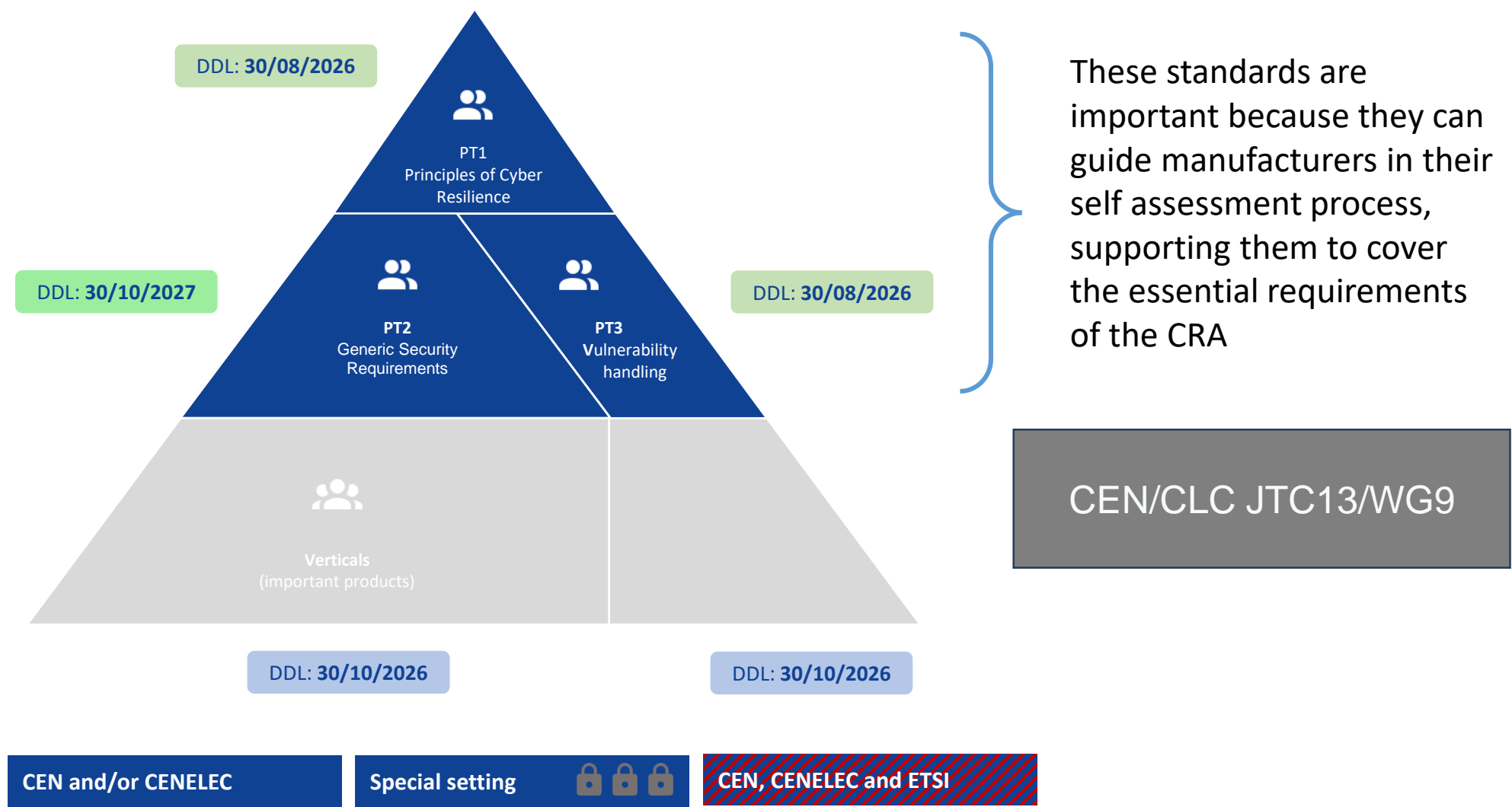
Standardization in Information
and Communication Technology
sectors



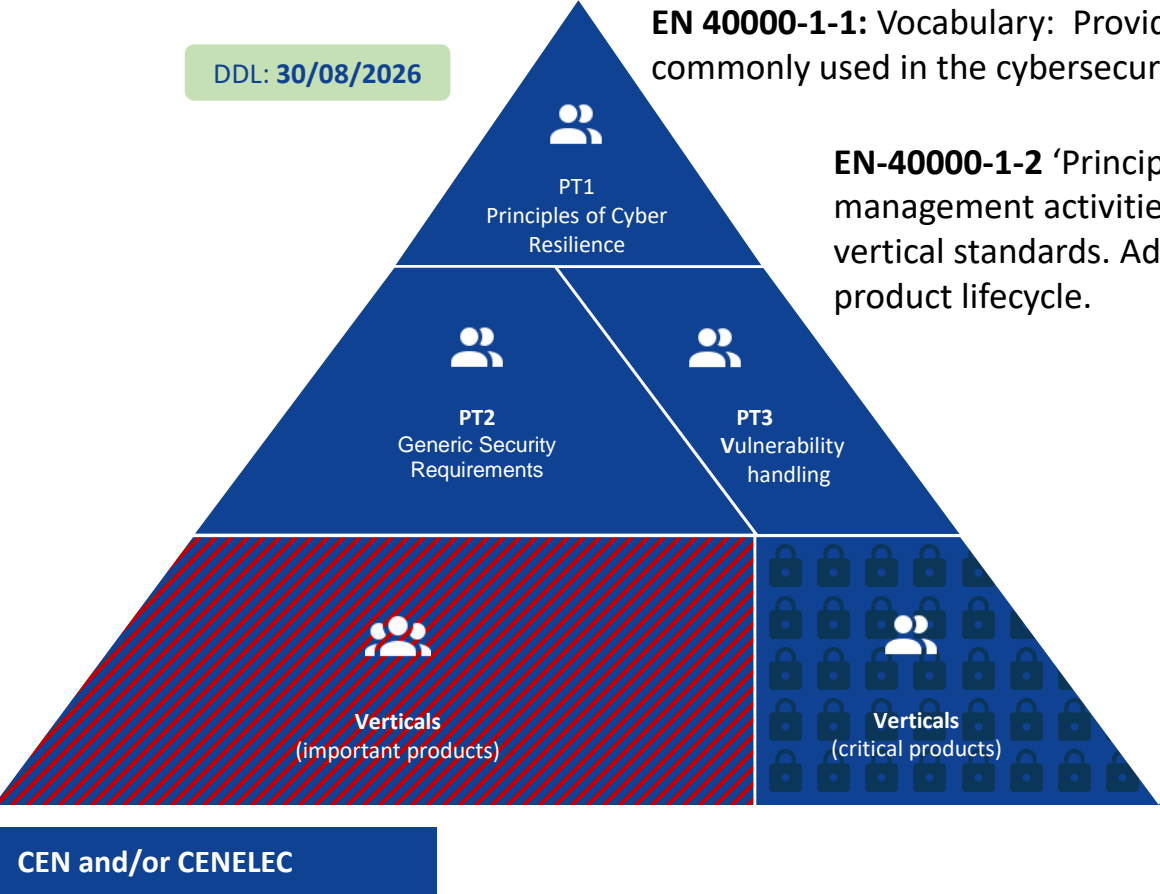
CRA standardization request



Horizontal standards



Horizontal standards



EN 40000-1-1: Vocabulary: Provides the terms and definitions commonly used in the cybersecurity requirements

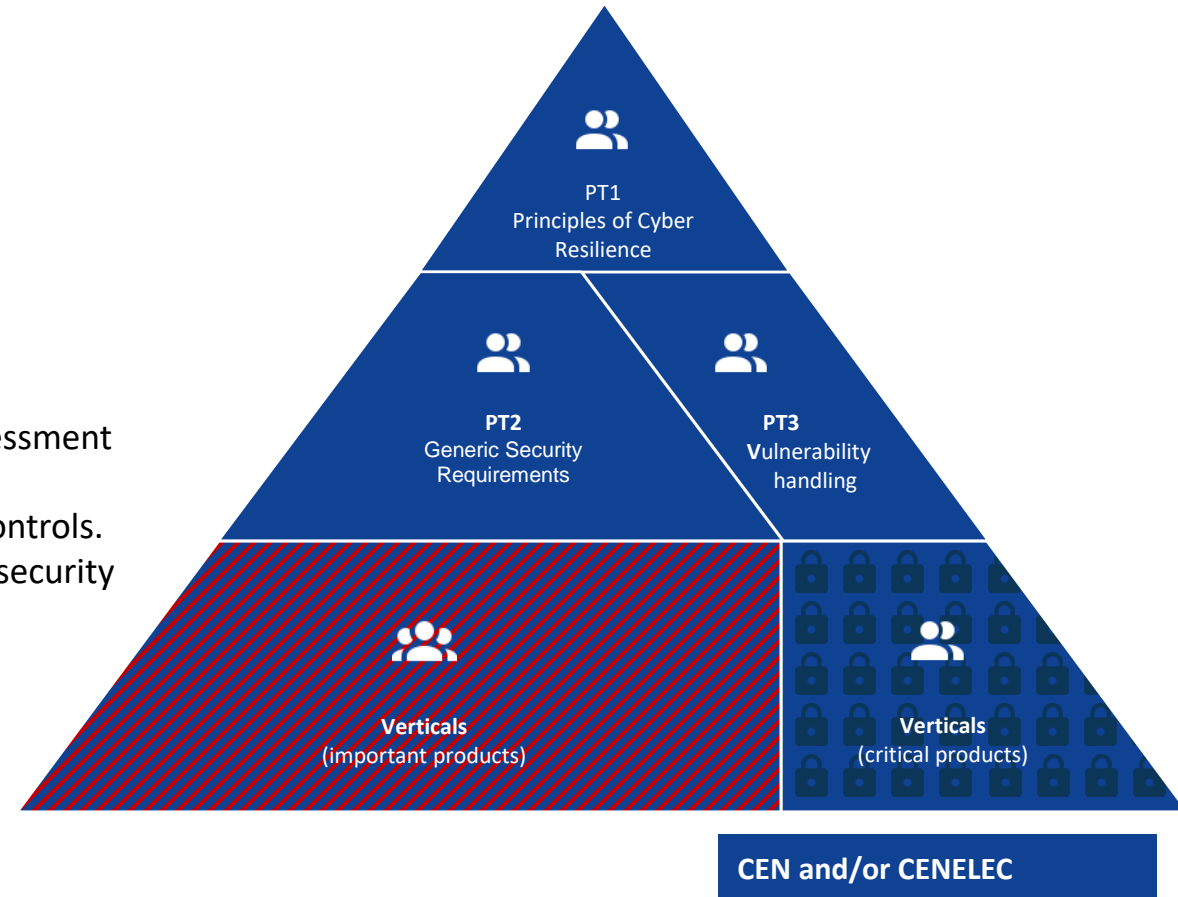
EN-40000-1-2 ‘Principles for Cyber Resilience’: General cybersecurity principles and general risk management activities for all products including generic elements to support the development of vertical standards. Addresses the process activities for security risk management during the total product lifecycle.

Horizontal standards

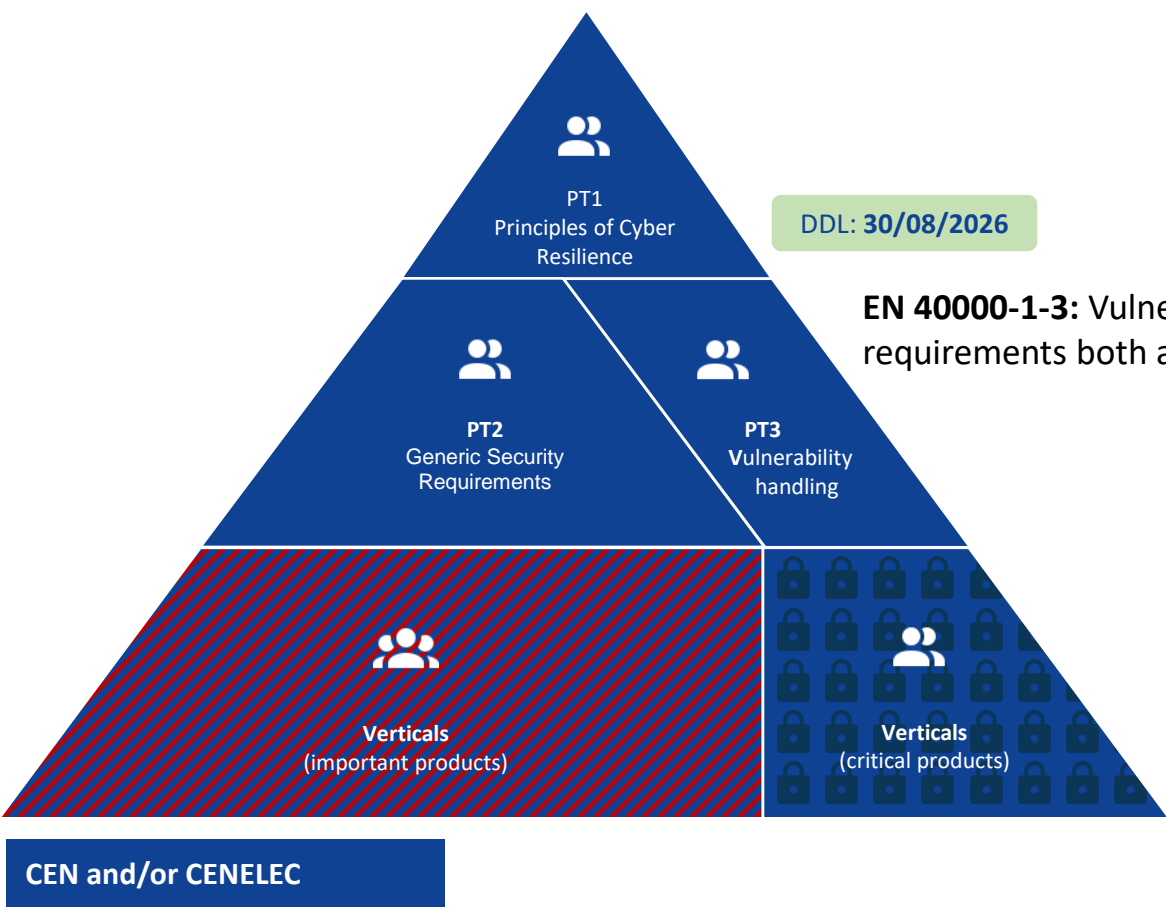
DDL: 30/10/2027

EN 40000-1-4: Security Controls - Generic security requirements

- Addressing the essential product requirements.
- Provides a library of security controls with their objectives and assessment criteria.
- Provides a mapping of the essential requirements to the security controls.
- Builds upon the EN 18031:2024 series, augmented with additional security controls.



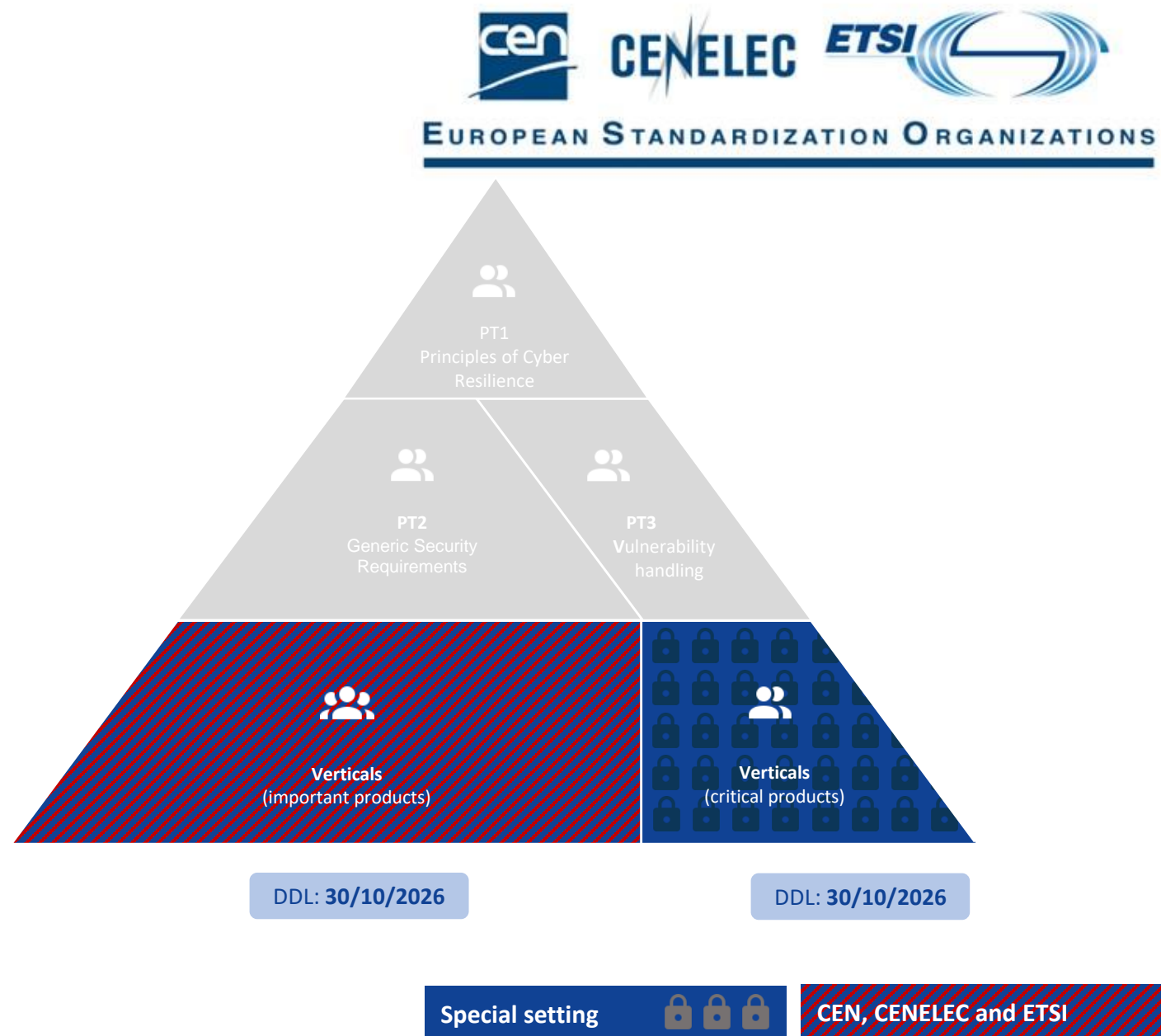
Horizontal standards



EN 40000-1-3: Vulnerability handling: specifies vulnerability handling requirements both at process and product level

Vertical standards

- 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
- 28 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 funded projects STAN4CR, STAN4CR2, CYBESTAND.eu



Vertical standards

ETSI TC Cyber EUSR

CEN/TC 224 WG 17

CLC/TC 47X WG 1-4

CLC/TC 65X WG 3

CEN-CLC/JTC 13 WG 6

ETSI TC Cyber WG EUSR

Dedicated to the development of standards in support of EU legislation, is responsible for:

- Drafting of 18 CRA product standards
- **Coordination** with relevant technical standardisation groups, CEN/CENELEC JTC 13 WG 9 and other involved groups in CEN CENELEC
- Appointment and supervision of a Specialist Task Force of experts and rapporteurs under the STAND4CR2 Action Grant
- **Inclusiveness, transparency, and openness** to allow direct participation of stakeholders of the cybersecurity ecosystem
- Early public consultations (during the drafting-stage)
- **Balanced representation** (e.g., SMEs, Open Source community, Industry, Member states agencies), and consensus-driven




Vertical standards



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

Vertical standards



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
-  Hardware Devices with Security Boxes
-  Smart card applications

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

Vertical standards



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

- microprocessors and microcontrollers with security-related functionalities
application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) security-related functionalities
- tamper-resistant microprocessors and microcontrollers
- Platforms of Smart Cards and Similar Devices Including Secure Elements

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

Vertical standards



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

Developments based on EN IEC 62443 based on the existing projects to update the following “broad verticals”:

- EN IEC 62443-4-1: Secure product development lifecycle requirements
- EN IEC 62443-4-2: Technical security requirements for IACS components
- EN IEC 62443-3-3: System security requirements and security levels

Vertical standards



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

Developments based on EN IEC 62443 for vertical standards focused on the OT aspects of:

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

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

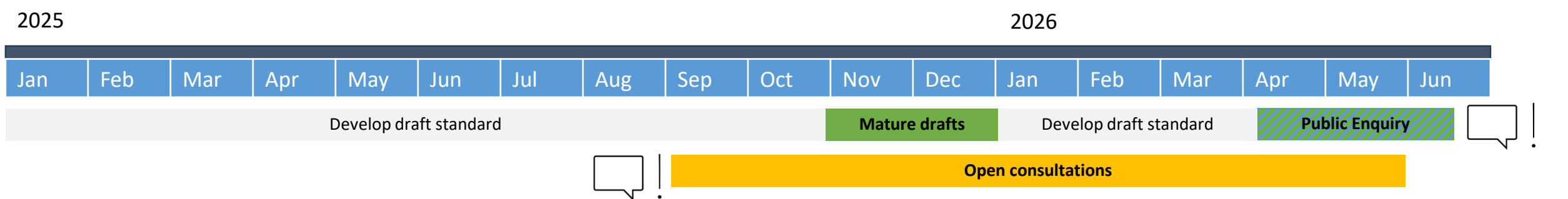
Vertical standards



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

- smart meter gateways within smart metering systems

High level timeline



How to contribute:

- Mature drafts:** Technical committee submits advanced and stable versions of the drafts for assessment of the European Commission
- Public Enquiry:** Consolidated final versions subjects to national vote and public commenting via the national members of CEN, Cenelec and ETSI
- Open consultations:** Additional stakeholder involvement, efforts under the project STAN4CR. Open to the public.





Q4 2026

Publication by ESOs

Stakeholders' engagement Dissemination roadmap



Upcoming and past Events

	Mon, Oct 13 Webinar 'CRA Standards Unlocked: Deep dive session on the draft standard focusing on the application layer of... / Webinar	DETAILS
	Mon, Sep 29 Webinar: CRA Standards Unlocked – Open public consultation on ETSI Vertical Standards / Webinar	DETAILS
	Tue, Sep 23 Workshop: Cyber Resilience Act and Horizontal Standards / Madrid	DETAILS
	Tue, Sep 09 Webinar 'CRA Standards Unlocked: From EN IEC 62443 to CRA: OT Cybersecurity for Important products Class ... / Webinar	DETAILS

[Events](#) | [Stan4cr](#)

Subscribe to get exclusive updates

Email *

[Join Our Mailing List](#)

Deep dive sessions with the rapporteurs

Home Topics Technical Work Events More

CRA Standards Unlocked: Deep Dive Session on Routers, Modems and Switches

Tue, Dec 16 | Webinar

As work on the Vertical Standards for the EU's Cyber Resilience Act (CRA) moves forward, ETSI warmly invites you to join an exclusive deep dive into the ongoing development of the European harmonized standard for Routers, Modems and Switches.

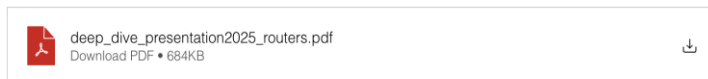
Time & Location

Dec 16, 2025, 2:00 PM – 3:30 PM
Webinar

About the event

 Recording of the webinar

▼ Download the presentation



Show More

Share this event



ETSI TC Cyber WG EUSR

How to engage in the standardisation work at ETSI – Engage directly the rapporteurs at deep dive sessions

- Agenda of upcoming sessions and replay of past sessions available on the : www.stan4cra.eu website

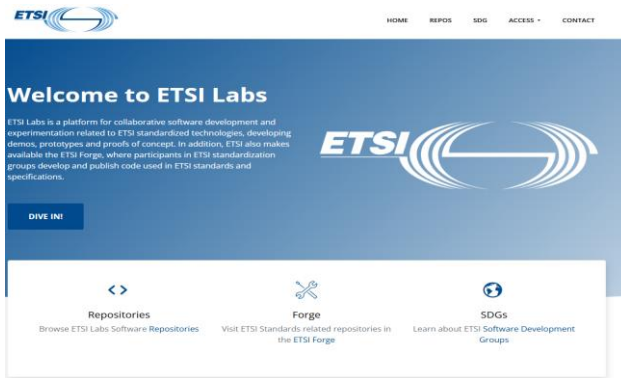
Objective:

- To present the mature drafts sent to HAS Assessment
- To collect inputs directly from stakeholders
- Recordings and slides available on the STAN4CR website

Open consultations on ETSI draft standards

ETSI TC Cyber WG EUSR

How to engage in the standardisation work at ETSI - Providing comments on working drafts



- Information website on CRA standards at : www.stan4cra.eu
- Open area for the CRA Vertical draft standards : <https://docbox.etsi.org/CYBER/EUSR/Open>
- **Online consultation platform** on working drafts at : <https://labs.etsi.org/rep/stan4cra/>
- **17 mature drafts** (and subsequent revisions) already shared publicly on this platform
- Comments handled by batch on a monthly basis **until the end of May 2026.**

Next stops of the EU Tour

Next stops:

- ▶ Paris, 27 April 2026
- ▶ Stockholm, 4 May 2026
- ▶ Malta, 21 May 2026
- ▶ Bucharest, 24 June 2026
- ▶ Lisboa, 17 Sept 2026
- ▶ Germany, TBC

Objectives:

- Get closer to potential stakeholders
- Allow direct interaction with the rapporteurs
- Leverage collaboration with other EU founded projects



Additional resources

[Home](#)

[Topics](#)

[Technical Work](#)

[Events](#)

[More](#)

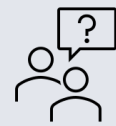


Standardization in support of the EU Cyber Resilience Act

— The Cyber Resilience Act (CRA) aims to enhance EU cybersecurity by ensuring that digital products and services remain secure throughout their lifecycle. It promotes proactive risk management and accountability, enabling businesses and users

www.stan4cra.eu

Discussion



Questions?





Normalización Española y la CRA

CRA Standards Unlocked - EU Tour in
Barcelona,
26 de marzo 2026

¿Quiénes somos?

- **La Asociación Española de Normalización**
- Somos el representante nacional oficialmente reconocido en los foros de normalización internacionales y regionales

Asociación Española de Normalización, UNE

C/Génova 6

28004 Madrid

España

E-mail: info@une.org

Tel. : (+34) 915 294 900





Entorno Europeo



Entorno Internacional



Infraestructura de la Calidad Española

Organismos Internacionales de Normalización



ISO - International Standardization Organization

- Organización internacional independiente y no gubernamental
- Integrada por 168 organismos nacionales de normalización.
- ISO elabora normas en todos los ámbitos técnicos y no técnicos, exceptuando electrotecnia y las telecomunicaciones.



IEC - International Electrotechnical Commission

- Organización internacional independiente y no gubernamental
- Integrada por 86 organismos nacionales de normalización.
- Normas relacionadas con electrotecnia y las telecomunicaciones

Organismos Europeos de Normalización



CEN – European Committee for Standardization

- Organización Europea sin ánimo de lucro integrada por 34 organismos europeos de normalización.
- Integrada CEN elabora normas en todos los ámbitos no relacionados con la electrotecnia ni las telecomunicaciones,



CENELEC – European Committee for Electrotechnical Standardization

- Organización Europea sin ánimo de lucro integrada por 34 organismos europeos de normalización
- Elabora normas en ámbitos relacionados con la electrotecnia



ETSI – European Telecommunications Standards Institute

- Organización sin ánimo de lucro
- Integrada por 850 organismos internacionales de normalización.
- Normas relacionadas con tecnologías de la información y la comunicación (TIC).

¿Qué es la normalización?

¿Qué es una norma?

Documento de carácter voluntario acordado por consenso entre expertos, en el que se definen los requisitos, las directrices o las características necesarias para garantizar que los productos, los procesos y los servicios sean adecuados para su finalidad.

Las normas respaldan la regulación, el comercio, la seguridad y la innovación: traducen las políticas en realidad técnica.

En la UE, las normas armonizadas ofrecen una «presunción de conformidad» con la legislación, como la CRA.

Cómo participar

1

Uniéndose a un comité nacional

Haciéndose miembro de un Comité Técnico a través de su organismo nacional de normalización (por ejemplo, CTN-UNE en España).

2

Colaborando como experto

Asistiendo a las reuniones de los grupos de trabajo, revisando los borradores, enviando comentarios y votando sobre las normas en fase de elaboración.


3

Influyendo en los trabajos de la UE y la ISO

Las posiciones nacionales se transmiten en CEN-CENELEC y ETSI (europeo) y en ISO – IEC (internacional).

UNE Comité Nacional de España: CTN-UNE 320

“Ciberseguridad, privacidad y protección de datos” - Comité espejo del CEN/CLC JTC 13 y del ISO/IEC JTC 1/SC 27

 **6**

CTN-UNE 320 / Subcomités
(SC1–SC6)

 **124+**

Expertos Registrados

 **60+**

Organizaciones participantes

Subcomités	Ámbito nacional	Espejo europeo	Espejo ISO/IEC
SC1	Cybersecurity Management Systems (ISMS)	CEN/CLC JTC13/WG2	ISO/IEC SC27/WG1
SC2	Cryptography & Security Mechanisms	CEN/CLC JTC13/WG10	ISO/IEC SC27/WG2
SC3	Security Evaluation, Testing & Specifications	CEN/CLC JTC13/WG3	ISO/IEC SC27/WG3
SC4	Security Controls & Services	CEN/CLC JTC13/WG4	ISO/IEC SC27/WG4
SC5	Data Protection, Privacy & Identity Mgmt	CEN/CLC JTC13/WG5	ISO/IEC SC27/WG5
SC6	Product Security · 5G · RED · CRA	JTC13/WG6+WG7+WG8+WG9	—

UNE Colaboración española a las normas técnicas de la CRA

Papel activo en la elaboración de las normas armonizadas exigidas por la CRA



Principales contribuciones de España

Dentro del CTN-UNE 320 se creó el CTN-UNE 320/SC 6, el grupo nacional equivalente al CEN/CLC JTC13/WG9 (Grupo de Trabajo CRA), para darle el debido seguimiento.

Presidencia del CEN-CENELEC JTC 13/WG 3 «Evaluación de la seguridad» y del WG 10 «Ciberseguridad para la criptografía» del comité Conjunto CEN/CLC, bajo la dirección de España (Miguel Bañón)

Jornada de difusión y taller inmersivo del proyecto STAN4CR (septiembre de 2025): 948 inscritos de más de 40 países.

Influencia activa con envío de comentarios de proyectos de normas prEN 40000-1-1, 40000-1-2 y 40000-1-3 (CRA PT 1, 2 y 3)



Hoja de ruta de normalización de la CRA

Ago 2026

Norma de procesos horizontales: principios generales de diseño de la ciberresiliencia (punto 1)

Ago 2026

Gestión de vulnerabilidades (punto 15)

Oct 2026

Requisitos específicos del producto (puntos 16 a 41 de la norma SR M/606)

Oct 2027

Norma horizontal sobre productos: requisitos generales de seguridad (puntos 2 a 14)

Dic 2027

Se exige el pleno cumplimiento de la CRA para todos los productos que contengan elementos digitales

Normalización
Española



¡GRACIAS POR SU
ATENCIÓN!

NOMBRE: FEDERICO SCHMIDT
CORREO ELECTRÓNICO:

fschmidt@une.org

UNE Normalización
Española





CRA STANDARDS UNLOCKED

IMPLICACIONES DE LA CRA PARA LA INDUSTRIA ESPAÑOLA Y LAS PYMES

26 de Marzo de 2026



David Jiménez
Director Técnico

- LA ASOCIACIÓN DE FABRICANTES DE MATERIAL ELÉCTRICO

AFME es la asociación que, desde 1982, representa los intereses de los fabricantes de material eléctrico, un sector clave en el proceso de descarbonización y la transición energética.

Nuestras empresas fabrican los equipos, componentes y soluciones para instalaciones eléctricas (Residencial, Terciario, Industrial, Red de Distribución Eléctrica y otras Infraestructuras).

137 miembros con 22.500 empleados y facturación de 6.500 millones de euros



¿Qué hacemos?





Evolución de las instalaciones técnicas con la digitalización

Las **instalaciones técnicas** han ido **evolucionando**, pasando de ser **infraestructuras aisladas** de un edificio, industria o infraestructura, a que los equipos que la forman estén conectados para **intercambiar información**

Infraestructuras Aisladas



Infraestructuras Conectadas





“La digitalización da pie a **oportunidades**, pero también a **ciber amenazas**. Como contrapartida, la UE desarrolla una **Estrategia de Ciberseguridad** y emprende iniciativas para reforzar la **seguridad** y la **resiliencia**.”

La **conectividad** aporta prestaciones y ventajas muy valiosas para un **mejor y más eficiente uso de las instalaciones** técnicas

Pero la otra cara de la moneda es la necesidad de tomar medidas para **mitigar** los nuevos **riesgos asociados** a la conectividad: la **CIBERSEGURIDAD**.



CONSECUENCIAS DE UN CIBERATAQUE

Cualquier equipo o dispositivo eléctrico conectado puede ser la **puerta de entrada** para un ciberataque, cuyas **consecuencias** pueden muy graves para las **personas** y las **empresas**.

Por ejemplo: desconexión de una instalación, parada de un proceso productivo, captura de datos sensibles, riesgos de seguridad, etc.



La Unión Europea ha desarrollado y está desarrollando regulación para abordar los **riesgos de Ciberseguridad**, de sus **países, empresas y ciudadanos**

Respecto a la Ciberseguridad y Ciber Resiliencia de los **productos** puestos en el mercado europeo, la reglamentación fundamental es la **RED DA** y la **CRA**

Directiva NIS2





La Ciberseguridad y Ciber Resiliencia de los productos conectados

REGLAMENTO DELEGADO (UE) 2022/30 DE LA COMISIÓN

de 29 de octubre de 2021

que completa la Directiva 2014/53/UE del Parlamento Europeo y del Consejo en lo que respecta a la aplicación de los requisitos esenciales contemplados en el artículo 3, apartado 3, letras d), e) y f), de dicha Directiva

RED DA

“Dispositivos inalámbricos con conexión a Internet”

Entrada en aplicación: 1 de agosto 2025



REGLAMENTO (UE) 2024/2847 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

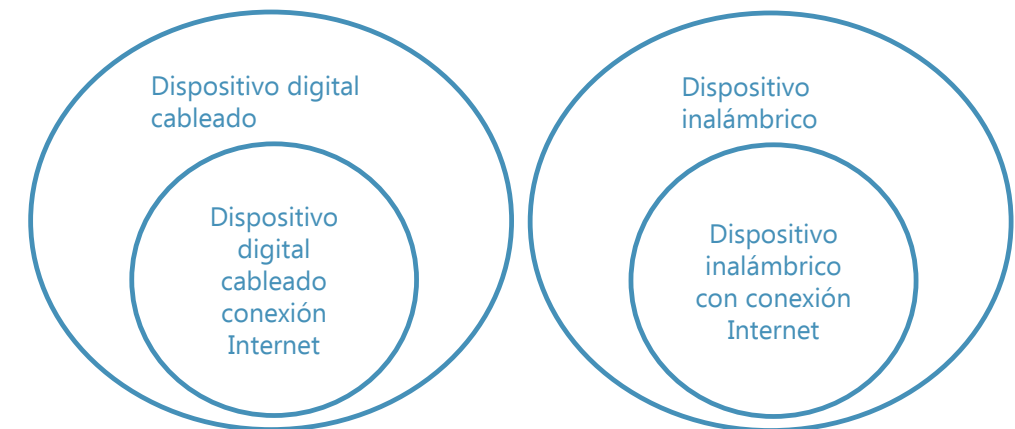
de 23 de octubre de 2024

relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia)

CRA

“Dispositivos con comunicaciones”

Entrada en aplicación: 11 de diciembre 2027



- Las empresas son muy conscientes de la importancia de que la seguridad de los equipos y dispositivos y con una larga trayectoria en la aplicación de requisitos técnicos exigentes, como las directivas: de baja tensión (LVD), de compatibilidad electromagnética (EMCD), equipos radioeléctricos (RED).
 - ☐ Directivas enfocadas a la **seguridad** que aportan los equipos (hardware)
 - ☐ **Puesta en el mercado** del producto
- La irrupción de los retos de **ciberseguridad** obliga a las empresas a **adaptarse** y **transformarse**.
 - ☐ Reglamentos que implican al **funcionamiento** del dispositivo (hardware y firmware)
 - ☐ Reglamento aplica al **sistema**, al dispositivo y elementos para su gestión (software)
 - ☐ **Puesta en el mercado** y durante su **vida operativa** (gestión vulnerabilidades)
- **Gestión de las vulnerabilidades** (nuevo paradigma para las empresas)
 - Conocer
 - Notificar
 - Evaluar
 - Corregir
 - Implementar

Anteproyecto de real decreto por el que se designa a la autoridad notificante y a la autoridad de vigilancia del mercado para los productos con elementos digitales

➤ **Autoridad de vigilancia de mercado para la RED DA y la CRA**

La **Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales** (SETID) del Ministerio para la Transformación Digital y de la Función Pública.

➤ **Autoridad Notificante de la CRA**

El **Centro Criptológico Nacional** (en adelante, CCN), adscrito al Centro Nacional de Inteligencia del Ministerio de Defensa.

La autoridad notificante podrá basarse en **certificados de acreditación** emitidos por la **Entidad Nacional de Acreditación** (en adelante, ENAC).

➤ **Laboratorio técnico de apoyo preferente**

Se designa a la S.M.E. **Instituto Nacional de Ciberseguridad de España**, M.P., S.A. (INCIBE) dependiente de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Anteproyecto de real decreto por el que se designa a la autoridad notificante y a la autoridad de vigilancia del mercado para los productos con elementos digitales

➤ Artículo 15. Medidas de apoyo a las empresas

1. De conformidad con el **artículo 33 de la CRA**, la **SETID**, en colaboración y coordinación con el **INCIBE**, podrá emprender, cuando proceda, **acciones** dirigidas a las **microempresas** y las **pequeñas y medianas empresas**, incluidas las empresas emergentes, que podrán comprender, entre otras:

a) Organizar **actividades** específicas de **sensibilización** y **formación** sobre la aplicación del Reglamento de Ciber Resiliencia.

b) **Establecer un canal** específico de comunicación con las **microempresas** y las **pequeñas empresas** y, en su caso, con las **autoridades públicas locales**, para **asesorar y responder** a preguntas sobre su aplicación.

➤ Comentario enviado por AFME a la Consulta Pública

b) Establecer un canal específico de comunicación con las microempresas, las pequeñas empresas **y medianas empresas** y, en su caso, con las autoridades públicas locales **o las asociaciones sectoriales**, para asesorar y responder a preguntas sobre su aplicación.

¿Qué papel deben de jugar la Asociaciones Sectoriales?

Las empresas se enfrentan a un doble desafío: primero el conocer y aplicar la **tecnología** asociada a la **ciberseguridad** y segundo, conocer y aplicar el **marco legal y normativo**, que además se encuentra en fase de desarrollo.

Este **esfuerzo** no es asumible por todas las empresas y les puede suponer un **gran reto** adaptarse a este nuevo paradigma, principalmente para las **pymes**.

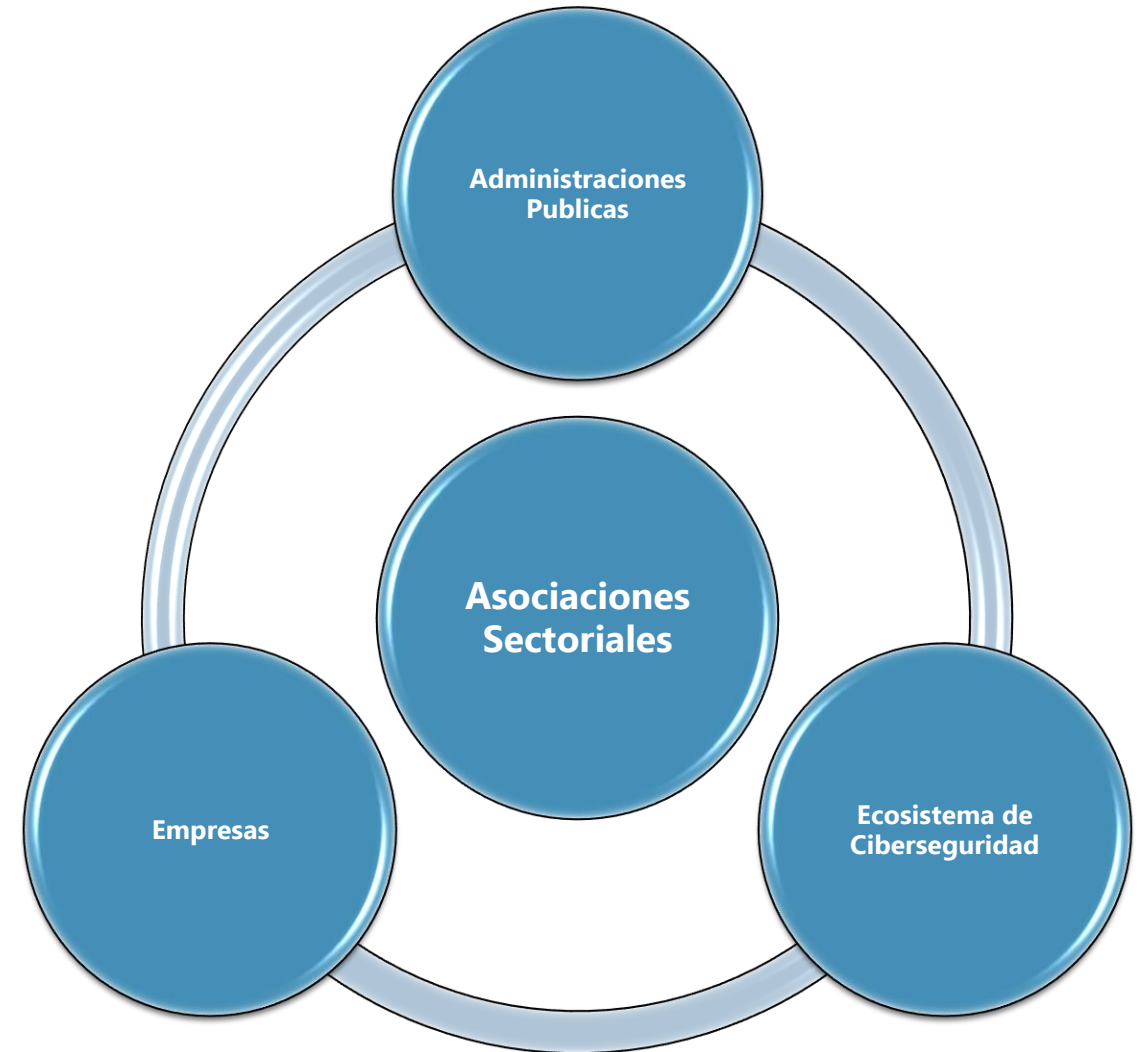
Ante esta situación, las **asociaciones sectoriales** deben jugar un **papel clave** en la promoción e interpretación de la legislación para las empresas.

Y ese papel debe jugarse **en colaboración** con las **Administraciones Públicas** y el **ecosistema** asociado a la **ciberseguridad** (empresas expertas en ciberseguridad, empresas de certificación, etc).

Pero también las **asociaciones sectoriales** deben de ser el **enlace** entre las **Administraciones Públicas** y las **empresas** que representan, para hacer llegar sus **inquietudes** y **aportaciones**.

Las **asociaciones sectoriales** como **catalizador** pueden aportar:

- Proximidad
- Difusión
- Conocimiento
- Formación
- Experiencia sectorial
- Interlocución
- Canalizar ayudas





Grupo de Trabajo AFME GT Ciber

- Canalización y procesamiento de la **información**
- **Seguimiento** de la evolución legislativa y normativa
- **Difusión** y **formación** a las empresas asociadas
- **Aportación** de las empresas a la legislación y normalización
- **Elaborar** documentos de posición y guías
- **Intercambio** de experiencias y conocimiento





MUCHAS GRACIAS POR SU
ATENCIÓN



David Jiménez
Director Técnico



DEN/CYBER-EUS-0018: Cybersecurity requirements for software that searches for, removes, or quarantines malicious software.

CRA Standards Unlocked - EU Tour in Barcelona

EN 304 619

Presented by:

Pol Alemany

Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA)



Agenda

Introduction

STAN4CR2 Project Context & Support

How the harmonised drafts aim to work

The Draft:

Clause 1 – Scope

Clause 4 – Product Context

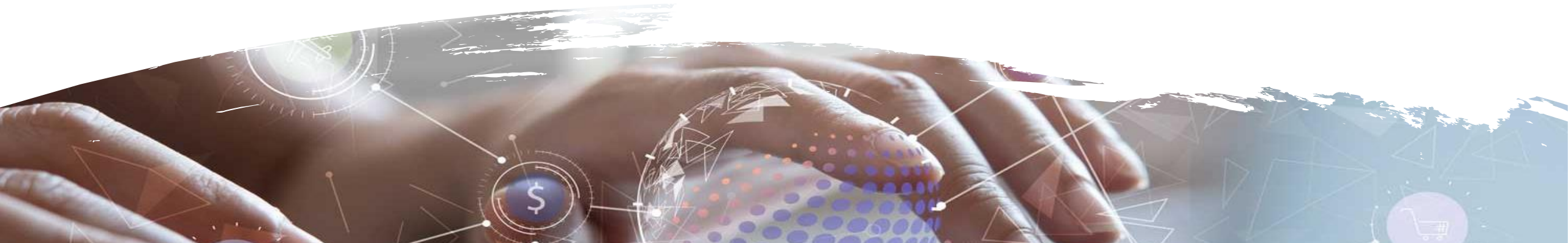
Clause 5 – Security Requirements

Clause 6 – Security Requirements Assessment

Annexes

NOTE: Clauses 2 & 3 contain
References and Definitions of terms.

Challenges & Collaboration to Solve Them



STAN4CR2 Project Context & Support

Harmonized Standards Development

STAN4CR2 focuses on creating multiple cybersecurity standards for different vertical products with digital elements to ensure CRA compliance.

Organizational Leadership and Funding

ETSI TC CYBER with funding from the European Commission and ENISA's support

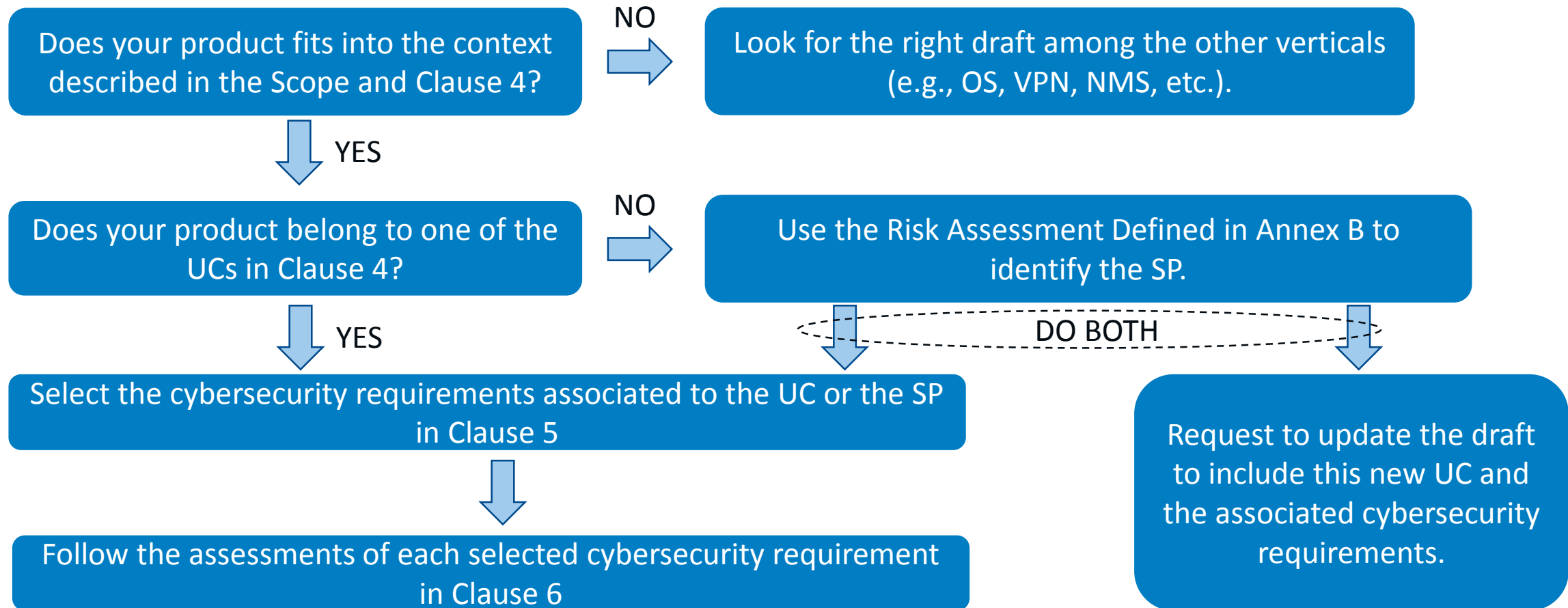
Collaborative Approach

Collaboration among industry, regulators, and academia to address cybersecurity challenges and align with EU regulations.

Impact on Product Design and Market Access

Standards developed will influence product certification and market access, promoting innovation and high security across Europe.

How the harmonised drafts aim to work



The Draft – Scope (Clause 1) & Product Context (Clause 4)

Scope (Clause 1)

Product Functions

Generic Product Architecture

Operational Environment, Distr. of Security Functions & Users

Use Cases



Scope

The draft does not substitute but complements the CRA with the main focus on ...

“software products with digital elements that detect or search for malicious software or code on a device, or remove or quarantine such software or code to prevent or mitigate system infection related to cybersecurity”



Antivirus/Antimalware

Product Functions

Identified Functions:

- **Threat Identification Function** → To analyze files, processes, system activities, or data flows to determine whether they exhibit characteristics associated with malware.
- **Threat Handling Functions** → To initiate actions that alter system state or data, such as isolating, restricting, or deleting content.
- **System Monitoring & Telemetry Functions** → To continuously observe system behavior, file operations, or network activity to enable its detection capabilities.
- **Update and maintenance Functions** → To manage the periodic updates to its detection logic, data sources, or operational modules.
- **User & System Interaction Functions** → Notifications, logs, or management interfaces that enable users or administrators to review identified threats or modify product behavior.

Generic Product Architecture

- **User Interface (UI):** ... users or administrators interact with the product.
- **Detection Data Sources:** ... local/remote sources of data used to support threat identification.
- **Behavioural or Heuristic Analysis Components:** ... analysis mechanisms ...
- **Dynamic Analysis Environment:** ... isolated or controlled execution environments ...
- **Detection Decision Logic:** Aggregates inputs (...) determines (...) potentially harmful content.
- **Threat Handling Components:** ...mechanisms for isolating, restricting, or removing content ...
- **Update and Maintenance Mechanisms:** ...means through which the product obtains updated data, configuration, or software components.
- **Logging & Telemetry Components:** Record operational events, product actions, and error conditions (...) telemetry may be shared with backend services to support threat intelligence ...
- **Backend or Remote Services:** ... remote infrastructure that may support (...) operational functions.

Operational Env., Distr. Of Cybersecurity Functions & Users

Operational Environment:

- **Physical/hardware Environment Aspects:** Physical Access Models, Removable Media and Peripheral Interfaces, Power, Shutdown and Availability Conditions, etc.
- **Logical/Software Environment Aspects:** Platform and Execution Environment, Backend and Remote Services, Interoperation with other Cybersecurity Components, etc.

Distribution of Cybersecurity Functions

- OS, Firewall, SIEM & SOAR, Boot managers, EDR/XDR

Users:

- **Security administrative user:** ...handles security-relevant settings (...) has an extensive knowledge...
- **IT administrative user:** ...deploys and maintains the product on a protected system...
- **Privileged user:** ...has elevated informative access (...), but does not have administrative access...
- **End user:** A user of the product who works on a protected system.

Use Cases

- **UC1 – Baseline Impact Context:** ... deployment scenarios in which compromise of the product would be expected to result in limited operational or systemic consequences.
- **UC2 – Elevated Impact Context:** deployment scenarios in which compromise of the product could result in organisational disruption, financial impact, or exposure of operational data.
- **UC3 – High Impact Context:** deployment scenarios in which compromise of the product could result in significant operational disruption, material financial consequences, compromise of high-value organisational data, or substantial disruption of core organisational operations.
- **UC4 – Critical Impact Context:** deployment scenarios in which compromise of the product could result in consequences extending beyond organisational boundaries, including threats to physical safety, disruption of essential services, or compromise of operations subject to critical infrastructure protection obligations.

The Draft - Requirements Specifications (Clause 5)

Cybersecurity Requirements Status

Example: Security Updates Definition and Applicability



Cybersecurity Requirements Status

No Known Exploitable Vulnerabilities (1)
Secure by Design (4)
Secure Updates (6)
Authentication and Access Control (4)
Confidentiality Protection (1+1*)
Integrity (2)
Data Minimization (1)
Availability Protection (1 + 4*)
Impact Minimization (2*)
Minimisation of Attack Surfaces (8*)
Exploitation Mitigation Mechanisms (3*)
Logging and Monitoring Mechanisms (8*)
Data Removal and Transference Mechanisms (3*)
Vulnerability Handling (14*)



- **Classified following the CRA essential requirements.**
- **20 Accepted**
- ***38 under discussion**

Example: Security Updates (I)

5.4 Secure Updates

This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (c).

- **REQ-SU-01:** The product shall validate the authenticity, integrity and provenance of all externally sourced cybersecurity-relevant data before use, including but not limited to detection signatures, threat intelligence feeds, heuristic rules, detection models, configuration data, and software updates, where applicable. Validation shall occur both during retrieval and before the data is applied or executed.
- **REQ-SU-02:** Where the product supports automatic cybersecurity updates, the product shall either (i) provide a mechanism to temporarily postpone installation of a cybersecurity update before it is applied, where technically feasible, (ii) allow update scheduling through authorised management systems, where technically feasible, or (iii) provide mechanisms to ensure the update does not negatively impact the operating environment during update (e. g., update without rebooting).
- **REQ-SU-03:** The product shall receive regular updates to the product code, configuration and detection databases during its support period (as defined in [i.1] Chapter II, Article 13, Section 8 Paragraph 3) since the product is acquired by the user.
- **REQ-SU-04:** Where the product supports automatic cybersecurity updates, the product shall either (i) provide a clear and easy to use mechanism to disable automatic cybersecurity updates, or (ii) provide mechanisms to

Applicability Example: Security Updates (II)

Table 3: Mapping of Cybersecurity Updates Requirements Applicability to the UCs & SPs

Requirements	UCs				SPs		
	UC1	UC2	UC3	UC4	Minimal	Medium	High
REQ-SU-01	X	X	X	X	X		
REQ-SU-02	X	X	X	X	X		
REQ-SU-03	X	X	X	X	X		
REQ-SU-04	X	X	X	X	X		
REQ-SU-05	X	X	X	X	X		
REQ-SU-06	X	X	X	X	X		

NOTE: As stated in Annex B.3, SPs are inclusive: Medium includes Minimal, High includes Medium.

NOTE: SP stands for Security Profile, which is defined in Annex B together with the risk assessment methodology used on the current UCs.

The Draft - Requirements Assessment (Clause 6)



Security Requirements Assessment

Assessment Objective: Defines the security property or capability that shall be verified.

Assessment Preparation: The environment, setup, and preconditions required before executing tests.

- Test environment
- Preconditions
- Required tools
- References (if necessary)

Assessment Activities: Tests execution steps to be performed such as documentation review, security functional or penetration tests, code or binaries analysis, configurations inspection and/or runtime behaviour observation.

Assignment of Verdict: Defines the pass/fail criteria.

Supporting Evidence: Defines the artefacts and documentation that shall be collected to demonstrate that the requirement has been assessed and fulfilled:


- Test or assessment reports
- Logs, configuration files, or audit traces
- Screenshots, captures, or console outputs
- Relevant vendor or design documentation

The Draft - Annexes

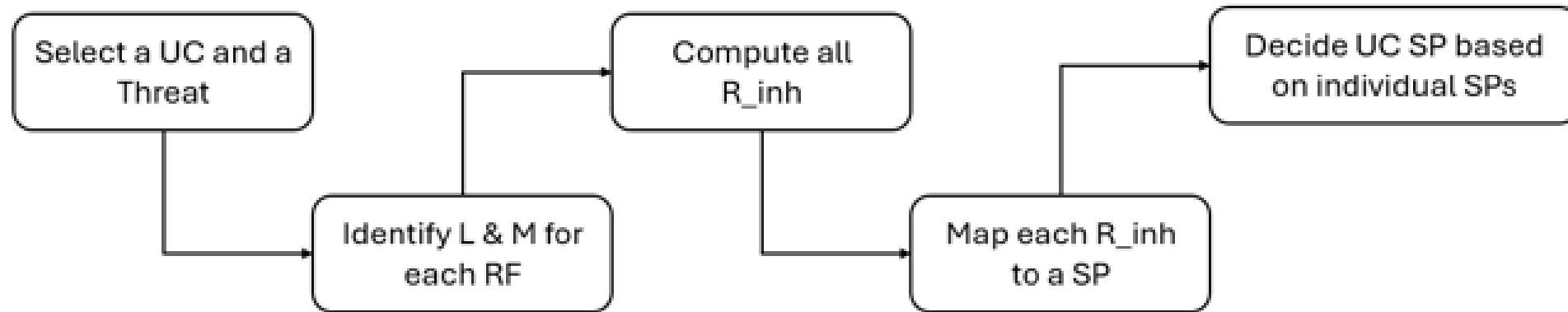
- A – Draft and EU Regulation 2024/2847 (CRA) Relationship**
- B – Methodology for the Assessment of Cybersecurity Risks**
- C – Use Cases Risk Assessment**
- D – Identified Threats
- E – Identified Risk Factors
- F – Current Virus and Malware Examples
- G – Relationship with other ETSI standards



Annex A – Draft & EU Regulation 2024/2847 (CRA) Relationship

Harmonised Standard ETSI EN 304 619					
Requirement				Requirement Conditionality	
No	Description in EU 2024/2847 (i.1)	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
1	"Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks."	Annex I, Part I, (1)	Clauses 5 and 6 <u>implement</u> a risk-based approach through scaled requirements	U	
2	"Products with digital elements shall be made available on the market without known exploitable vulnerabilities."	Annex I, Part I, (2)(a)	Clause 5.3	U	
3	"Products with digital elements shall be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state."	Annex I, Part I, (2)(b)	Clause 5.2.2	U	
4	"Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them."	Annex I, Part I, (2)(c)	Clause 5.2.3	U	
5	"Products with digital elements shall ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access"	Annex I, Part I, (2)(d)	Clause 5.2.4	U	
6	"Products with digital elements shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by best practice mechanisms, and by using other technical means."	Annex I, Part I, (2)(e)	Clause 5.2.5	U	
7	"Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions."	Annex I, Part I, (2)(f)	Clause 5.2.6	U	
8	"Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation)."	Annex I, Part I, (2)(g)	Clause 5.2.7	U	
9	"Products with digital elements shall protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks."	Annex I, Part I, (2)(h)	Clause 5.2.8	U	
10	"Products with digital elements shall minimise the negative impact by the products themselves or connected products on the availability of services provided by other products or networks."	Annex I, Part I, (2)(i)	Clause 5.2.9	U	
11	"Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces."	Annex I, Part I, (2)(j)	Clause 5.2.10	U	
12	"Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques."	Annex I, Part I, (2)(k)	Clause 5.11	U	
13	"Products with digital elements shall provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user."	Annex I, Part I, (2)(l)	Clause 5.2.12	U	
14	"Products with digital elements shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner."	Annex I, Part I, (2)(m)	Clause 5.2.13	U	

Annex B – Methodology for the Assessment of Cybersecurity Risks



Scenario: UC2 – Elevated Impact Context

Threat: TH-D1.2: Compromised Update Packages.

➡ Individual Inherent Risk = 12

L	RFL1	RFL2	RFL3	RFL4	RFL5	RFL6	RFL7	Mean RFL	Final L (rounded Mean RLF)
	3	3	4	4	3	4	3	3,43	3
M	RFM1	RFM2	RFM3	RFM4	RFM5	RFM6	RFM7	Mean RFM	Final M (rounded Mean RLM)
	4	4	5	4	4	3	3	3,86	4

Annex C – Use Cases Risk Assessment: UC2 Example

	L	M	R_inh	Individual SP	Overall SP
TH-D1.1	3	3	9	Medium (2)	High (2,111)
TH-D1.2	3	4	12	Medium (2)	
TH-D1.3	3	3	9	Medium (2)	
TH-D2.1	4	4	16	High (3)	
TH-D2.2	3	2	6	Medium (2)	
TH-D2.3	3	4	12	Medium (2)	
TH-D3.1	3	3	9	Medium (2)	
TH-D3.2	3	3	9	Medium (2)	
TH-D3.3	3	4	12	Medium (2)	
TH-D4.1	3	4	12	Medium (2)	
TH-D4.2	3	5	15	Medium (2)	
TH-D4.3	2	3	6	Medium (2)	
TH-D5.1	3	5	15	Medium (2)	
TH-D5.2	4	4	16	High (3)	
TH-D5.3	2	5	10	Medium (2)	
TH-D6.1	3	3	9	Medium (2)	
TH-D6.2	4	3	12	Medium (2)	
TH-D6.3	3	2	6	Medium (2)	

CONTRIBUTIONS ARE ALWAYS WELCOME

Access Draft Documents

ETSI Open Area provides public access to draft documents for review and commenting by diverse stakeholders.

→ <https://docbox.etsi.org/CYBER/EUSR/Open>

Collaborative Comments

ETSI Labs offers a space technical discussions to improve draft standards.

→ <https://labs.etsi.org/rep/stan4cra>



Q&A





Thank you for your attention!!

Contact: pol.alemany@cttc.cat



Co-funded by
the European Union

Follow us on:



Applied Standard Reading

Starring the VPN standard!

Presented by: Aki 🌹 Braun, Expert Zebra 🦓

For: CRA Standards Unlocked

26/03/2026



Agenda



- Explore how Pol's talk applies to a different "Important Class I" product
- Dig in to how VPNs are special
- Discuss Use Cases
- YOU can make your mark!
- Priorities for next draft

Follow along! →

<https://labs.etsi.org/rep/stan4cra/en-304-620-1/>



What am I doing here

(a question I have often asked myself)

- Rapporteur for the CRA vertical standard for VPNs
- Programmer of nearly 30 years
- Standards leader of nearly 10 years in programming languages and software
- Career in and around free and open-source software

Today is officially one year that I've been working on CRA standards!



4. Product context



- 4.1 Product Functions
- 4.2 Product Architecture
- 4.3 Operational Environment
- 4.4 Distribution of Security Functions
- 4.5 Users
- 4.6 Use Cases

Don't overthink the numbering in the current draft which is still in progress—focus on the clause titles



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#user-content-4-product-context>

4. Product context

4.1. Product functions



- What does a VPN do?



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#user-content-4-product-context>

WAIT HOLD ON



WHAT IS A VPN EVEN?

<p>5. Products with digital elements with the function of virtual private network (VPN)</p>	<p>Products with digital elements that establish an encrypted logical tunnel that is constructed from the system resources of a physical or virtual network.</p> <p>This category includes but is not limited to virtual private network clients, virtual private network servers and virtual private network gateways.</p>
---	---

For the purpose of the CRA, all of the parts **together** that allow a VPN to fulfil that function collectively constitute a **product** known as a VPN.

A VPN is a *product* consisting of VPN clients, VPN servers, et cetera.

4. Product context

4.1. Product functions



- What does a VPN do?
- Is it an enterprise VPN?
- Is it a consumer VPN?
- Is it a mesh VPN?



4. Product context

4.2. Product architecture



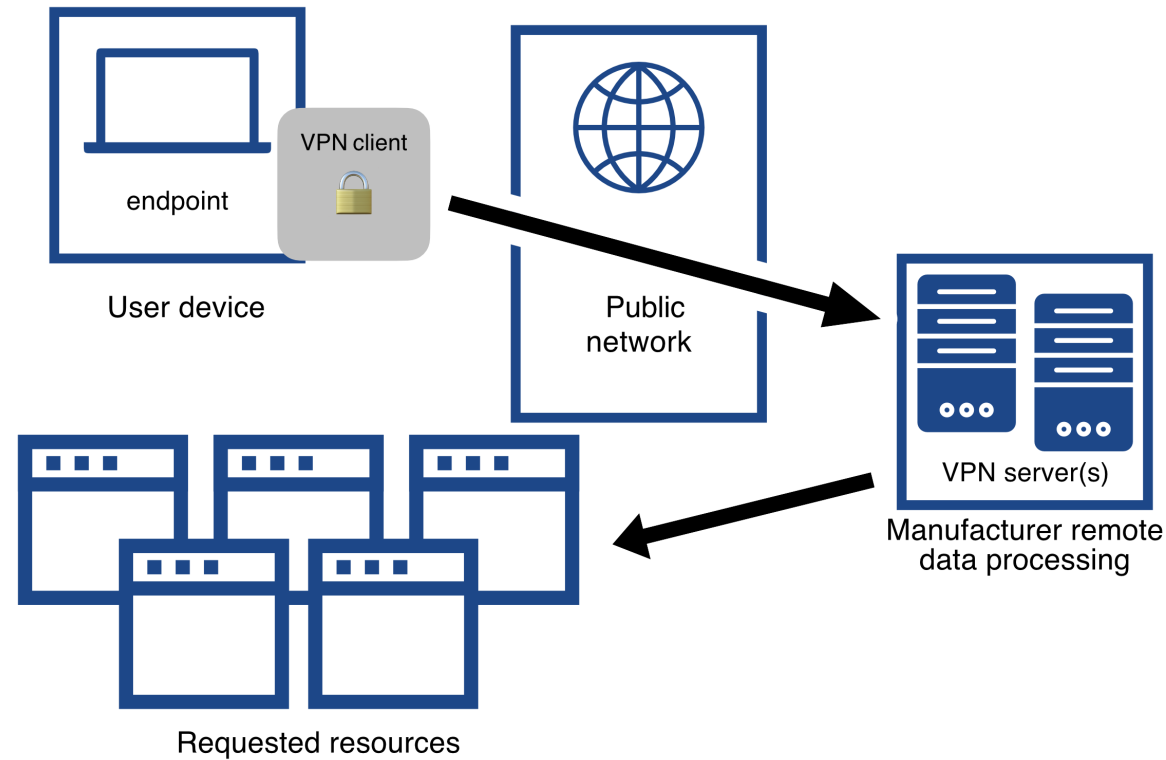
- This is what makes VPNs special
- Endless combinations



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#43-product-architecture>

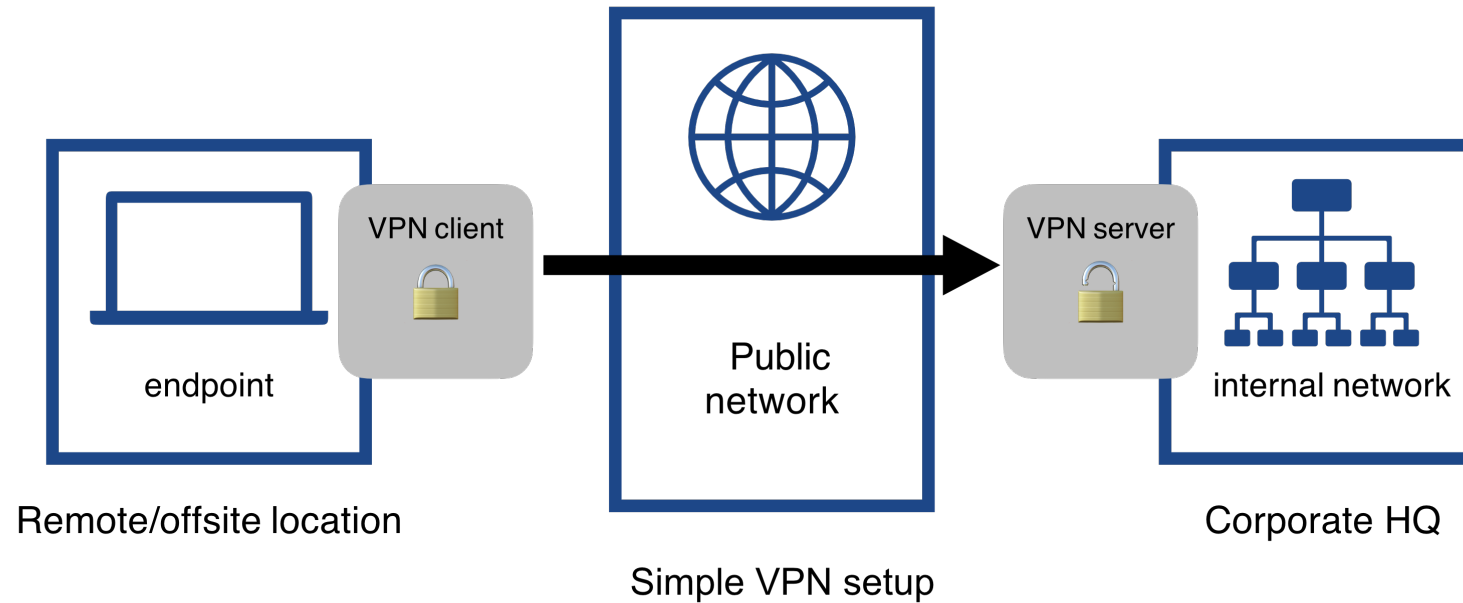
4. Product context

4.2. Product architecture



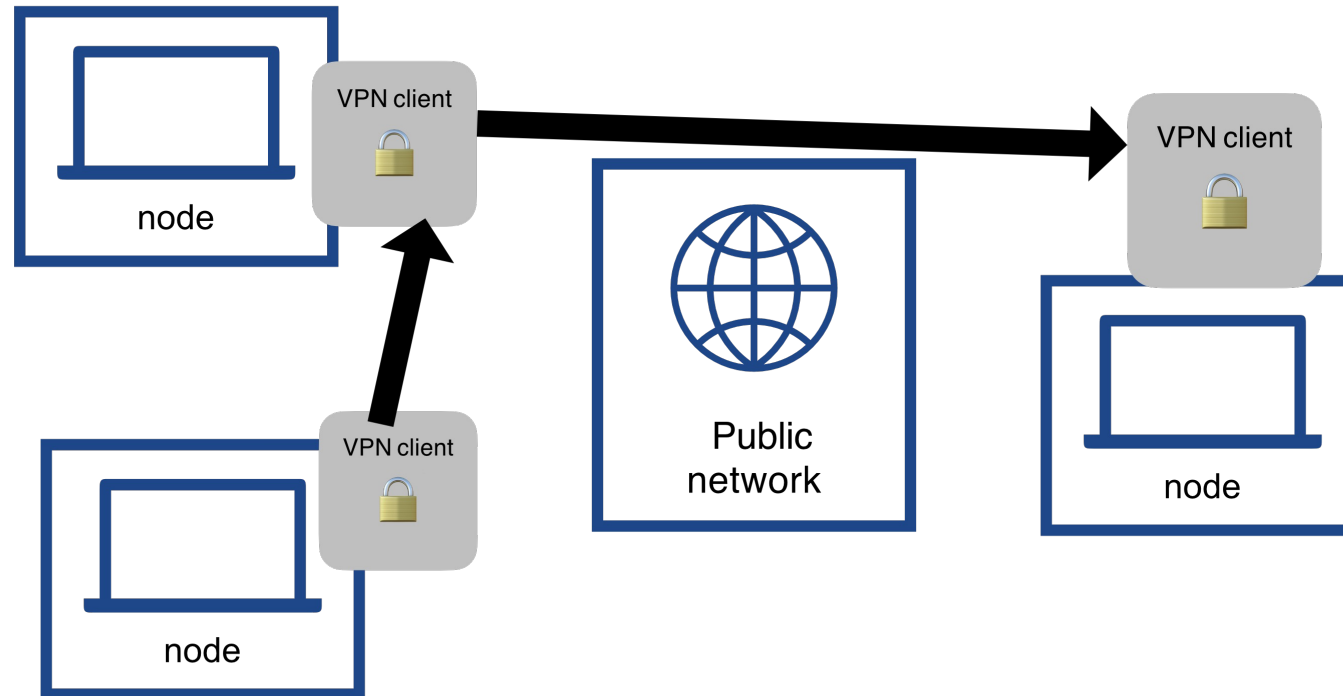
4. Product context

4.2. Product architecture



4. Product context

4.2. Product architecture



4. Product context

4.5. Users



- Users of which?!
- Consumers
- IT departments
- Network administrators
- Journalists
- White collar workers



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#46-users>

4. Product context

4.6. Use cases



- Complete solution
- A la carte
- Hardware appliance



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#47-use-cases>

Detour! The Annexes!



Use Cases map to Security Profiles

Security Profiles are collections of controls to mitigate risks, thereby fulfilling Requirements

Security Analysis helps manufacturers figure out which Requirements apply if none of the Use Cases fit



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#annex-c-informative-risk-identification-and-assessment-methodology>

4. Product context

4.6. Use cases



- Complete solution
- A la carte
- Hardware appliance



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#47-use-cases>

5. Requirements



- Sorted by associated essential cybersecurity requirement in the CRA Annex I Part I (2) (a)–(m)
- Each requirement is designed to be clear the threat it is attempting to control for
- Product doesn't fit into an existing Use Case?
 - do a thorough risk assessment
 - identify relevant requirements to mitigate identified risks



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#5-requirements-specifications>

Current draft priorities: Requirements



- Concentrating on ensuring as many threats are mitigated by requirements within the standard
- Manufacturers who notice a gap are writing the requirements that are missing



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#5-requirements-specifications>

Next draft priorities: Use Cases & Clause 4



- Once the requirements are written, we refine the Use Cases
 - We want to cover as many real use cases as possible
 - That requires manufacturers tell us about their Use Cases!
- Once Use Cases are covered, improving the details in Clause 4 should come easier



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#user-content-4-product-context>

Later draft priorities:

Annex: Security Analysis



- Collect requirements into Security Profiles
- Apply Security Profiles to Use Cases
- Make the standard as easy as possible to use



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/blob/main/EN-304-620.md#annex-c-informative-risk-identification-and-assessment-methodology>

THIS DRAFT NEEDS YOU



- Just like open source: more eyes makes a better product possible
- Add your comment! → → → → → → → → → → → → → → → →

Open consultation *right now*, make sure to FOLLOW THE TEMPLATE and PROPOSE AN ALTERNATIVE

Don't include any patented technology



<https://labs.etsi.org/rep/stan4cra/en-304-620-1/-/issues>

Questions?

email a@expertzebra.com

signal aki.rose01





The Standards People

Web browser vertical standard: A work in progress

Daniel Ari Ehrenberg Goldberg

ETSI co-rapporteur, EN 304 617

CRA Standards Unlocked,

Barcelona

26/03/2026

Audience choice

Spanish or Catalan?





Agenda



- What is a web browser
 - What do browsers already do well
 - Untreated risks in web browsers on the market
 - How might the CRA apply to web browsers
-
- Mature draft and feedback on it
 - Next steps plan
 - The shared skeleton from ETSI
 - Current progress

Who am I?



“Daniel Ehrenberg”, a.k.a. @littledan

10+ years in web standards, mostly JavaScript,
(dabbling in HTML, WebAssembly)

Former president of Ecma International

Previously worked at Google, Igalia, Bloomberg

Live here in Catalunya, just a bit further down the coast

Les Roquetes del Garraf (Sant Pere de Ribes)



What is a web browser?



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 pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council

C/2025/8052

Software products with digital elements that enable end users to access, render, and interact with web content and services hosted on servers that are connected to networks such as the Internet. They typically include a browser engine for interpreting and displaying content written in markup language (e.g. HTML), support for web protocols (e.g. HTTP, HTTPS), the ability to execute scripts and manage user inputs as well as storage of temporary or persistent data from websites (cookies).

This category includes but is not limited to standalone applications that fulfil the functions of browsers, embedded browsers intended for integration into another system or application as well as browsers with AI agent integration.

What is a web browser?



- Software which accesses general web content, not just first-party content
- Being built with web technologies does not make something a browser

Your Electron app is probably not a web browser

But a WebView component which can access arbitrary websites is

...if that component is the product itself

Browsers are Important (Class 1)



→ need to conform to a harmonized standard or get a third-party assessment to be put on the EU market

Reasonable, because:

- Trusted base for lots of other software
- If browsers are insecure, everything else you're doing is insecure

What do browsers do well?



All major browsers are open source at their core and use strong security practices, including:

- Frequent updates addressing security issues
- Prompt handling of any discovered or reported vulnerability
- State-of-the-art encryption implementations, used in TLS
- UIs which demonstrate risk, trust context, block some risky actions
- Design of APIs which protect privacy, preserve privilege boundaries
- Sandboxing/multiprocess architecture
- Fuzz testing, conformance testing
- Much, much more...

Untreated risks in browsers on the market



Many web browsers are based on open source upstream browsers, and then not updated over time.

There is a constant stream of CVEs against all web browsers.

If you let users access the web, they will often trust their browser, and do arbitrarily important things in the web browser.

There is no low-risk use case for a web browser

You need to update against upstream regularly (at least monthly)

How the CRA might apply to web browsers



Annex 1 part 1 (1) (e)

“protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;”

- TLS
- How to define that?

How the CRA might apply to web browsers



Annex 1 part 1 (1) (g)

“process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);”

- Same-Origin Policy
- Only give personally identifying information with user consent
- Third-party cookies?

How the CRA might apply to web browsers



Annex 1 part 1 (1) (k)

“be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;”

- Sandboxing
- Multiprocess architecture
- But how do we make sure to be open to future innovations?

How the CRA might apply to web browsers



Annex 1 part 1 (1) (m)

“provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.”

- Product-wide reset button
- Clearing storage per-site?

Development of the standard



The “Mature Draft”

From December 23, 2025

433 pages

Written entirely by co-rapporteur

Detailed requirements and assessments

Capability/conditions framework

Draft ETSI EN 304 617 V0.1.0 (2025-12)



**Cyber Security (CYBER);
CRA;**

Cybersecurity requirements for Browsers

Exercising one of the Principles of international standardization - Openness - and taking it to a different level, ETSI is piloting informal public consultations of the vertical standards in support of the Cyber Resilience Act at a much earlier stage than it is usual in the standardization world. In this context, please keep in mind that the standard draft herein is an INTERIM DRAFT, which expectably will be subject to substantial changes before its target publication date in the second semester of 2026.

Disclaimer

This **INTERIM DRAFT** document is provided for information and is for future development work within the ETSI Technical Committee CYBER EUSR Working Group (CYBER-EUSR) only. ETSI and its Members accept no liability for any further use/implementation of this Specification. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at <http://www.etsi.org/standards-search>

Commenting guidelines

Your comments to improve this early draft are very welcomed. To ensure the effectiveness of your contribution, please make sure to include the following elements in your comment:

1. Clear identification of the section of the draft your comment is referring to.
2. Objective proposal to delete content, add content or substitute content.
3. Concrete contribution (exact content you suggest including in the draft as an addition to, or in substitution of, existing content).
4. Disposition to identify the need for a change to the standard text. We should be able to identify the need for a change to the standard text.

Feedback on the mature draft



Several parties posted detailed reviews

- HAS assessment
- Marshall Vale and Andrew Whalley, Google
- Sebastian Ledru and Giancarlo Pascutto Mozilla
- Giovanni Corti of Fondazione Bruno Kessler, Simone Onofri of W3C
- Yngve of Vivaldi

All pointed to the need for a new approach

Next steps plan



- Common web security model, rather than defining multiple profiles
- Requirements to be more high-level, product-driven, from risk assessment
- Draft collaboratively among several contributors, with code review
- Follow the common cross-vertical structure by starting from the shared skeleton

The shared skeleton

- Emphasizes the top-down, product-driven approach:
- Requirements come from CRA paragraphs, rather than functional components

5. Technical requirements for the Products

This is the normative clause of the standard, defining the technical requirements to implement the Essential Security Requirements of the CRA regulation. The text of the regulation shall never be copied or interpreted in the standard.

The requirements shall be indexed, to facilitate their referencing, preferably using a common indexing structure throughout all standards.

Proposed structure for indexing the requirements:

REQ – PP – ESR – NNN

REQ: Used to identify requirement in the text

PP: Product short name added only if relevant when the product category may be divided in sub categories

ESR: Proposed abbreviations referring to the different essential requirements of the regulation

■ **NNN – Incremental and unique number**

ETSI

{Draft Skeleton} ETSI EN 304 6DD V0.0.21 (2026-02)

14

[Part of element] or [Release #]

It is strongly recommended to follow the sequence of the CRA Annex I requirements when defining the subclauses in Clause 5. However, where this structure would result in unnecessary duplication/overlap, subclauses and requirements may be organized in a more suitable way, provided that clear traceability to the relevant CRA Annex I requirements is maintained.

5.1 Introduction – Applicability of the requirements

If there is a matrix mapping the use cases to the technical requirements of the standard, it should be inserted in this clause. Alternatively, there can be such a matrix/mapping in each subclause below.

5.2 No known exploitable vulnerabilities

Proposed ESR code: KEV

This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (a).

5.3 Secure by design

Proposed ESR code SBD

This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (b).

5.4 Secure Updates

Proposed ESR code: SU

This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (c).

■ **5.5 Authentication and access control**

Proposed ESR code: AC

Current progress



Use cases:

- Consumer standalone web browsers
 - "Enterprise" web browsers which may be used in critical infrastructure contexts
 - Embedded browser-like tabs with no access from the embedding application into the web content.
-
- Annex O: things not handled by this specification
 - Browsers with AI agent integration: too new and powerful for us to define risks and mitigations
 - WebViews deeply integrated with host app: significant risks if used with 3rd party content

Current progress



- Annex V: Advice for derivative browsers, downstream of open source
 - **Rebase from upstream frequently**
 - Otherwise you are certainly shipping known exploitable vulnerabilities

Open Requirements for TLS tls-reqs into main_publish

Overview 8 Commits 2 Pipelines 1 Changes 1

6 open threads ^ v ⋮ Add a to-do item



Andrew Whalley @whalleya started a thread on the diff 3 hours ago

▼ Collapse replies

EN_CRA_Vertical_Harmonised_Standard_Skeleton_draft.md

371	384	
372	385	This clause addresses the requirements in the CRA <code>\[i.1\](#_ref_i.1)</code> Annex 1 Part 1 (2) (b).
373	386	
	387	+ REQ-TLS-SBD-1 : The web browser shall be configured by default to reject TLS protocol versions, ciphers and configurations which present high-risk known exploitable vulnerabilities.
	388	+
	389	+ Editor's note: Consider whether "high-risk known exploitable vulnerabilities" is an appropriate phrase, and whether this requirement should say "reject or warn" instead. See also REQ-TLS-CON-3.



Andrew Whalley @whalleya 3 hours ago

✓ 😊 ⋮

"at high (imminent?) risk of exploitation" perhaps? Back in the SHA1 deprecation days we'd want folks to move off known-weak algorithms before there were known practical exploits.

I do like the "configured by default" wording, since a deprecation story usually involves having an enterprise policy to allow use of weak configurations where somebody's taken a positive risk decision for their deployment

0 Assignees Edit
None - assign yourself

0 Reviewers Edit
None - assign yourself

Labels Edit
None

Milestone Edit
None

Time tracking ⌚ +
No estimate or time spent

3 Participants



Getting involved

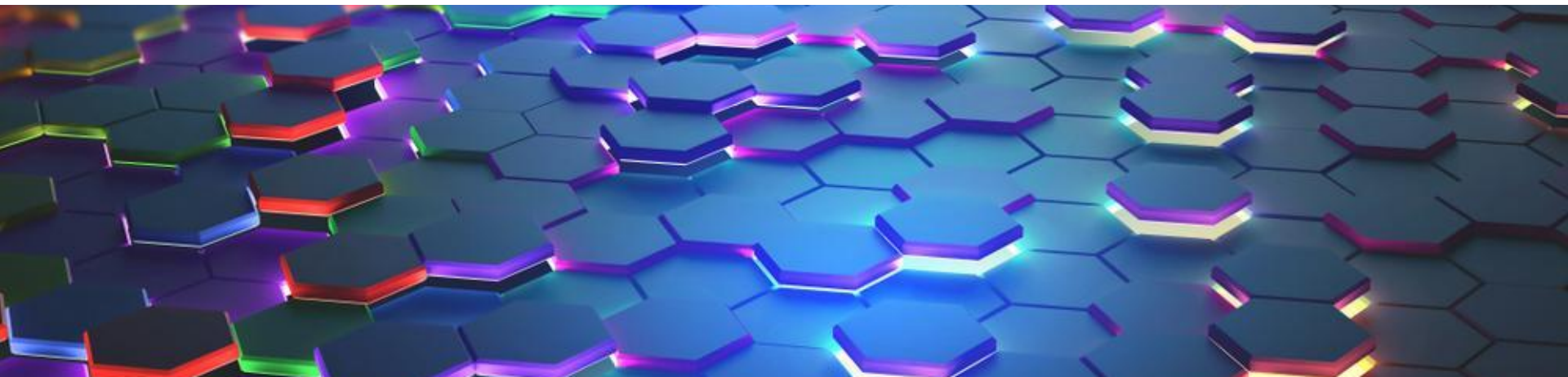


We need your help to move this standard forward!

- Review and leave comments in <https://labs.etsi.org/rep/stan4cra/en-304-617>
- Join ETSI's CYBER EUSR committee
 - Internally, we develop via GitLab – make a PR against our markdown
 - If you're an open-source developer, you may be able to participate via OSI
- Get in touch with me if you're interested!
- dan@littledan.dev

Q/A

Contact me:
dan@littledan.dev





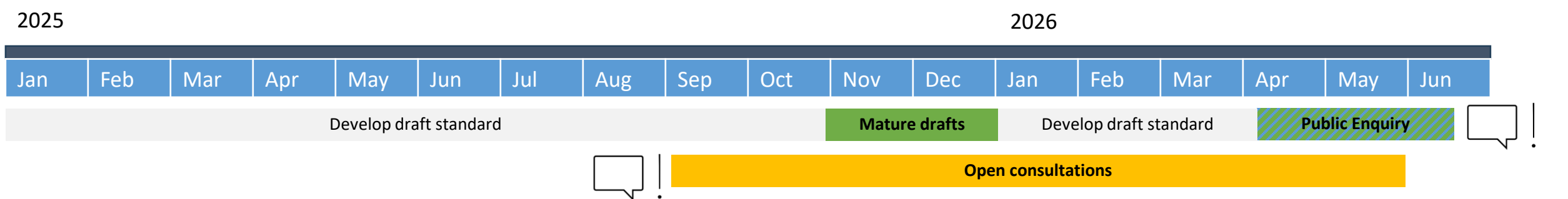
JOIN US!!

Federica BOZZI – STAN4CR Project Leader

federica@nextgcloud.com



High level timeline



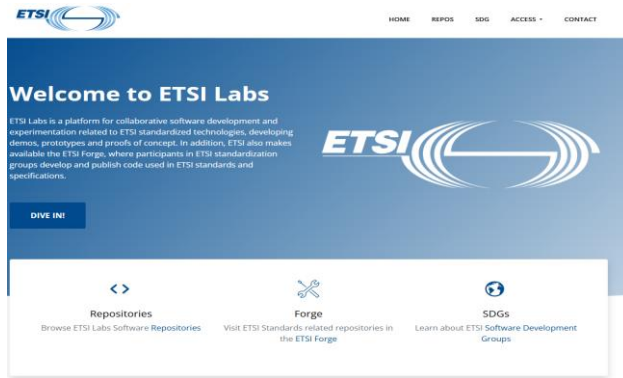
How to contribute:

- Mature drafts:** Technical committee submits advanced and stable versions of the drafts for assessment of the European Commission
- Public Enquiry:** Consolidated final versions subjects to national vote and public commenting via the national members of CEN, Cenelec and ETSI
- Open consultations:** Additional stakeholder involvement, efforts under the project STAN4CR. Open to the public.

Q4 2026

Publication by ESOs

Open consultations on the ETSI standards



How to contribute and send inputs/comments:

- Information website on CRA standards at : www.stan4cra.eu
- ETSI Open area: <https://docbox.etsi.org/CYBER/EUSR/Open>
- ETSI Labs: <https://labs.etsi.org/rep/stan4cra/>



ETSI Open Area



docbox.etsi.org / **CYBER** / **CYBER** / Open

 sort by name/desc	sort by date/desc	sort by size/desc
<input type="checkbox"/>  EN-304-617_V0.1.0_2025-12-23_Browsers_Mature-draft.pdf	2025-12-23 19:06	4426,9 KB
<input type="checkbox"/>  EN-304-618_V0.1.0_2025-12-23_Password-managers_Mature-draft.pdf	2025-12-23 16:42	1243,8 KB
<input type="checkbox"/>  EN-304-619_V0.0.12_2025-12-11_Antivirus-Antimalware_Mature-draft.pdf	2025-12-11 7:15	1626,3 KB
<input type="checkbox"/>  EN-304-620_V0.1.0_2025-12-23_Virtual-Private-Networks_Mature-draft.pdf	2025-12-23 17:35	855 KB
<input type="checkbox"/>  EN-304-621_V0.1.2_2025-12-23_Network-Management-Systems_Mature-draft.pdf	2025-12-23 19:06	742,3 KB
<input type="checkbox"/>  EN-304-622_V0.1.0_2025-12-23_Security-Information-Event-Management_Mature-draft.pdf	2025-12-23 17:18	994,3 KB
<input type="checkbox"/>  EN-304-623_V0.0.12_2025-12-19_Boot_Managers_Mature-draft.pdf	2025-12-20 9:20	1109,3 KB
<input type="checkbox"/>  EN-304-624_V0.0.8_2026-01-14_PKI_and_Digital_certificates_issuance_software_Mature-draft.pdf	2026-01-14 18:18	5298,2 KB
<input type="checkbox"/>  EN-304-625_V0.0.13_2025-12-22_Network-Interfaces_Mature-draft.pdf	2025-12-22 10:34	851,5 KB
<input type="checkbox"/>  EN-304-626_V0.1.0_2025-12-23_Operating-Systems_Mature-draft.pdf	2025-12-23 17:26	1026,2 KB
<input type="checkbox"/>  EN-304-627_V0.0.11_2025-11-24_Routers-modems-switches_Mature-draft.pdf	2025-12-02 14:53	1197,9 KB
<input type="checkbox"/>  EN-304-633_V0.2.3_2026-02-05_Connected-toys_Mature-Draft.pdf	2026-02-05 17:00	2089,1 KB
<input type="checkbox"/>  EN-304-635_V0.0.10_2025-12-09_Virtualization-Container_Mature-draft.pdf	2025-12-09 17:18	2584,7 KB
<input type="checkbox"/>  EN-304-636_V0.0.9_2025-12-15_Firewalls_Mature-draft.pdf	2025-12-15 18:31	1090,6 KB
<input type="checkbox"/>  EN_304-631_V0.2.1_2026-02-05_Smart-home-virtual-assistants_Mature-draft.pdf	2026-02-05 18:31	2075,7 KB
<input type="checkbox"/>  EN_304-632_V0.2.1_2026-02-05_Smart-home-security_Mature-draft.pdf	2026-02-05 17:51	2076,4 KB
<input type="checkbox"/>  EN_304-634_V0.2.3_2026-02-05_Personal-wearables_Interim-draft.pdf	2026-02-05 19:16	1855,6 KB
<input type="checkbox"/>  ETSI Commenting Format for Open Consultation_v8.xlsx	2026-02-05 16:06	41,6 KB
<input type="checkbox"/>  ETSI_Commenting_Guidelines_for_Open_Consultation_2026-01-14.pdf	2026-01-14 7:21	67,9 KB
<input type="checkbox"/>  OC1_ETSI_CYBER-EUSR_Comments_Resolutions_Public Version.xlsx	2026-01-15 14:25	58 KB

- 17 draft (ready to read and download)
- Commenting Guidelines
- Commenting Format
- Comments handled on a monthly basis

CRA Standards Unlocked EU Tour

CRA Standards Unlocked - EU Tour Next Steps 2026



-  Barcelona, 26 March
-  Paris, 27 April
-  Stockholm, 4 May
-  Malta, 21 May
-  Bucharest, 24 June
-  Lisbon, 17 September



Co-funded by
the European Union



ECCC
European Cyber Crime Centre





Your unique skills and expertise
are the missing link.

Come and join us!!!

federica@nextgcloud.com

For Compliance read **Security, Trust & Confidence** - Standards Tools and Funding for the CA

Barcelona
26th March 2026

www.cyberstand.eu



EC-Funded Projects Supporting CRA Implementation

Certification, Tools & Alignment with EU Legislation



Simplifying CRA compliance with automated tools for cybersecurity certification and assessments.



Enhancing cybersecurity compliance and certification across the EU and aligning with major EU regulations.



Tools, Methodologies and Training for Compliance



Open-source tools to facilitate and automate compliance with the CRA.



CRA compliance tools and services automation and capacity building.



Open-source toolkit to automate the compliance process for Free and Open Source Software (FOSS).



AI-powered platform built to guide product companies through the full CRA conformity journey.



Compliance tools for SMEs, documentation automation, and open-source accessibility promotion.



Strengthening Europe's cybersecurity through AI-driven defence, collaborative intelligence, and real-world validation.



Methodologies and tools to facilitate the documenting process to ensure compliance with the CRA.



Empowering SMEs with open-source tools for compliance with the CRA for PDES.



Funding SME Compliance



Open calls and resources for SMEs to comply to the CRA



Funding & Support for Standardisation



Funding contributions to develop standards for the CRA.





Chair - Patricia Shields, CyberCertLabs (Spanish)

Juan Rico, Eclipse Foundation (Spanish)

Héctor Laiz Ibanez, LSEC (Spanish)

Carlos Eduardo Rizzo e Silva, 28Digital

Emil Simion, SAFETECH (English)

James Philpott, Digital SME Alliance

Eleni Seralidou, Trustilio

Thank you!

www.cyberstand.eu



CRA-AI

Ayudando a las PYME a crear productos seguros



Attestra es una plataforma de seguridad de productos impulsada por IA que apoya a los fabricantes en el proceso del CRA para obtener el marcado CE y crear productos seguros.

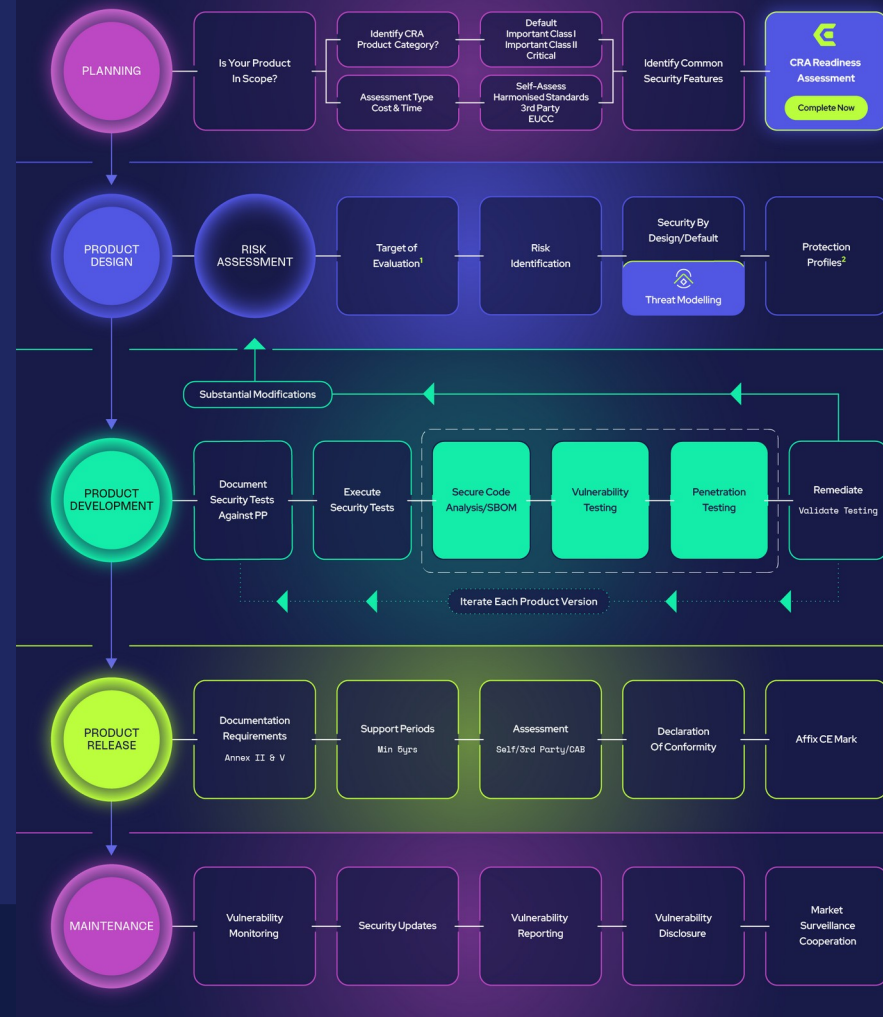
Recorrido del cliente CRA

El CRA desglosado paso a paso en relación con un ciclo de vida típico de desarrollo de productos.

Estas son las nuevas actividades que la mayoría de las PYME deberán implementar para obtener el marcado CE.

¡Es de gran importancia poner en marcha el proceso ahora!

Nuestro consejo es: ¡no espere, comience a planificar ahora!



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



CRA - AI
CYBER RESILIENCE ACT
ARTIFICIAL INTELLIGENCE

Attestra

Productos seguros. Más rápido.

HITOS REGULATORIOS CLAVE

-  **11 Sep 2026** Comienza la notificación de vulnerabilidades
-  **11 Jun 2027** Se requiere preparación de los OEC
-  **11 Dec 2027** Se aplica el CRA

Q1 2026

SEPT '26 LISTO

Módulo 1: Notificación de vulnerabilidades e incidentes

Cumpla con todas sus obligaciones de Septiembre de 2026: gestione la divulgación de vulnerabilidades, el triaje y la notificación desde el primer día.

Q3 2026

Módulo 2: Evaluación de riesgos

Importe su SBOM, construya un modelo de su producto, realice evaluaciones de riesgos basadas en amenazas y documente las decisiones de seguridad por diseño.

Q4 2026

Módulo 3: Pruebas de producto

Cree conjuntos de pruebas, vincúlelos a objetivos de seguridad, recopile evidencia y genere informes de pruebas. Integración API con pruebas de vulnerabilidades.

Q1 2027

Módulo 4: Documentación y certificación

Genere la documentación técnica requerida para la conformidad, prepare su Declaración y Evaluaciones de Conformidad. Integración con OEC..

Q1 2027

Módulo 5: Mantenimiento del producto

Gestione el ciclo de vida continuo: realice seguimiento de correcciones, actualice la documentación y vuelva a las evaluaciones a medida que los productos evolucionen.

Continuo

Attestra Academy

Cursos de formación para adquirir conocimientos internos y aplicar los requisitos del CRA con confianza.

Comience Ahora



Evaluación de preparación para el CRA



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Únase al programa de primeros usuarios de CRA-AI



- Obtenga acceso a talleres prácticos gratuitos específicos para fabricantes de productos
- Obtenga acceso anticipado a Attestra, la plataforma de seguridad de productos CRA impulsada por IA
- Proporcione comentarios sobre el producto para ayudar a informar el diseño
- Obtenga ofertas anticipadas y descuentos en formación



El proyecto financiado en el marco del Acuerdo de Subvención N.º 101190243 cuenta con el apoyo del Centro Europeo de Competencia en Ciberseguridad



Co-funded by
the European Union



OCCTET

**Técnicas Exhaustivas y Herramientas Esenciales
para el Cumplimiento del Código Abierto.**



Juan Rico - Senior Manager - Eclipse Foundation
26 -03-2026

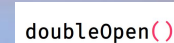


Co-funded by
the European Union



OCCTET en 1 vistazo

Misión: Democratizar la ciberseguridad y el cumplimiento mediante herramientas de código abierto (OSS).



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE


OCCTET project has received funding from the Digital Europe Programme (DIGITAL), under grant agreement number: 101190474. The content does not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union



Objetivos alineados a las realidades de las PYMES

Definir y dar soporte con procedimientos aplicables a las obligaciones de cumplimiento

- Entender los requerimientos de la CRA.
- Aplica a mi producto?
- Cuáles son mis obligaciones?
- Cómo puedo cumplir de forma efectiva?

Automatiza la evaluación y el reporte con herramientas de código abierto

- Descubrimiento: SBOMs
- Datos de referencia
- Triage, evaluación de la postura de seguridad y corrección de vulnerabilidades.
- Reportes: SBOM, VEX, Attestations.



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union



La herramienta de autoevaluación de la CRA de OCCTET

Aplicación y Rol ¿Estoy expuesto a la CRA?

Identificación del Rol: Determina si actúas como fabricante, importador o distribuidor según el marco legal de la UE.

Análisis del Alcance: Filtra si tu producto digital está cubierto por la CRA o si ya está regulado por normativas específicas (médica, automoción o aviación).

Exenciones Clarificadas: Evalúa si tu actividad se clasifica como software de código abierto no comercial para definir si existen obligaciones legales.

Clasificación y Ruta de Conformidad: ¿Qué nivel de control necesito?

Categorización de Riesgo: Clasifica el producto según los criterios de la CRA (Producto por defecto, Importante Clase I/II o Crítico).

Determinación de la Evaluación: Define si el producto permite una autoevaluación interna o si requiere obligatoriamente una auditoría de terceros.

Traducción Jurídica: Convierte la lógica compleja de los Anexos III y IV en una hoja de ruta clara sobre los pasos técnicos y legales a seguir.

Preparación y Madurez: ¿Cómo de preparado estoy?

Evaluación de Requisitos Esenciales: Desglosa el Anexo I en áreas clave: diseño seguro, gestión de vulnerabilidades y actualizaciones de software.

Perfil de Madurez: Clasifica el estado actual de la empresa (Básico, Intermedio o Avanzado) para identificar brechas de seguridad críticas.

Plan de Acción: Transforma los requisitos legales en tareas accionables, permitiendo pasar del diagnóstico a la implementación en solo 15 minutos.



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



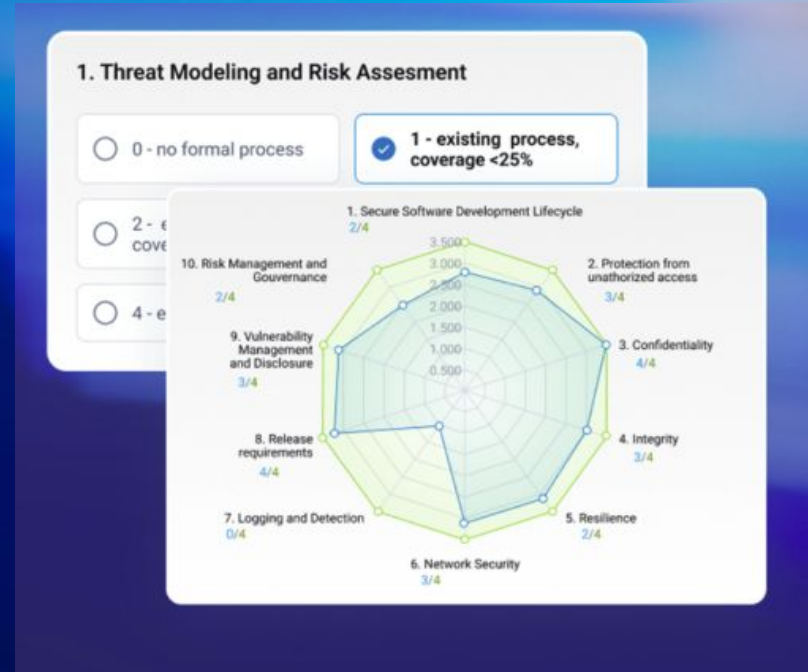
Co-funded by
the European Union



La herramienta de autoevaluación de la CRA de OCCTET

Acceded a ella aquí:

<http://cra.occtet.eu>





Toolkit para automatizar el cumplimiento

1

Input

PYMES y desarrolladores
Suben sus proyectos y sus componentes
FOSS

2

Eclipse Apoapsis

Plataforma de seguridad y cumplimiento
automatizada

3

OSS Review Toolkit (ORT)

Análisis automático de los componentes
open source

4

OCCTET Tool

Lista de cumplimiento, herramienta de
evaluación de la conformidad, herramienta
de reporte

5

Salida

Obtención del reporte final con grado de
preparación para cumplir con la CRA



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union



OCCTET y ORC

1. ORC: Definiendo las Reglas del Juego (Policy)

El grupo de trabajo **ORC**, impulsado por la **Fundación Eclipse**, actúa como la voz del ecosistema ante las instituciones europeas. Su labor de *policy* asegura que las regulaciones no asfixien la innovación abierta. Al colaborar estrechamente con la Comisión Europea, el ORC traduce las necesidades de las comunidades de software en marcos normativos sostenibles, garantizando que el "Open Source" sea un motor de seguridad y no una víctima de la burocracia.

2. OCCTET: Las Herramientas para la Acción (Tech)

Donde termina la política, empieza la acción. **OCCTET.eu** es el brazo ejecutor que convierte esos acuerdos marcos en realidad técnica. Mientras el ORC negocia *cómo* debe cumplirse la ley, OCCTET desarrolla el **kit de herramientas** (como los cuestionarios de aplicabilidad y los generadores de SBOM) que permiten a las PYMES y desarrolladores ejecutar ese cumplimiento en menos de 15 minutos.

3. Una Alianza Estratégica

Esta relación crea un ciclo de retroalimentación único:

- **De la Ley a la Práctica:** El ORC analiza la legislación y OCCTET la traduce en herramientas automatizadas.
- **De la Práctica a la Ley:** El *feedback* técnico recopilado por OCCTET sobre las dificultades de las PYMES ayuda al ORC a informar a los legisladores sobre qué funciona y qué debe ajustarse en futuras normativas.



Open
Regulatory
Compliance



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union



Contactanos!



[occtet.eu](https://www.occtet.eu)



www.occtet.eu



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union

OCCTET project has received funding from the Digital Europe Programme (DIGITAL), under grant agreement number: 101190474. The content does not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union

CRA COMPLIANCE TOOLING

- **CRACY TOOLS TO SUPPORT CRA COMPLIANCE**

Hector Laiz Ibanez – Leaders In Security – CRACY coordinator

March 26th 2026

WELCOME

CRACY IS ABOUT THE CYBER RESILIENCE ACT MADE EASY

CRACY IS A GROUP OF 12 LEADING EUROPEAN CYBERSECURITY EXPERTS, DEDICATED TO HELPING SMES IMPLEMENT THE CRA



CRACY – CRA MADE EASY



- SECURITY tools: sase.cra-cy.eu, test, repo
- White Papers & Guidance cra-cy.eu
- COMPLIANCE & SBOM tools: H1/2026
- Compliance Support: H1/2026
- COMPLIANCE Tools: H2/2026
- Checklists, Guidance: risk management, controls, tooling
- Use cases: high, class 1, class 2 – general products
- Guidance, relation with NCA's, DABs
- Supporting SME manufacturers to become compliant
- Continuous CRA developments assessment

PARTNERS



TIMELEX



resillion



IDLab
INTERNET & DATA LAB



TOREON
Business driven cyber consulting



EXPECTED CRACY OUTCOMES

- CRA compliance tools
- European SME's PDEs CRA compliant
- continuous awareness raising activities to targeted stakeholders
- improvement of security and resilience of Operators of Essential Services and Critical Infrastructures, and of the Digital Supply Chains

CRACY-platform - The ecosystem for cyber resilience and compliance



CORE SOLUTIONS

- SECURE BY CRACY

- CRACY SASE
- CRACY SCA – INFRAMAPPER
- CRACY REPO
- Essential Requirements
- Risk & Vulnerability Assessments
- Cybersecurity Controls for PDEs

- COMPLIANCE WITH CRACY

- Checklists and self-assessment tools for security requirements
- Software for testing and vulnerability analysis
- Tools for managing Software Bills of Materials (SBOMs)
- Guidance for compliance documentation and self-attestation



CRACY SASE – Network Protection for PDEs

- Find the resources to connect PDE's to the platform for supported OS's Windows, IOS, Linux
- See at a glance the status of connected PDE's
- Users: manage the PDE's
- Groups: granular access controls
- Domains: conform to to be able to become a user

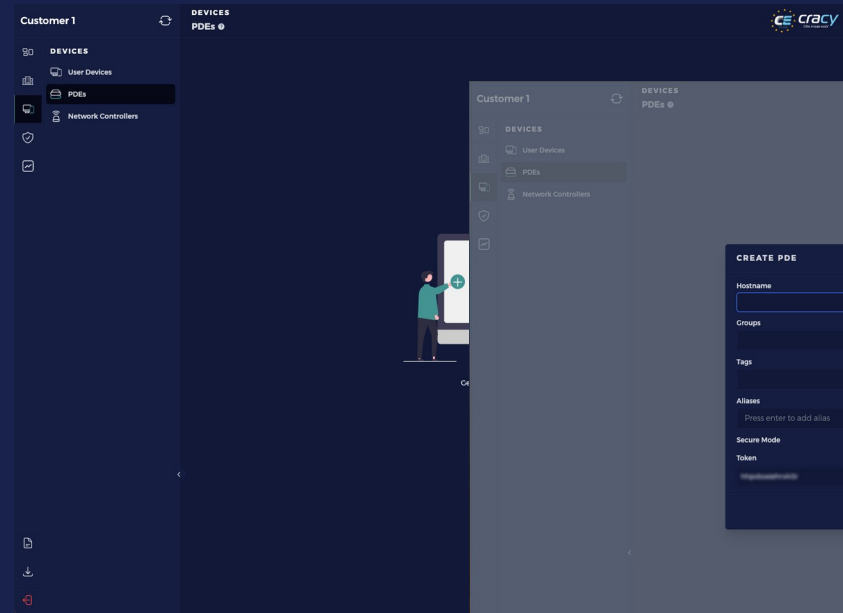
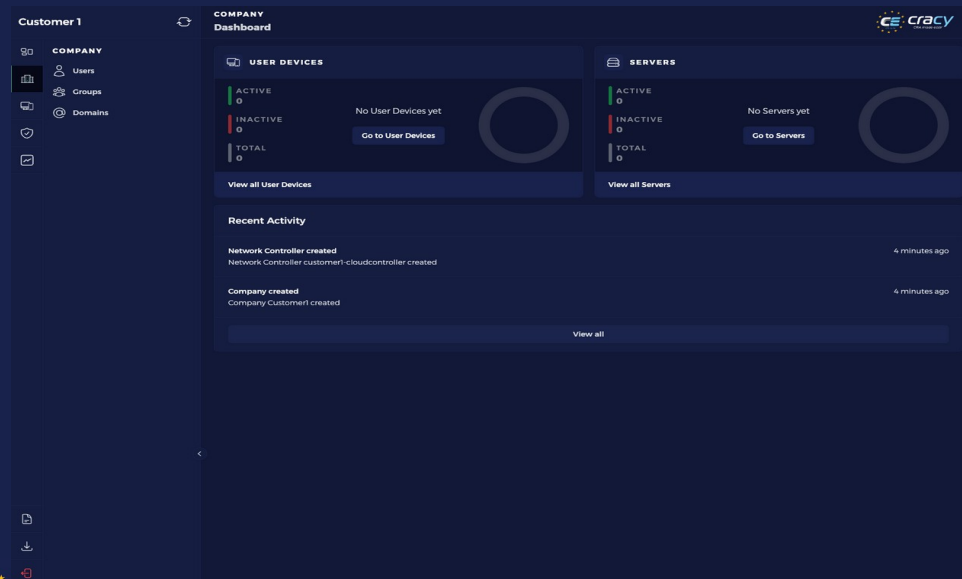
Available: <https://sase.cra-cy.eu/>

Welcome to the
CRACY SASE Platform


Sign in to your account

Sign in with Email

Downloads



CREATE PDE

Hostname

Groups

Tags

Aliases
Press enter to add alias

Secure Mode ☐

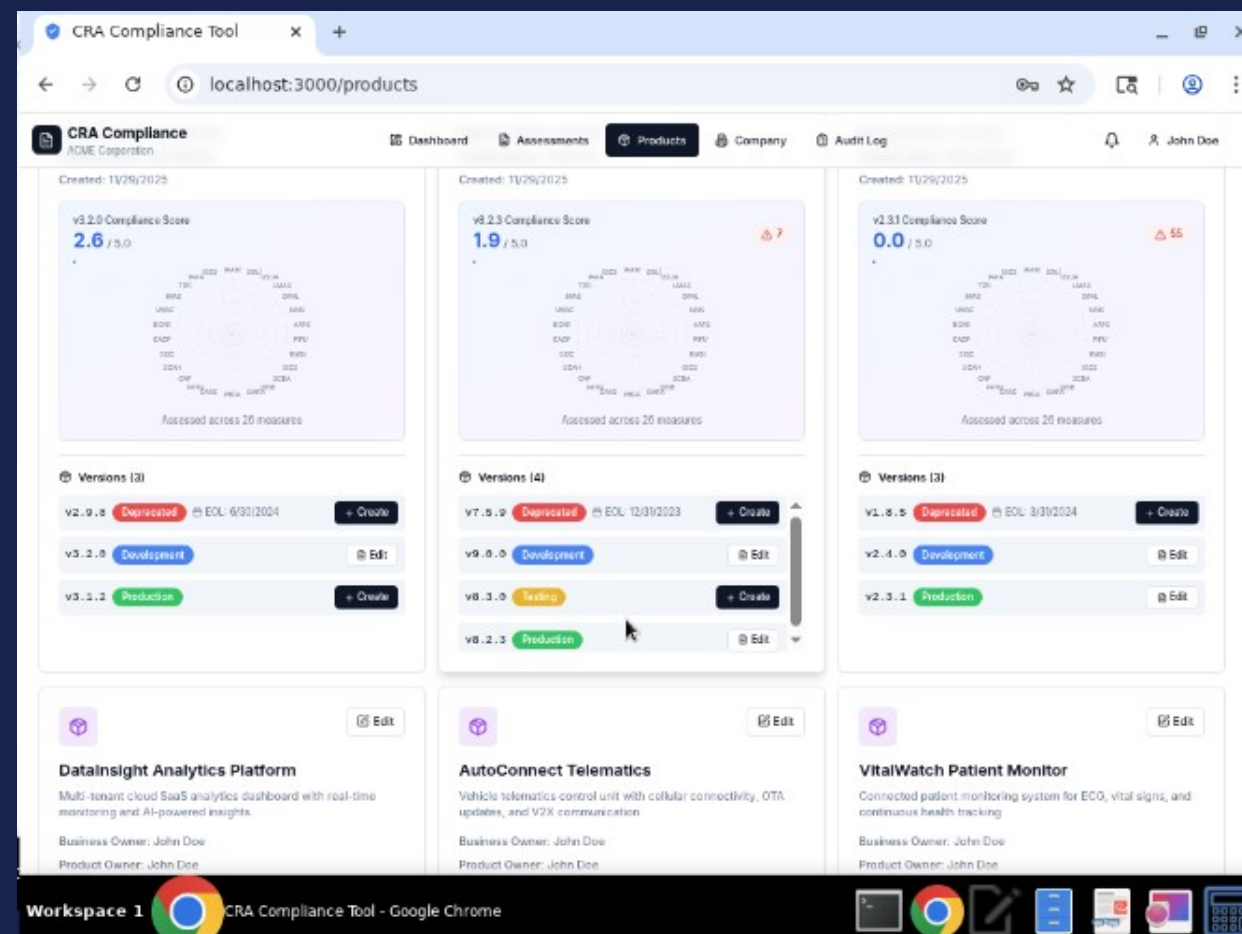
Token

Cancel Create PDE

CRACY REPO – Tooling Integration Platform

Prototype Available

- Register companies and products
- Register and introduce risk assessments
- Register and introduce security measures
- Integrate references to existing security solutions
- Ensure continued updating of PDE security measures
- Integrate CRACY Tools
- Integrate CRA (non CRACY) Tools



CRACY REPO – Tooling Integration Platform

Prototype Available

The screenshot displays the CRA Compliance Tool interface. The top navigation bar includes 'Dashboard', 'Assessments', 'Products', 'Company', and 'Audit Log'. The main content area shows a survey titled 'Industrial/OT Embedded System - Q1' with a domain-specific guidance section. Below this, there are four questions related to identity and access management, each with a 'Critical' status indicator.

Industrial/OT Embedded System - Q1
Domain-specific guidance for this question

Intended Outcome:
Verify that Strong auth for privileged/admin is effectively implemented in the Industrial/OT embedded environment.

Domain Example:
Check for: Role-Based Access Control (RBAC) is enforced. Operators, engineers, and admins have different permissions. Passwords are unique per user.

Score Guidance:
Score 0: Default passwords (e.g., 'admin/admin') are used across the factory floor. Attackers can easily gain control of SCADA systems.
Score 3: Role-Based Access Control (RBAC) is enforced. Operators, engineers, and admins have different permissions.

1. Identity and Access
0 / 12 questions answered

Q1: Strong auth for privileged/admin Critical
Strong authentication (prefer MFA) for all admin/privileged functions; TLS enforced.

Q2: Secure-by-default onboarding Critical
No default/shared credentials; unique initial secrets changed at first use or passwordless.

Q3: Least privilege, RBAC, JIT/JEA, reviews Critical
RBAC enforced, least privilege; JIT/JEA for high-risk; periodic access reviews.

Q4: Privileged Access Management (PAM) Critical
PAM for privileged actions, session recording where lawful, controlled break-glass.

The screenshot displays the CRA Compliance Tool interface. The top navigation bar includes 'Dashboard', 'Assessments', 'Products', 'Company', and 'Audit Log'. The main content area shows the 'Company Profile' section, which includes 'Company Information' and 'Invite Team Members'. Below this, there is a 'Team Members' section. The bottom section shows the 'Audit Log' with a table of system activities and changes.

Company Profile
Manage your organization's information and team members

Company Information Edit
Company Name: ACME Corporation
Description: Technology company focused on cybersecurity compliance

Invite Team Members New Invitation
Send invitations to join your organization
No pending invitations

Team Members View
Users in your organization
John Doe (john@doe.com) Admin

Audit Log
Track all system activities and changes

TIMESTAMP	USER	ACTION	ENTITY	CHANGES
11/30/2025, 4:32:02 PM	John Doe	UPDATE	Survey	["selected_domain_id":"Consumer_wearable_health"]
11/29/2025, 9:38:21 PM	John Doe	CREATE	Survey	["name":"test","product_id":"cmik2d00f5ocigooso5H"]
11/29/2025, 7:55:57 PM	John Doe	UPDATE	Survey	["selected_domain_id":"Industrial_embedded"]
11/29/2025, 7:55:04 PM	John Doe	CREATE	Survey	["name":"Datainsight Analytics Platform v3.4 Assessment","product_id":...

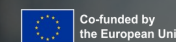
GET IN TOUCH

Do you (PDE manufacturers) want to

- Identify risks and essential security requirements
- Secure your PDEs
- Handle vulnerabilities and dependencies
- Navigate compliance requirements
- **Get guidance throughout the CRA compliance process**

Call us +32 16 79 85 85

Mail info@cra-cv.eu



CURIMUM Project Presentation

26th March 2026

Carlos Eduardo Rizzo e Silva
28DIGITAL



Co-funded by the
European Union



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

The project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre ('granting authority'), under the powers delegated by the European Commission ('European Commission'), under the Grant Agreement No. 101190372. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC. Neither the European Union nor the granting authority can be held responsible for them.

Project Overview

Project acronym: **CURIMUM**
Project number: **101190372**
Project name: **Cra sUppoRt continuUM**
Call: **DIGITAL-ECCC-2024-DEPLOY-CYBER-06**

Project website: **<https://curium-project.eu>**

Total budget: **3,006,764.00 €**
EU contribution: **2,488,140.55 €**

Project duration: **18 months**

Project start: **January 1st 2025**
Project end date: **June 30th 2026 (extension in progress - September 30th 2026)**



Partners



A consortium of nine partners from seven EU Member States, including SMEs, a Competence Center, and National Authorities, will contribute their expertise to strengthen Europe's cybersecurity landscape.

Objectives

- Developing an innovative **Compliance Continuum** to automate CRA compliance.
- Driving widespread adoption with modular, cost-efficient, and **open-source solutions** tailored to industry needs.
- Stimulating **knowledge and capacity building** to support CRA implementation.
- Utilizing an **agile validation process** with continuous feedback loops.
- Fostering **long-term sustainability** by actively engaging industry stakeholders and policymakers in tool development and training.





DPMA

Digital Product Maturity Assessment

Offers a structured **risk mitigation framework** based on product maturity, helping manufacturers implement effective security measures.



PSTVA

Penetration Self-Testing and Vulnerability Assessment

Equips users with **tools** for **vulnerability assessment, code review**, and **penetration testing**, reinforcing compliance efforts.



CyReA

Cyber Resilience Assessment

Identifies whether a product with digital elements **falls within the scope of the CRA** and determines the required conformity assessment process.



DPRA

Digital Product Risk management

Supports manufacturers in **assessing cybersecurity risks** across the product lifecycle to proactively minimize security threats.

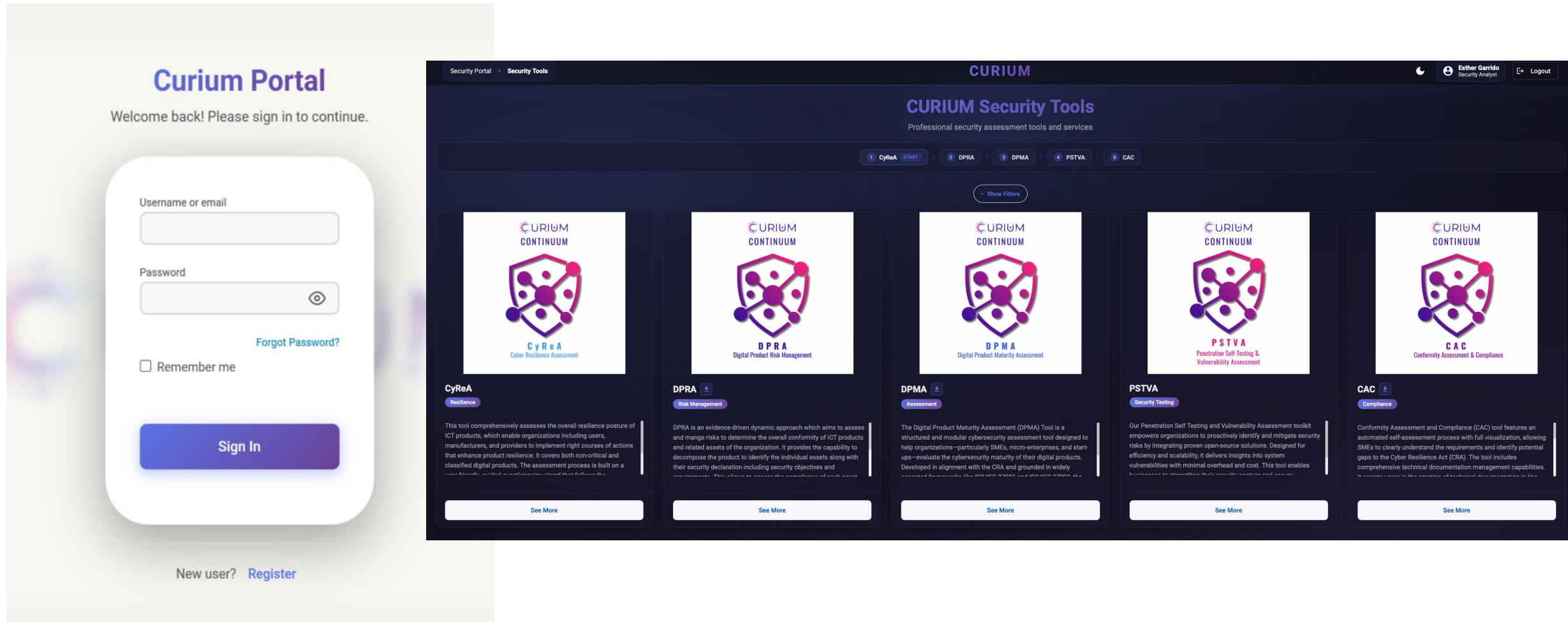


CAC

Conformity Assessment and Compliance

Provides a guided approach to **technical documentation** and **self-gap analysis**, ensuring alignment with CRA requirements.

User Interface of the CURIMUM continuum



Validation rounds

- CURIMUM tools have been validated at different events with SMEs
 - Techritory - Riga Oct25
 - Cyprus – Dec25
 - Athens – March26
 - Zagreb – April26 (upcoming)
- Want to test the tools yourself?

Book an online demo session

<https://curium-project.eu/contact/>



Let's keep in touch!



curium-project



@Curium_Project



curium-project.eu

Subscribe to our newsletter:



Thank you!



**A Certification approach for dynamic, agile and reUSable assessment fOr
composite systems of ICT proDucts, servicEs, and processeS**

CUSTODES Project Presentation

Carlos Eduardo Rizzo e Silva (28DIGITAL)

26th March 2026



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101120684.

- Cybersecurity **certification is a complex process**, posing a variety of challenges to the different interested parties.
- Cybersecurity certification as introduced by the **EU Cybersecurity Act** (EUCSA) will play a crucial role in increasing the **trust and security** of ICT Products, ICT Services and ICT Processes.

CUSTODES has developed a Composite Inspection and Certification (CIC) system: a variety of components to provide trustworthy, cost-effective, agile and portable conformity assessment capabilities, to a variety of interested parties, covering multiple Assurance levels of Composite ICT products or ICT services.

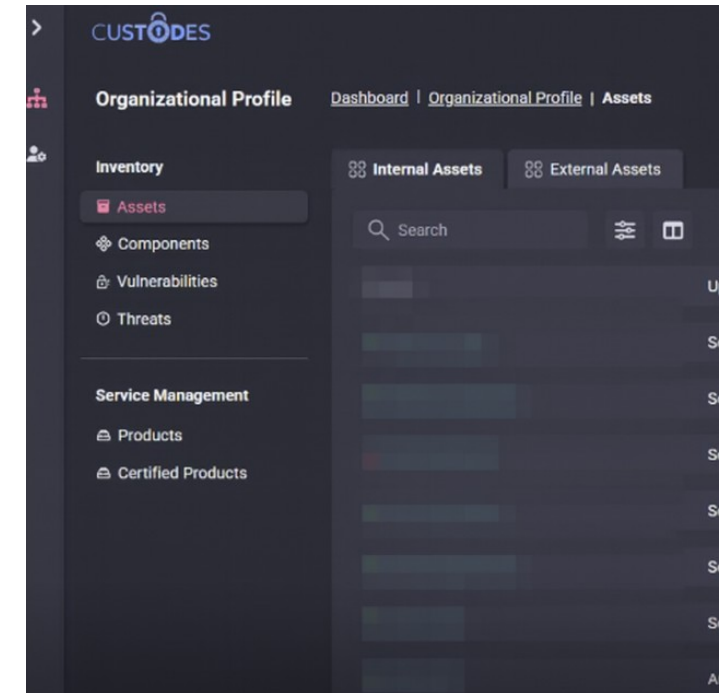




How is CUSTODES helping SMEs and Startups?

As part of its piloting activities, **CUSTODES** gives vendors practical support and tools to make conformity assessment easier and accelerate their cybersecurity certification readiness.

Running
from Apr26
to Sept26



Prepare your company for the future of cybersecurity!
Position yourself as a trusted leader in the digital market!

How can YOU benefit from it?

Sign up for
the initial
presentation
meeting!



20, 21 or 23
April at
13:00

Act as active users of the platform

- Initial presentation meeting
- Glossary and onboarding material
- Register to the platform

Engage in your own product evaluation process

- Personalised scope definition adapted to your availability and resources
- Restricted environment
- Supported by CUSTODES team (platform admin and security experts)

Provide feedback for continuous improvement

- Share practical feedback on usability, process, and results
- Propose enhancements to optimize the platform

Contact Us!



Web Page: <https://custodes-project.eu/>



X: <https://twitter.com/CustodesEu>



LinkedIn: <https://www.linkedin.com/company/100379582>



Facebook: <https://www.facebook.com/profile.php?id=61553693646385>

Subscribe to our
newsletter!





**A Certification approach for dynamic, agile and reUSable assessment fOr
composite systems of ICT proDucts, servicEs, and processeS**

Thank You



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101120684.



TrustBoost: Enabling CRA Compliance through Automated Cybersecurity Certification

Dr. Emil Simion
Head of Security Evaluation Laboratory, Safetech
Innovations



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them



ECCE 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

The project funded under Grant Agreement No. 101158687 is supported by the European Cybersecurity Competence Centre

CRA compliance is complex and fragmented



- Multiple standards and certification schemes across the EU
- High cost and complexity of cybersecurity certification
- Limited resources and expertise, especially for SMEs



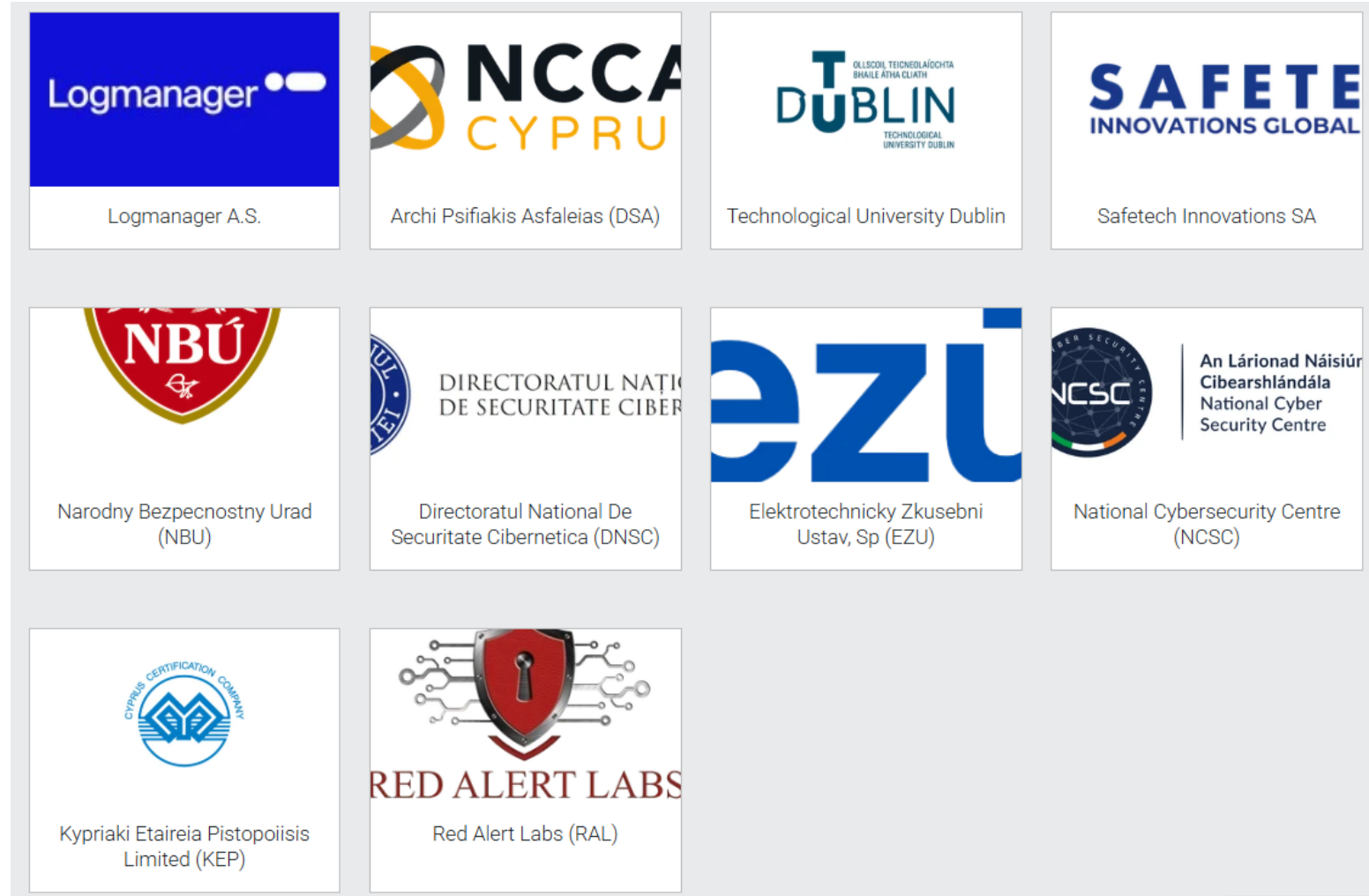
Business impact of non-compliance

- Delayed market access
- Increased certification and operational costs
- Loss of customer trust and reputational risks

Trustboost consortium lead by NSAI



- <https://www.trustboost.eu/>
- Presentation video: <https://www.youtube.com/watch?v=aC6Zfhxt4Sg>



The CyberBoost Platform: TrustBoost's core tool for SMEs



- SaaS platform that manages the full certification lifecycle of digital products – from gap identification to certification status monitoring
- Automated product categorisation aligned with CRA, NIS2, CSA and RED-DA – so SMEs know exactly which obligations apply to them
- Real-time compliance dashboard with ML-powered risk assessment and predictive analytics
- Connects all stakeholders in one place: SME vendors, certification bodies (CABs), national authorities (NCCAs), and ENISA



Safetech: Our Role in TrustBoost

- Romania's ITSEF (IT Security Evaluation Facility) – laboratory performing technical security evaluations of digital products
- Participation in trainings on CRA, CSA, EUCC, Common Criteria – building knowledge capacity across the consortium
- Contributing to CyberBoost platform design – translating evaluation expertise into automated assessment tools
- Participating in pilot certifications – validating the platform with real ICT products under CRA requirements



How TrustBoost works

- Input: Digital product or system
- Process: Automated security & compliance assessment
- Output: Compliance status and certification support



Access and availability

- Training modules available now: CSA/CRA, EUCS, ISO 17025/17065, CC/EUCC – delivered remotely across the consortium
- CyberBoost platform prototype: in development
- Pilot certifications with real ICT products
- How to get involved: visit trustboost.eu or contact your national cybersecurity authority

Use case

- An ICT product manufacturer – TrustBoost consortium partner – pursues EUCC Substantial assurance level certification via CyberBoost
- CyberBoost platform supports the full process: evidence preparation, CAB engagement, and compliance monitoring
- EUCC Substantial certification provides CRA presumption of conformity – no separate CRA assessment needed
- Post-certification: CyberBoost monitors compliance status and manages vulnerability handling continuously



Impact

- Reduced certification costs
- Faster CRA compliance
- Increased trust in digital products
- Stronger European cybersecurity ecosystem



Q&A?

Muchas gracias por la atención
prestada!



adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs



NERO | adva**N**ced cyb**E**rsecurity awa**R**eness ec**O**system for SMEs

CRA Standards Unlocked - EU Tour in Barcelona

26 March 2026

Dr Eleni Seralidou, Project manager at trustilio BV
eleni.seralidou@trustilio.com



Funded by
the European Union



ECCC
European Cyber Crime Centre
European Union Agency for
Cybercrime

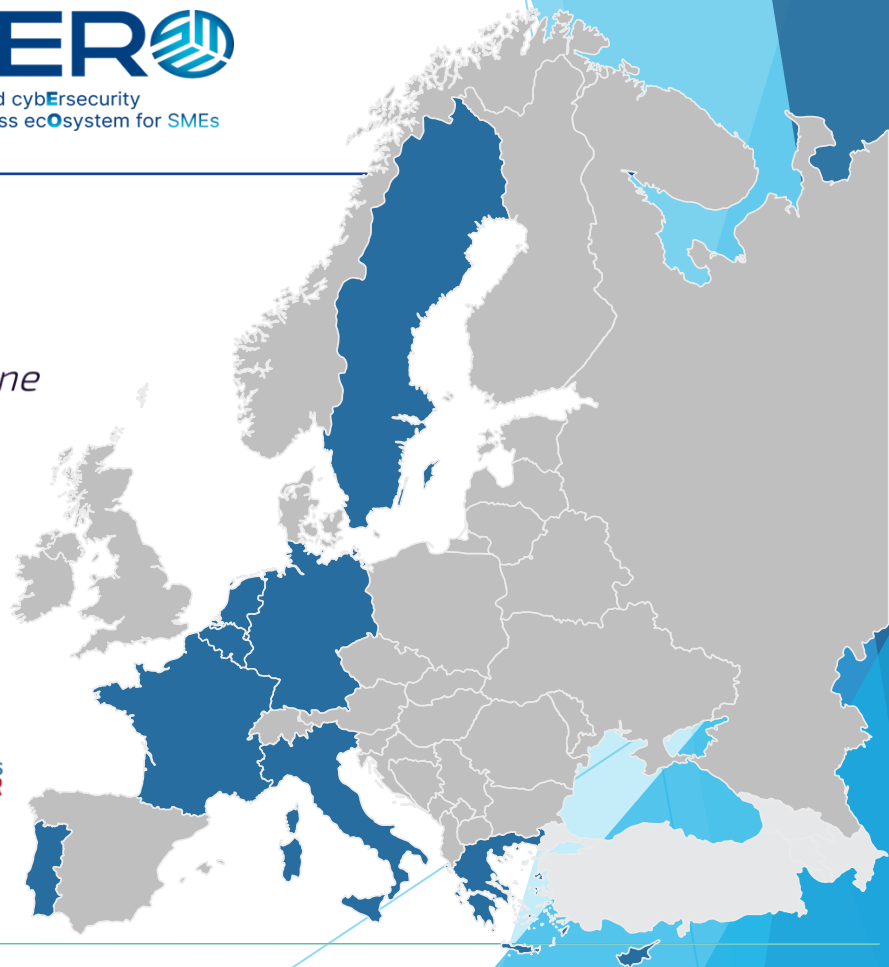
What is NERO?



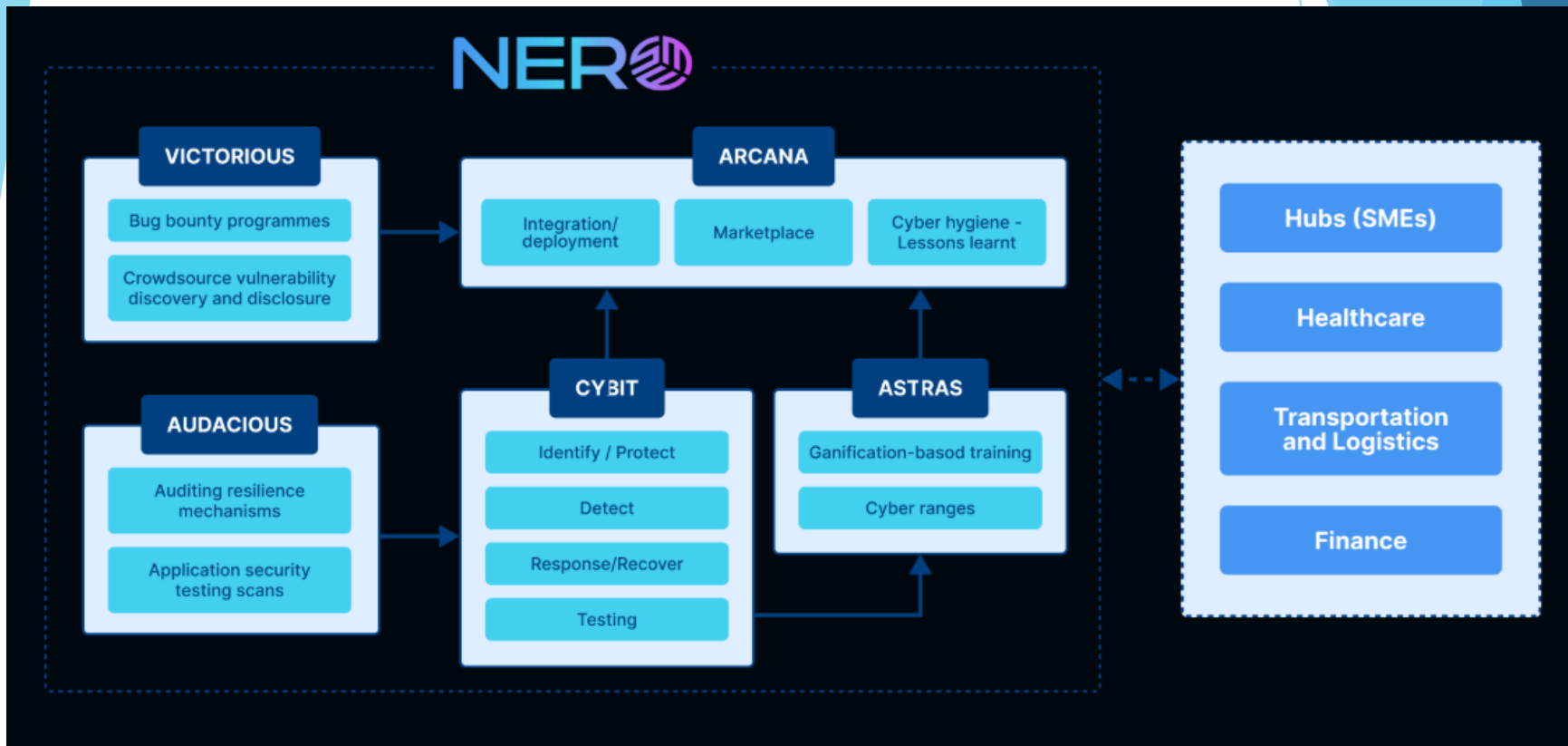
adva**N**ced cyb**E**rsecurity
awa**R**eness ec**O**system for SMEs

- A project focused on **improving cybersecurity for SMEs** by connecting them with innovative solutions and expertise.
- Aims to build a **dynamic ecosystem** to help SMEs **adopt cybersecurity tools** and **enhance resilience**.

Consortium



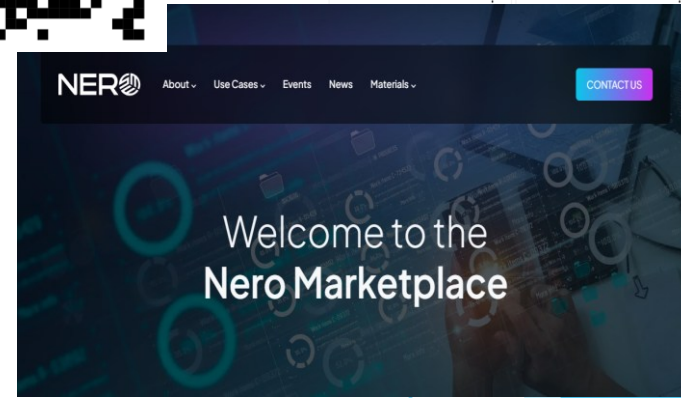
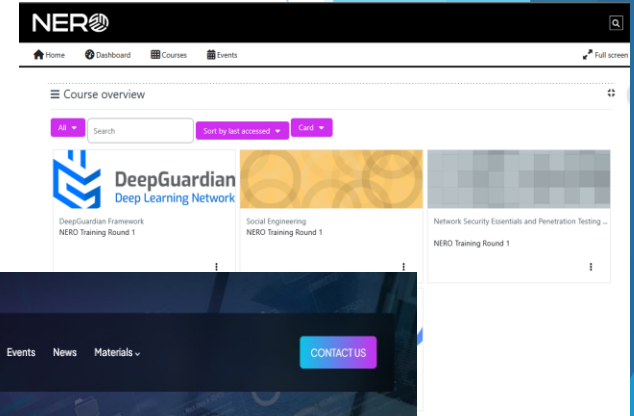
The NERO Ecosystem



The NERO Marketplace & Training Platform

<https://nerocybersecurity.eu>

- ▶ The **NERO marketplace** is a platform for integrating tools.
- ▶ Showcase the types of **cybersecurity solutions and resources** available on the marketplace.
- ▶ **Benefits for SMEs:** access to up-to-date cybersecurity solutions and support.



Demonstrations



UC1: Enhancing Patient Data Security in **Healthcare** through Cybersecurity Tools.



UC2: Strengthening Supply Chain Resilience through Cybersecurity Awareness in the **Transportation/Logistics Industry**.



UC3: Boosting **Financial** Security through Enhanced Cybersecurity Awareness and Tools.

Simplifying CRA Compliance for SMEs

We automate **Cyber Resilience Act (CRA)** compliance through modular, security-focused solutions:

Security by Design



Vulnerability Handling



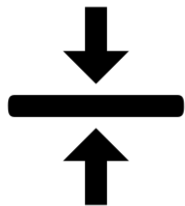
Lifecycle Security



Alignment with European Skills Standards

ECSF Role Alignment

Scenario-Based Learning



Hands-on Competency



NERO

8 advanced cybersecurity
awareness ecosystem for SMEs

CRA-Ready NERO Marketplace

- ▶ **Standardized Solution Discovery**
- ▶ **Built-in Comparison**
- ▶ **Ecosystem Viability**



NERO: A Sustainable Foundation for CRA Compliance

NERO helps build a "CRA-compliant culture" within the SME ecosystem.

Strengthening EU
Cybersecurity

Supporting EU Policy
& Standards

Building a Robust
Cybersecurity
Ecosystem



*isn't just a project; it's a living
ecosystem that will sustain the
European cybersecurity landscape
by fostering **collaboration** and
driving **innovation** for SMEs as they
transition into the **CRA** era.*

Thank you for your attention!

Dr Eleni Seralidou (she/her)

Project Manager at trustilio B.V.

eleni.seralidou@trustilio.com



<https://nerocybersecurity.eu/>