Cyber Resilience Act

Understanding the new regulation and essential requirements

17th October 2025

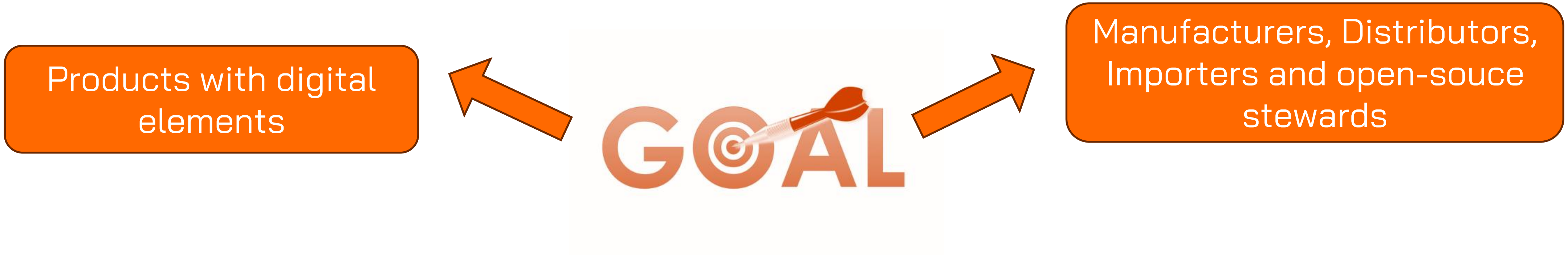
Applus+ Laboratories

Applus+ Cybersecurity

01 INTRODUCTION

The **Cyber Resilience Act (CRA)** is an EU regulation that sets cybersecurity requirements for hardware and software products to ensure they are secure throughout their lifecycle and protect consumers from digital threats.

"Strengthen the cybersecurity of products with digital elements (hardware and software) placed on the EU market."



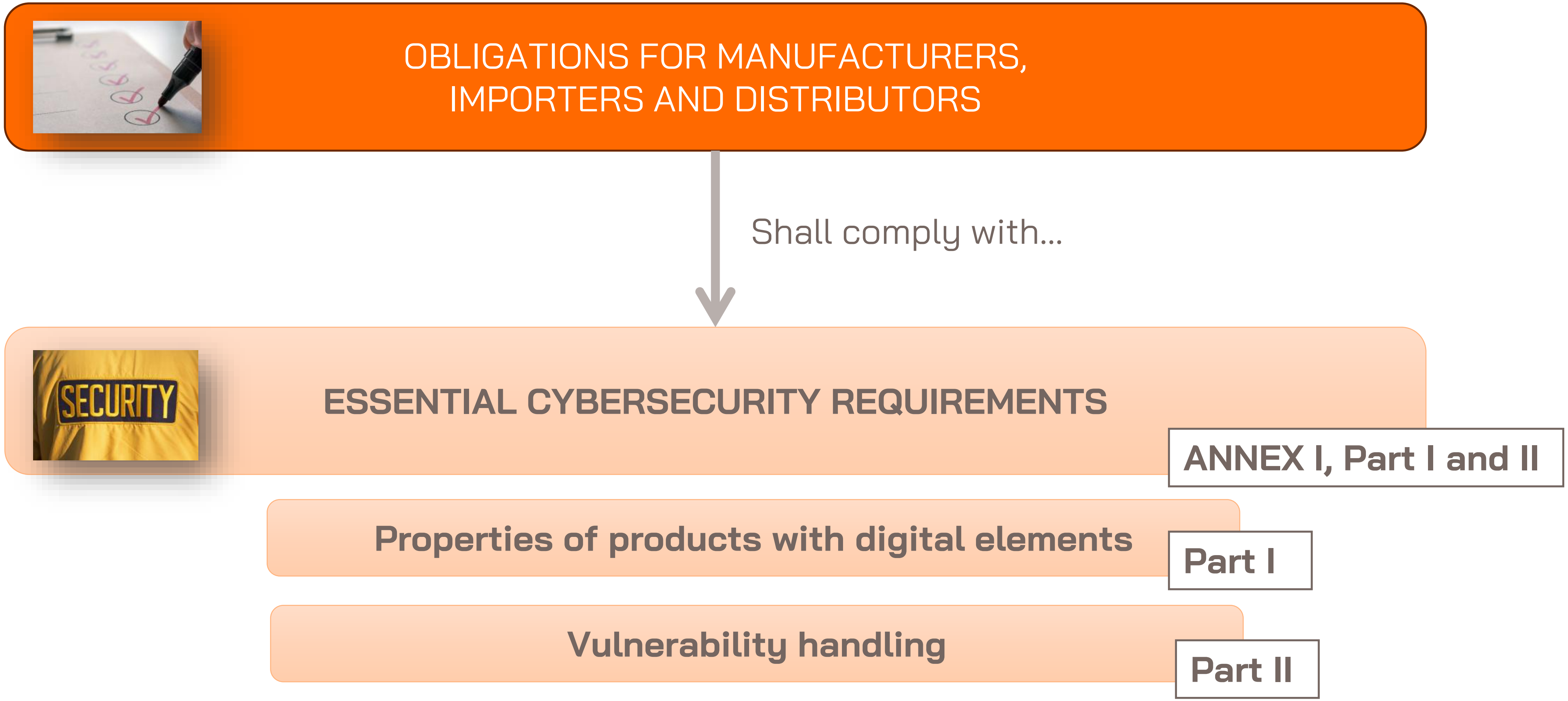
Products with digital elements

Manufacturers, Distributors, Importers and open-souce stewards

Why It Matters

- Ensures consumers and businesses can **trust digital products**.
- Prevents insecure devices and software from flooding the EU market.
- Encourages **secure innovation** while creating a **level playing field** for companies.

Basic idea of the CRA…



OBLIGATIONS FOR MANUFACTURERS, IMPORTERS AND DISTRIBUTORS

Shall comply with…

ESSENTIAL CYBERSECURITY REQUIREMENTS

ANNEX I, Part I and II

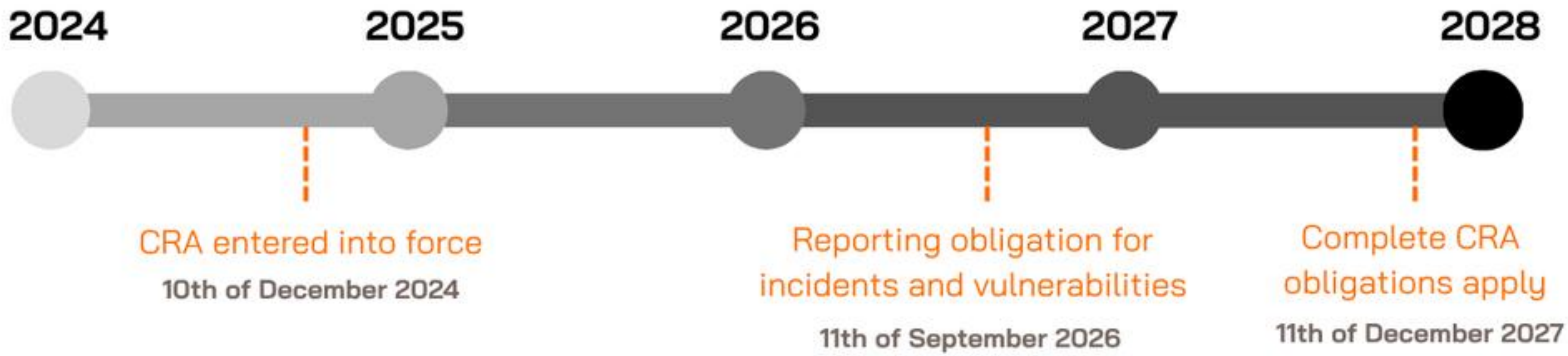
Properties of products with digital elements

Part I

Vulnerability handling

Part II

CRA key dates



- **Entry into force:** 10th December 2024.
- **Transition period:** There is a 36-month transition period before most obligations become fully applicable.
- **Full application:** 11th December 2027. This is when manufacturers and other economic operators must fully comply with the CRA requirements.
- **Reporting obligations for incidents and vulnerabilities**:11th September 2026. Some reporting obligations (e.g. for vulnerabilities) apply earlier, after 21 months.

Reporting Obligations

✓ WHAT WE KNOW

Reporting obligations for incidents and vulnerabilities: 11th September 2026.

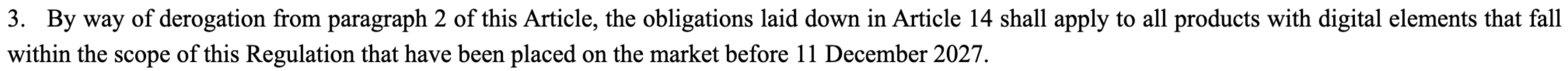
⚠ CRA Reporting Obligations → Apply to *All Products*

- Assuming reporting applies *only to new products*. **NO!**

2. Reality, the Article 69(3)...

- Obligations extend to *all products with digital elements*, even those sold before **11 Dec 2027**.

- From **11 Sept 2026**, any product still on the market (whether shipped in 2010 or 2025) must have processes to **detect** and **report vulnerabilities**. If it is still in the market...applies.



3. By way of derogation from paragraph 2 of this Article, the obligations laid down in Article 14 shall apply to all products with digital elements that fall within the scope of this Regulation that have been placed on the market before 11 December 2027.

Reporting Obligations

✖ WHAT WE DON'T KNOW

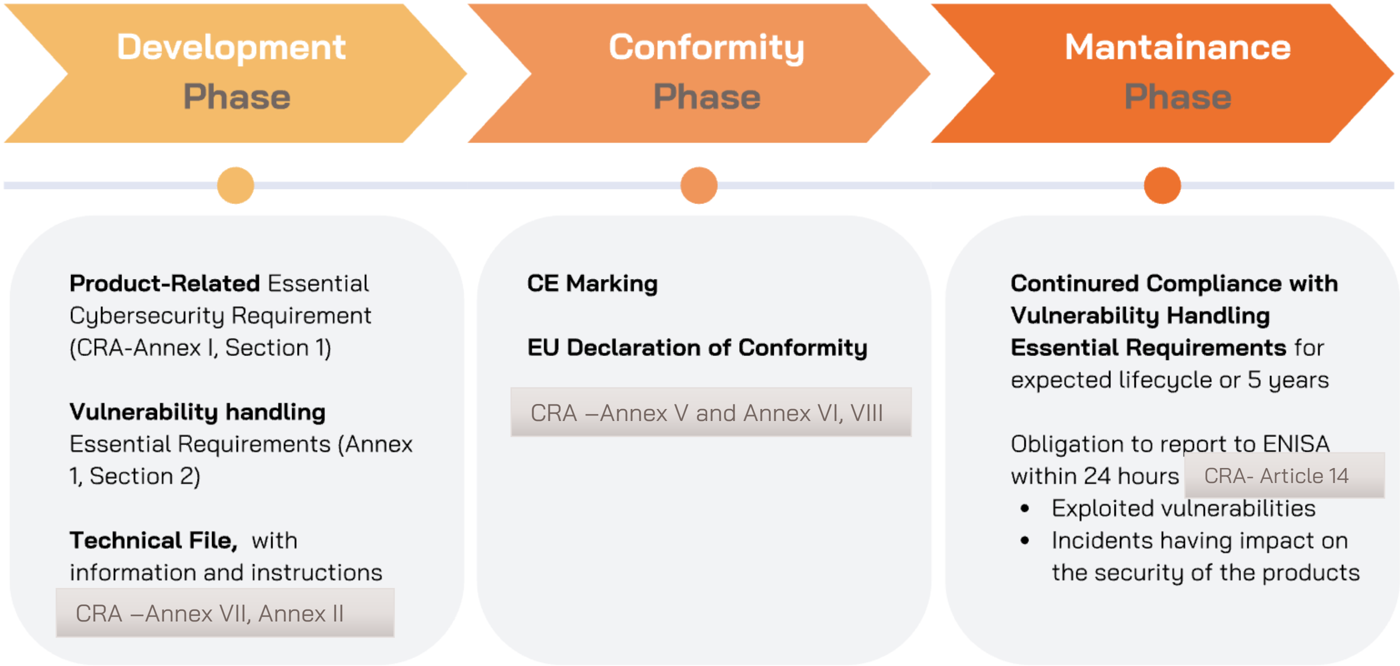
- How to report something on a product you don't know?
- How to identify what is a vulnerability without the Risk Assesment?

💡 START WITH SBOMs ASAP!

INTRODUCTION

Lifecycle: all main steps of conformity along the life of a product

If you are a manufacturer, make sure you are aware of the main process and all the steps to be followed:



Development Phase

Product-Related Essential Cybersecurity Requirement (CRA-Annex I, Section 1)

Vulnerability handling Essential Requirements (Annex 1, Section 2)

Technical File, with information and instructions

CRA –Annex VII, Annex II

Conformity Phase

CE Marking

EU Declaration of Conformity

CRA –Annex V and Annex VI, VIII

Mantainance Phase

Continured Compliance with Vulnerability Handling Essential Requirements for expected lifecycle or 5 years

Obligation to report to ENISA within 24 hours CRA- Article 14

- Exploited vulnerabilities
- Incidents having impact on the security of the products

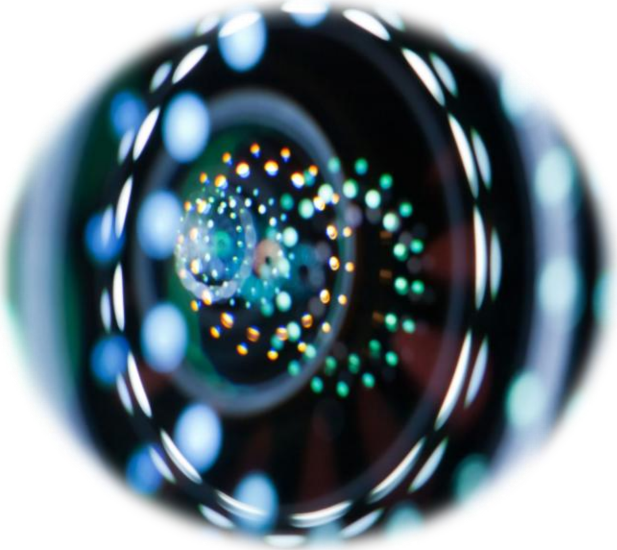
02 SCOPE

CRA scope is wide and profound. It is critical to understand the categories and classify our products on all the possible categories.

“This Regulation applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.”

PDE (Product with digital elements)

‘product with digital elements’ means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;



Is there any exception? YES!

Products excluded? YES

- Excluded from CRA are product categories already regulated by specific EU frameworks:
    - Medical devices and invitro diagnosis medical devices (Regulation (EU) 2017/745 and (EU) No 2017/746).
    - Motor vehicles (Regulation (EU) 2019/2144).
    - Certified aviation products (Regulation (EU) 2018/1139).
    - Marine equipment (Directive 2014/90/EU).
    - Identical spare parts (spare parts that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications).
    - Digital elements developed exclusively for national security (products with digital elements developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information).
    - Pure SaaS offerings may be outside scope unless they qualify as remote data processing solutions.
    - Non-monetized open-source software may also be exempt.

Be careful because pertaining to a sector does not mean you are excluded. The idea behind the CRA is that products covered by other regulations.

03 CATEGORIES

The **EU Cyber Resilience Act (CRA)** classifies products into three main categories for compliance:

Default category, Important and Critical products

CRA categories Annex III

90% of the Products
NON-CRITICAL

Default

Self-Assessment

- Module A
- Module B+C
- Module H

10% of the Products
IMPORTANT & CRITICAL

Important Class I

Self-Assessment if HS or 3rt party Assessment

- Module A
- Module B+C
- Module H

Important Class II

3rd Party Assessment

- Module B+C
- Module H
- CSA scheme, if available and applicable (Substantial)

Critical

3rd Party Assessment

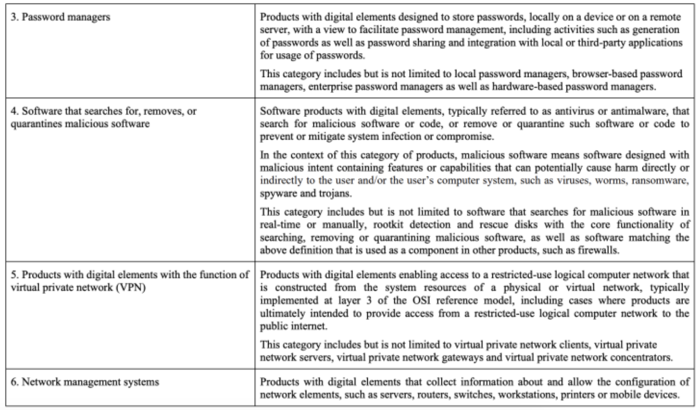
- CSA Scheme (EUCC)
- Procedures referred in “Important class II” if no delegated act

Categories

WHAT WE KNOW

- Guidance is expected from the European Commission and implementing acts to help manufacturers and providers determine the correct categorization.

- Commission has drafted the technical description of the categories of important and critical products in Draft implementing regulation - Ares(2025)2037850 and Annex - Ares(2025)2037850 in [Technical description of important and critical products with digital elements](). Note that this document is still under discussions.



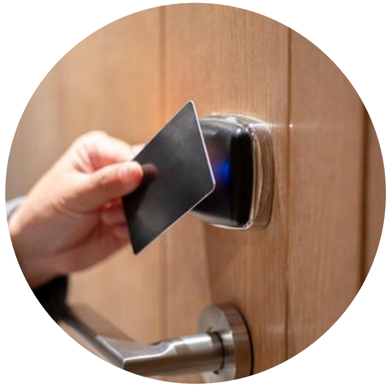
3. Password managers	Products with digital elements designed to store passwords, locally on a device or on a remote server, with a view to facilitate password management, including activities such as generation of passwords as well as password sharing and integration with local or third-party applications for usage of passwords. This category includes but is not limited to local password managers, browser-based password managers, enterprise password managers as well as hardware-based password managers.
4. Software that searches for, removes, or quarantines malicious software	Software products with digital elements, typically referred to as antivirus or antimalware, that search for malicious software or code, or remove or quarantine such software or code to prevent or mitigate system infection or compromise. In the context of this category of products, malicious software means software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system, such as viruses, worms, ransomware, spyware and trojans. This category includes but is not limited to software that searches for malicious software in real-time or manually, rootkit detection and rescue disks with the core functionality of searching, removing or quarantining malicious software, as well as software matching the above definition that is used as a component in other products, such as firewalls.
5. Products with digital elements with the function of virtual private network (VPN)	Products with digital elements enabling access to a restricted-use logical computer network that is constructed from the system resources of a physical or virtual network, typically implemented at layer 3 of the OSI reference model, including cases where products are ultimately intended to provide access from a restricted-use logical computer network to the public internet. This category includes but is not limited to virtual private network clients, virtual private network servers, virtual private network gateways and virtual private network concentrators.
6. Network management systems	Products with digital elements that collect information about and allow the configuration of network elements, such as servers, routers, switches, workstations, printers or mobile devices.

Categories

☒ WHAT WE DON'T KNOW

- Similar products but different categories based on the risk assessment?
- Under which circumstancies similar products can or not fall into an specific category?

VS



SHOULD DEPEND ON THE RISK ASSESSMENT MADE BY THE MANUFACTURER

04 CONFORMITY ASSESSMENTS

MODULE A, B+C AND H AND EUCC.

WHAT WE KNOW

Module A

Conformity assessment procedure based on internal control
Self-Assessment

Module B+C

EU-Type Examination + Internal Control
Third-Party Conformity Assessment

Module H

Conformity based on full quality assurance
Third-Party Conformity Assessment

Others: EUCC/CSA schemes

European cybersecurity certification scheme
Third-Party Conformity Assessment

Conformity to type based on internal production control (based on module C) is a **combination**: first, an external or designated authority verifies a type/model under Module B; then Module C requires the manufacturer to show that ongoing production matches what was certified.

Assessment procedures

❌ WHAT WE DON'T KNOW

- Regarding module H, how could it be used and what would it be accepted?
- No guidelines for the CAB's and Notified Bodies accreditation
- Broad scope of products; would the CAB's and Notified Bodies be accredited according specific product type?

UNDERSTAND THE ”NEW LEGISLATIVE FRAMEWORK”

WHAT is a HARMONISED STANDARD?

Harmonised Standards

A technical specification developed by a recognized European Standards Organization (CEN, CENELEC, or ETSI) at the request of the European Commission, and published in the Official Journal of the EU (OJEU).

Key Points:

Voluntary Use

Manufacturers are not legally obliged to use harmonized standards.

Pressumption of conformity

If a product is designed and tested according to the relevant harmonized standard, it is presumed to comply with the corresponding essential requirements of EU legislation (e.g. safety, cybersecurity, radio equipment, machinery).

Simplifies Compliance

Instead of proving compliance from scratch, manufacturers can rely on harmonized standards to demonstrate conformity.

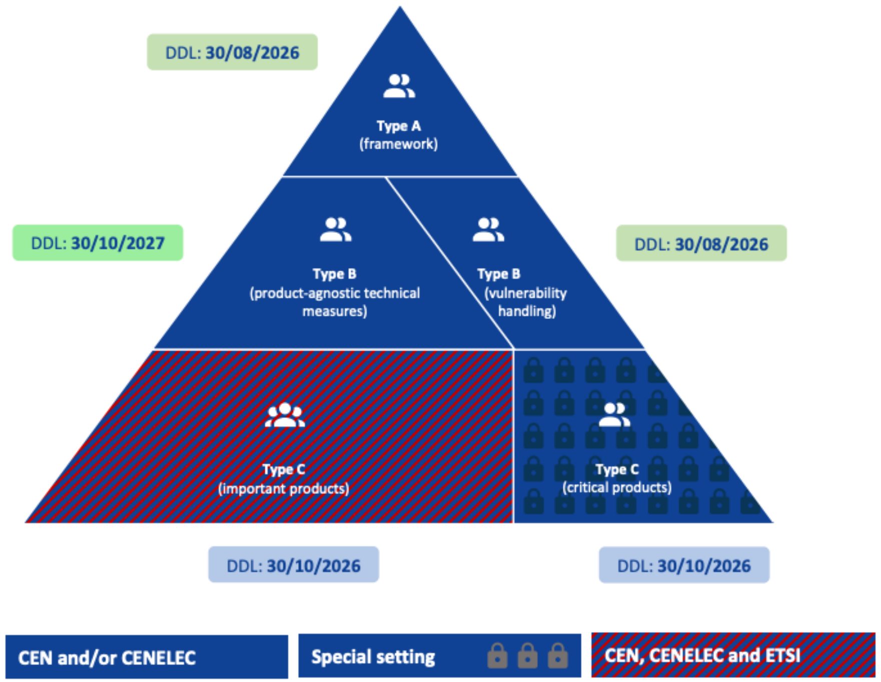
Linked to CE marking

Using harmonized standards is the most common way to show that a product meets EU legal requirements before affixing the CE mark.

Standardization work (Standardisation request M/606)

WHAT WE KNOW

- Standard have been requested by the European Commision to CEN/CENELEC and ETSI
- Currently being developed



DDL: 30/08/2026

Type A (framework)

DDL: 30/10/2027

Type B (product-agnostic technical measures)

Type B (vulnerability handling)

DDL: 30/08/2026

Type C (important products)

Type C (critical products)

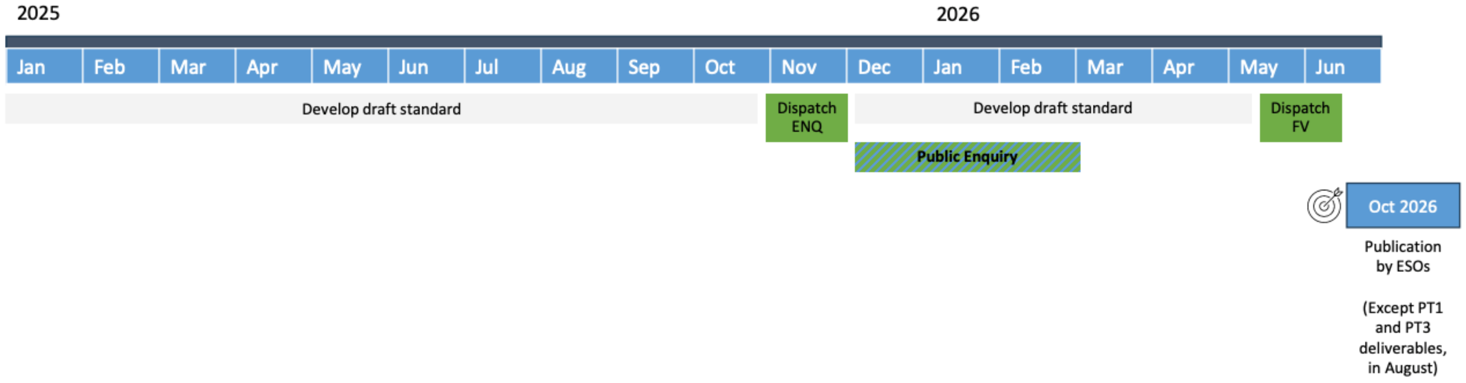
DDL: 30/10/2026

DDL: 30/10/2026

CEN and/or CENELEC

Special setting

CEN, CENELEC and ETSI



2025: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

2026: Jan, Feb, Mar, Apr, May, Jun

Develop draft standard (Jan–Oct 2025)

Dispatch ENQ (Nov 2025)

Develop draft standard (Dec 2025–Apr 2026)

Public Enquiry (Dec 2025–Feb 2026)

Dispatch FV (May 2026)

Oct 2026

Publication by ESOs

(Except PT1 and PT3 deliverables, in August)

Source: Webinar “CRA Standards Unlocked: Unlocking CRA Security Controls: preparation for UNE Event.” – 8th September 2025

Standardization work

✗ WHAT WE DON'T KNOW

- How can I start perfoming the risk assessment of my products?
- How can I start covering the Vulnerability Analysis Requirements?
- Under which circumstancies I can cover an specific threat with assumptions and policies?
- Vertical harmonized Standards for Default products?

COLLABORATE WITH STANDARDIZATION WORK AND OBTAIN EARLY DRAFTS

05 OBLIGATIONS TO MANUFACTURERS

OBLIGATIONS TO MANUFACTURERs

General view of Manufacturer obligations

Article 13

Obligations of manufacturers

Defines manufacturers' obligations to ensure products with digital elements are secure, maintained and compliant throughout their lifecycle.

Annex VII

Content of the Technical Documentation

Specifies that technical documentation must show how the product meets cybersecurity requirements, including design, risks, standards, tests, and conformity evidence.

Annex II

Information and instructions to the user

Specifies the required information and instructions to ensure secure use, support, and vulnerability handling of a product.

General view of Manufacturer obligations (Article 13)

1. MEET ESSENTIAL REQUIREMENTS AND RISK ASSESSMENT

2. DUE DILIGENCE AND VULNERABILITY HANDLING

3. SECURITY UPDATES

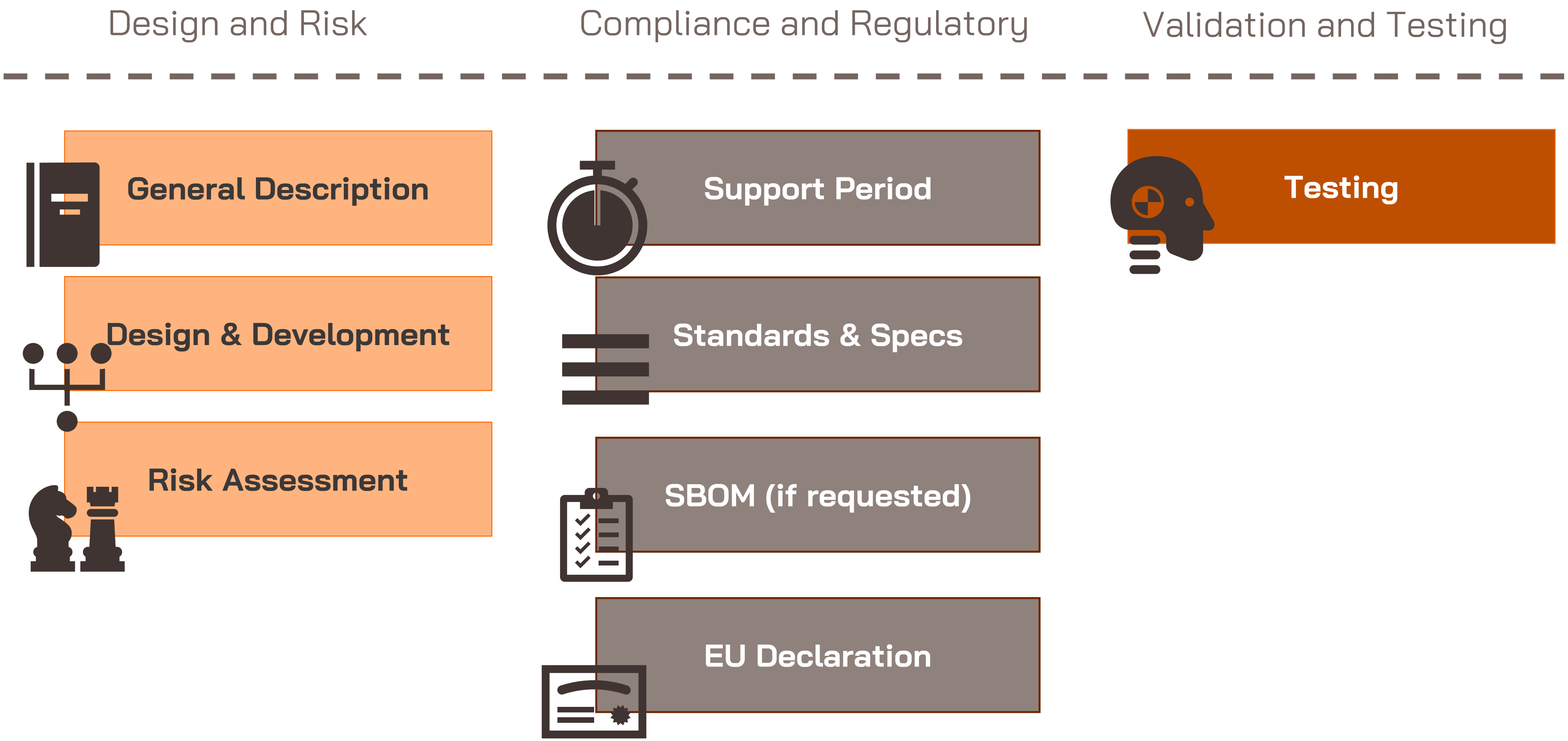
4. TECHNICAL DOCUMENTATION and GUIDELINES

5. PRODUCT IDENTIFICATION and MANUFACTURER CONTACT

6. EU DECLARATION OF CONFORMITY AND COMPLIANCE

OBLIGATIONS

Technical documentation (Annex VII)



Design and Risk

- General Description
- Design & Development
- Risk Assessment

Compliance and Regulatory

- Support Period
- Standards & Specs
- SBOM (if requested)
- EU Declaration

Validation and Testing

- Testing

Information and instructions to the user (Annex II)

1. Manufacturer Information

- Name
- Registered trade name or trademark
- Postal address
- Email or digital contact
- Website (if available)

3. Product Identification

- Product name and type
- Additional information enabling unique identification

2. Vulnerability Reporting Contact

- Single point of contact for reporting vulnerabilities
- Coordinated vulnerability disclosure policy can be found.

4. Intended Purpose & Security Information

- Intended purpose and security environment
- Essential functionalities
- Security properties

Information and instructions to the user (Annex II)

5. Cybersecurity Risk Information

- Known or foreseeable misuse scenarios.
- Potential significant cybersecurity risks

6. Technical Security Support

- Type of technical security support offered.
- End-date of support period for handling vulnerabilities and providing updates.

7. EU Declaration of Conformity

- Product name and type
- Additional information enabling unique identification

8. Security Instructions & Information

(Provide directly or via online link) information such as:

- Secure inital commisioning and lifecycle measures

how changes to the product with digital elements can affect the security of data;

- How security-relevant updates can be installed;
- The secure decommissioning of the product with digital elements, including information on how user data can be securely removed;

06 REPORTING OBLIGATIONS

REPORTING OBLIGATIONS FOR MANUFACTURER

ARTICLE 14

WHAT AND TO WHO?

What to report?

- **Actively exploited vulnerabilities**
- **Severe security incidents**

…and their impact!

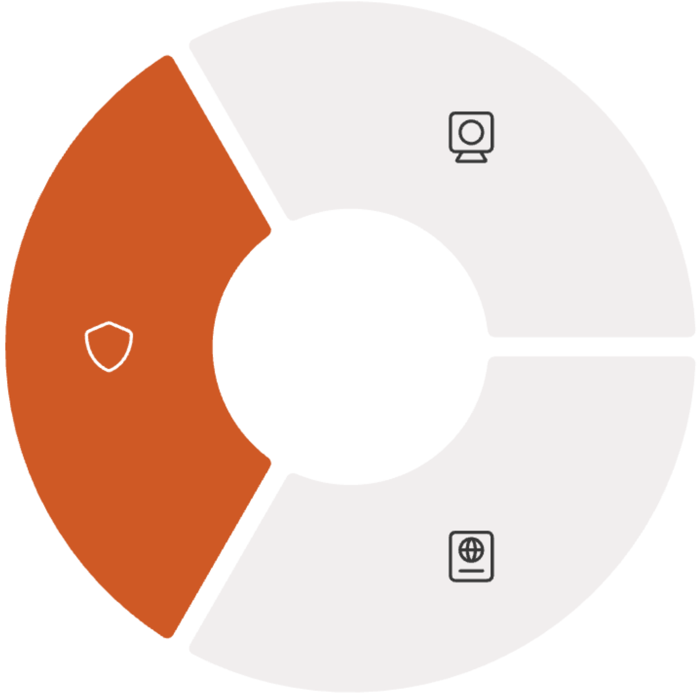
Who to report to?

- Designated coordinating CSIRT
- ENISA simultaneously
- Through **Single reporting platform (2026)**

REPORTING OBLIGATIONS IN A NUTSHELL

24h - Early Warning

- Warning notification of an actively exploited vulnerability.
- The incident is suspected of being caused by unlawful or malicious acts
- Member states where product is available



72h – Notification

- General nature of the exploit.
- Initial assessment of the incident
- Corrective/Mitigating measures

1 month – Final Report (for incidents)

- 14 days after corrective/mitigating measures(aev).
- Detailed description, root cause, and mitigation measures.

Thanks!