CEN-CLC JTC 13/WG 9

Horizontal cybersecurity for products with digital elements

Update @ SEMI - 2025.09.17

Ben Kokx – Convenor of JTC 13/WG 9

Photo by Kendall Scott on Unsplash

(EU) 2024/2847 "EU Cyber Resilience Act" Summary Slide

Timeline

- Entry into force: December 10, 2024
- Date of applicability:
  - conformity: **December 11, 2027**
  - reporting: **September 11, 2026**

Focus

"**Products with digital elements**"

- Software
- Hardware
- Remote data processing solutions
- Open-source part of commercial activities

Excluded

- MDR/IVDR, cars, aeronautical products

Aim

Uniform legal framework for cybersecurity of "Products with digital elements" placed on the Union Market

Addresses

Economic Operators placing / making available products on the Union market

- **manufacturers**
- authorized representatives
- importers
- distributors

Implementation

- **Regulation**
  - binding and directly applicable in all member states
  - no national transposition
- Based on **New Legislative Framework**
- **Presumption of conformity**
  - harmonized standards
  - common specification
  - cybersecurity certification schemes
- **Penalties**
  - manufactures up to 15 M€ or 2.5% of the worldwide annual turnover
  - others 10 M€ or 2.0%

Obligations

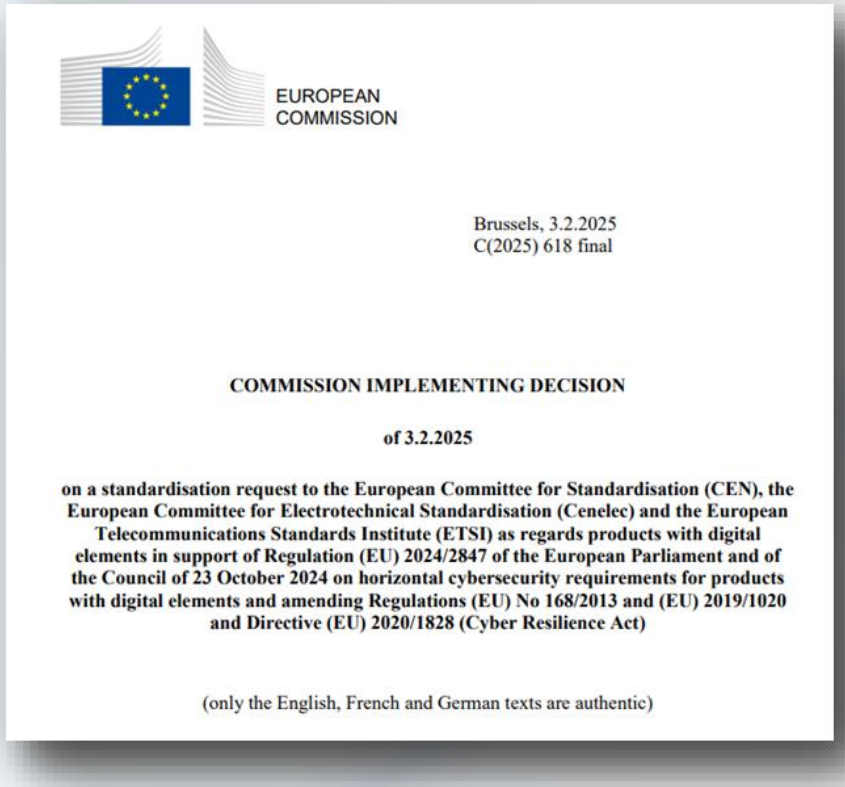
- **Fulfillment of essential cybersecurity requirements**
  - risk based approach
  - security properties
  - product lifecycle processes
  - vulnerability handling
- **Reporting**
  - actively exploited vulnerabilities
  - incidents having impact on product
- **Conformity assessment**

Cyber Resilience Act

Main timeline

- Published in OJEU : 2024-11-20
- **Entry into Force : 2024-12-10**
- Stand. Req. M/606 : 2025-02-03
- Std. Req. Accepted : 2025-03-02
- Draft implementing act : 2025-03-13
- ESO's provided work program : 2025-04-03
- Implementing act : Exp. 2026-Q1
- Delegated acts : ?
- Horizontal **process** standards : 2026-08-30
- **Reporting obligation : 2026-09-11**
- Vertical standards : 2026-10-30
- Horizontal **product** standards : 2027-10-30
- **Date of applicability : 2027-12-11**

CRA Standardization Request M/606



EUROPEAN
COMMISSION

Brussels, 3.2.2025
C(2025) 618 final

COMMISSION IMPLEMENTING DECISION

of 3.2.2025

on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(only the English, French and German texts are authentic)

JTC13 / WG9

Horizontal cybersecurity for products with digital elements

Established: March 27, 2023
Convenor : Ben Kokx
Secretariat : NEN

Committee members : 382
National organizations : 24
Liaisons : 16

WG9 meets bi-weekly with a 3-day hybrid plenary every 2 months.
Project teams have weekly meetings

Three project teams working on the horizontal deliverables for the CRA.
Currently meeting > 16 hours/week!

The SR asks in total for 41 items, 15 horizontal and the remaining are vertical deliverables for specific products, e.g. processors, networking equipment, operating systems, hypervisors, smartcards, certain toys, smart home products with security functions, etc., all to be delivered by 30/10/2026!

WG9 Deliverable

Project team 1

Cybersecurity requirements for products with digital elements – Principles for cyber resilience

CRA Stand. Req. Item	: 1
Document type	: EN
WI number	: JT013089
Status	: Draft Comment resolution
Next phase	: Submit for ENQ, Sep. 30
DAV target date	: October 2026

- Covers CRA Annex I, Part 1, Requirement 1
- **Process** standard to ensure products are developed and maintained with a risk-based approach to cover **any** security risks (as a catch-all, as 2a-m do not cover all possible cybersecurity risks)
- Implementation demonstrated via documented process outputs
- **Covers all** process activities

WG9 Deliverable

Project team 1

Cybersecurity requirements for products with digital elements – Principles for cyber resilience

CRA Stand. Req. Item : 1

Document type : EN

WI number : JT013089

Status : Draft Comment resolution

Next phase : Submit for ENQ, Sep. 30

DAV target date : October 2026

WG9 Deliverable

Project team 2; item 1

Cybersecurity requirements for products with digital elements – Generic security requirements

CRA Stand. Req. Item	: 2 - 14
Document type	: EN
WI number	: JT013091
Status	: On Hold
Next phase	: Draft review, Jan 2026
DAV target date	: January 2027

- Covers CRA Annex I, Part 1, Requirement 2 (a-m)
- **Product** standard addressing a specific set of security requirements by mapping security objectives to a catalog of possible security controls;
- Implementation demonstrated via the product itself and/or supported by technical documentation;
- **Refers to PT1 (/ PT3)** for process activities and might augment technical documentation content requirements;
- Builds upon the EN 18031:2024 series, augmented with additional security controls.

WG9 Deliverable

Project team 2; item 1

Cybersecurity requirements for products with digital elements – Generic security requirements

CRA Stand. Req. Item : 2 - 14

Document type : EN

WI number : JT013091

Status : On Hold

Next phase : Draft review, Jan 2026

DAV target date : January 2027

WG9 Deliverable

Project team 2; item 2

Cybersecurity requirements for products with digital elements – Threats and Security Objectives

CRA Stand. Req. Item	: Supports PT2 & verticals
Document type	: TR
WI number	: JT013097
Status	: On Hold
Next phase	: Ballot, Jan 2026
DAV target date	: August 2026

- This TR provides guidance on the common threats related to the essential product requirements of Annex I, Part 1, requirement 2 and the security objectives.
- The NWIP was circulated with a mature draft text to expedite the availability to all CRA standard writers.

WG9 Deliverable

Project team 2; item 2

Cybersecurity requirements for products with digital elements – Threats and Security Objectives

CRA Stand. Req. Item	: Supports PT2 & verticals
Document type	: TR
WI number	: JT013097
Status	: On Hold
Next phase	: Ballot, Jan 2026
DAV target date	: August 2026

WG9 Deliverable

Project team 3

Cybersecurity requirements for products with digital elements – Vulnerability handling

CRA Stand. Req. Item	: 15
Document type	: EN
WI number	: JT013090
Status	: Draft Comment resolution
Next phase	: Submit for ENQ, Oct. 20
DAV target date	: October 2026

- Covers CRA Annex I, Part 2
- **Process** standard to ensure products are maintained in a secure state using a risk-based approach
- Implementation demonstrated via documented process outputs and actions in the market (updates, notifications, recalls, etc.)
- **Augments PT1** activities with specific requirements and assessment criteria
- Perceived as a horizontal standard that the verticals should be able to normatively reference with no or minimal adoptions.
- The only horizontal standard of the three that hopefully might be suited for citation to provide a presumption of conformity for Annex I, part II.
- Strong normative dependency on the SOTA standards EN ISO/IEC 30111 and 29147.

WG9 Deliverable

Project team 3

Cybersecurity requirements for products with digital elements – Vulnerability handling

CRA Stand. Req. Item : 15

Document type : EN

WI number : JT013090

Status : Draft Comment resolution

Next phase : Submit for ENQ, Oct. 20

DAV target date : October 2026

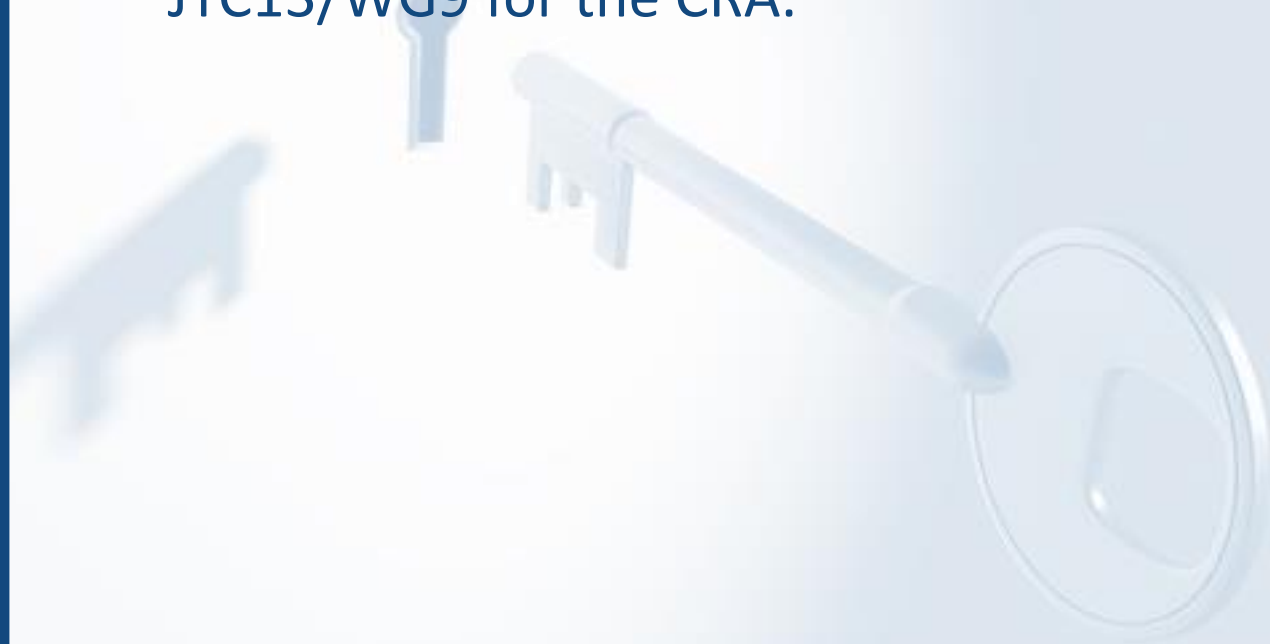
WG9 Deliverable

WG9 (shared by all PT's)

Cybersecurity requirements for products with digital elements – Vocabulary

CRA Stand. Req. Item	: T&Ds for WG9 documents
Document type	: EN
WI number	: JT013095
Status	: Drafting
Next phase	: Submit for ENQ, Sep. 30
DAV target date	: October 2026

- Ensure consistent use of **terms and definitions** for all horizontal deliverables of JTC13/WG9 for the CRA.



JTC13/WG9

Horizontal standards have a dual purpose

- State-of-the-art for all stakeholders to understand the expectations of what is required under the CRA
  - Manufacturers of the default class products (>90%) can understand what they must do and what security capabilities their products should have.
  - Should be aligned with market surveillance authorities' views.
  - Can be used by third parties for evaluation where verticals do not exist (yet).
- Can serve as a basis for vertical standards
  - The “General principles for cyber resilience” provides a skeleton and sets the expectations what verticals would need to address
  - The “Generic security requirements” can be used by the verticals as a normative reference to specific controls or be used as the basis for the product specific controls

Thank you

Ben Kokx