25.09.2025

PREPARE YOUR SME FOR EU CYBER RULES

HELPING SMES NAVIGATE EU CYBERSECURITY REGULATION WITH PRACTICAL TOOLS AND EXPERT GUIDANCE.

Getting to know the CRA

Chatzopoulou Argyro, Co-founder, Senior Cybersecurity Policy Advisor, APIROPLUS Services

CURIUM

SME4DD
Training SMEs for the Digital Decade

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The projects are 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 Agreements No. 101190372 and 101100768. 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.

Event & Participants' Insights

On **25 September 2025**, within the framework of the **CURIUM project**, an event on the **Cyber Resilience Act (CRA)** brought together SMEs to explore its impact.

Through live questions on **Slido**, participants' voices and perspectives were actively captured.

The following slides contain both the information provided as part of the workshop and the answers of the participants to the questions raised.

Have you ever heard of the CRA?

Yes
60%

No
20%

Maybe
4%

CRA, is it a bird sound?
16%

Which do you believe is the scope of the CRA?

Is actually what people call NIS2
15%

Defines horizontal cybersecurity requirements for products with digital elements
65%

Defines a framework for voluntary EU certification schemes
4%

I do not know what the scope of CRA is
12%

I still believe it has to do with birds
4%

The CRA

CRA shall apply from **11 December 2027**.
However, Article 14 (reporting) shall apply from **11 September 2026**
Chapter IV (Articles 35 to 51) (notification) shall apply from 11 June 2026.

=

CRA

Cyber Resilience Act

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) No 2019/1020 and Directive (EU) 2020/1828

The subject

The Regulation lays down:

- (a) rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products;
- (b) essential cybersecurity requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity;
- (c) essential cybersecurity requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the products are expected to be in use, and obligations for economic operators in relation to those processes;
- (d) rules on market surveillance, including monitoring, and enforcement of the rules and requirements.

Please provide examples fulfilling the term "Product with digital elements"

- **IoT**
- **Mobile applications**
- **Firewalls**
- **Wearables**
- **Software Platforms**
- **Industrial Communication Systems**
- **Email**
- **Web services**
- **Hardware & software solutions**
- **Any ICS**

Which of the following are Products with digital elements based on the CRA? (1/3)

Accounting software
80%

Mobile gaming app
87%

Software firewall
80%

MRI device connected to hospital network
73%

Which of the following are Products with digital elements based on the CRA? (2/3)

Blood sample analysis software
67%

Smart car
73%

Nanny cam
40%

Connected toy
47%

Which of the following are Products with digital elements based on the CRA? (3/3)

Personal wearable health technology
60%

Cloud application
67%

Door, Calculator, Dress, Hair dryer,
None of the above
0%

Products 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 (Article 3, Definitions)

with exceptions and specifics

Products 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 (Article 3, Definitions)

In simpler terms, a product with digital elements is:

- Software that has or is able to have a data or network connection during use. (accounting software, mobile gaming apps, software firewalls, security information and event management (SIEM))
- Hardware that has or is able to have a data or network connection during use. (smartphones, laptops, home cameras, smartwatches, connected toys, but also modems, firewalls, and smart meters.)
- A hardware product requiring a direct or indirect logical or physical data connection to a device or network. (industrial control systems, sensors)

Products with digital elements CRA

Medical devices as defined and regulated by the Regulation (EU) 2017/745;

Meaning any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, or diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, or investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, or providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

but not personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children.

In **vitro diagnostic medical devices** as defined and regulated by the Regulation (EU) 2017/746;

meaning any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on a physiological or pathological process or state or concerning congenital physical or mental impairments or concerning the predisposition to a medical condition or a disease or to determine the safety and compatibility with potential recipients or to predict treatment response or reactions or to define or monitoring therapeutic measures.

Products with digital elements CRA

Motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles as defined and regulated by the Regulation (EU) 2019/2144;

vehicles of categories M, N and O, as defined in Article 4 of Regulation (EU) 2018/858, and to systems, components and separate technical units designed and constructed for such vehicles (Vehicles having at least four wheels and used for the carriage of passengers, power-driven vehicles having at least four wheels and used for the carriage of goods, trailers)

Products **certified** under the Regulation (EU) **2018/1139**;

products, parts and equipment to control aircraft remotely, covering also the design, production, maintenance and operation of aircraft, as well as their engines, propellers, parts, non-installed equipment and equipment to control aircraft remotely, safety-related aerodrome equipment used or intended for use at the aerodromes, ATM/ANS in the Single European Sky airspace.

But not aircraft, and their engines, propellers, parts, non-installed equipment and equipment to control aircraft remotely, while carrying out military, customs, police, search and rescue, firefighting, border control, coastguard or similar activities.

Products with digital elements CRA

equipment that falls within the scope of Directive **2014/90/EU** of the European Parliament and of the Council;

> equipment placed or to be placed on board an EU ship and for which the approval of the flag State administration is required by the international instruments

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** as the components that they are intended to replace;

Products with digital elements **developed or modified exclusively for national security or defence purposes** or to products specifically designed to **process classified information**;

Websites that do not support the functionality of a product with digital elements, or **SaaS / PaaS / IaaS services cloud services** designed and developed outside the responsibility of a manufacturer of a product with digital elements;

Products with digital elements qualifying as **free and open-source software** that are not monetised by their manufacturers.

What should be ensured for every product with digital elements before its release to the market?

- **Security by design**
- **End user data protection**
- **Free of vulnerabilities**
- **Security compliance**
- **Integrity**
- **Technical & Organizational Measures (TOMs)**
- **Security certificate**
- **Secure Information Exchange**
- **Digital Identity Protection**
- **Intellectual property security**
- **CIA**

Products with digital elements shall be made available on the market only where:

- they **meet the essential cybersecurity requirements** set out in Part I of Annex I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed; and
- the **processes put in place by the manufacturer comply** with the essential cybersecurity requirements set out in Part II of Annex I.

Which of the following activities should be carried out in relation to products with digital elements? (1/2)

Vulnerability management
90%

Risk assessment
85%

Penetration testing
80%

Certification
55%

ISMS based on ISO/IEC 27001
45%

Which of the following activities should be carried out in relation to products with digital elements? (2/2)

Optimized web accessibility
10%

Cost optimization
0%

No mandatory requirements
0%

I do not know
7%

Essential cybersecurity requirements

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**.

... products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

(b) 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;

(c) 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;

(d) 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;

(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;

(f) 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;

Essential cybersecurity requirements

(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);

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

(j) be designed, developed and produced to limit attack surfaces, including external interfaces;

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

(l) 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;

(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.

As SMEs you are ...

Affected by the CRA if the organization manufactures products with digital elements, regardless of size

84%

Affected by the CRA if the organization is an economic operator in relation to such products

16%

Not affected / Only AI-related / SME-fit version / Not sure

0%

Economic operators of the CRA

The CRA 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.

The CRA enforces requirements for specific types of “economic operators” - economic operator’ means the manufacturer, the authorised representative, the importer, the distributor, or other natural or legal person who is subject to obligations in relation to the manufacture of products with digital elements or to the making available of products with digital elements on the market.

Economic operators of the CRA

‘**manufacturer**’ means a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge;

‘**authorised representative**’ means a natural or legal person established within the Union who has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks;

‘**importer**’ means a natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union;

‘**distributor**’ means a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties;

Figure 7: CRA requirements for manufacturers, importers and distributors (2/2)

https://core.se/en/blog/cyber-resilience-act-end-regulators-patience

Requirements of the CRA Act for manufacturers, importers and distributors | X Implementation | △ Check if implemented | □ High effort

No.	Manufacturer (Article 10)	Importer (Article 13)	Dealers (Article 14)	Requirements for manufacturers, importers and distributors	Manufacturer	Importer	Dealers
14	(14)	(9)	(6)	14 Information to market surveillance authority in case of discontinuation of operation	X	X	X
15	(15)	...	...	15 EU-COM may define elements of the software bill of materials	...	...	...
16	...	(3)	...	16 Inform. to market surveillance authority in case of cyber security risks	...	X	...
17	...	(4)	(2) b)	17 Contact details of the importer	...	X	△
18	...	(5)	...	18 Annex II in an easy language for users	...	X	...
19	...	(6) Part 1	(4) Part 1	19 Non-compliance with Annex I leads to corrective action (recall)	...	X	X
20	...	(6) Part 2	(4) Part 2	20 Information to manufacturer and market surveillance authority[1]	...	X	X
21	...	(7)	...	21 Keeping the documentation and the EU declaration of conformity available	...	X	...
22	...	(8)	(5)	22 Provision of all information to market surveillance authority2	...	X	X
23	...	...	(1)	23 Observing the Cyber Resilience Act with "due diligence".	...	...	X

Source: CORE | 1: Information to manufacturer on vulnerabilities and to market surveillance authority on cybersecurity risks and corrective actions | 2: should this be so requested

Products with digital elements

Important products with digital elements

(a) the product with digital elements primarily performs functions **critical to the cybersecurity of other products, networks or services,** including securing authentication and access, intrusion prevention and detection, end-point security or network protection;

(b) the product with digital elements **performs a function which carries a significant risk of adverse effects** in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.

Default class

Critical products with digital elements

(a) there is a **critical dependency of essential entities** on the category of products with digital elements;

(b) incidents and exploited vulnerabilities concerning the category of products with digital elements could lead to **serious disruptions of critical supply chains across the internal market.**

Products with digital elements

Important products with digital elements

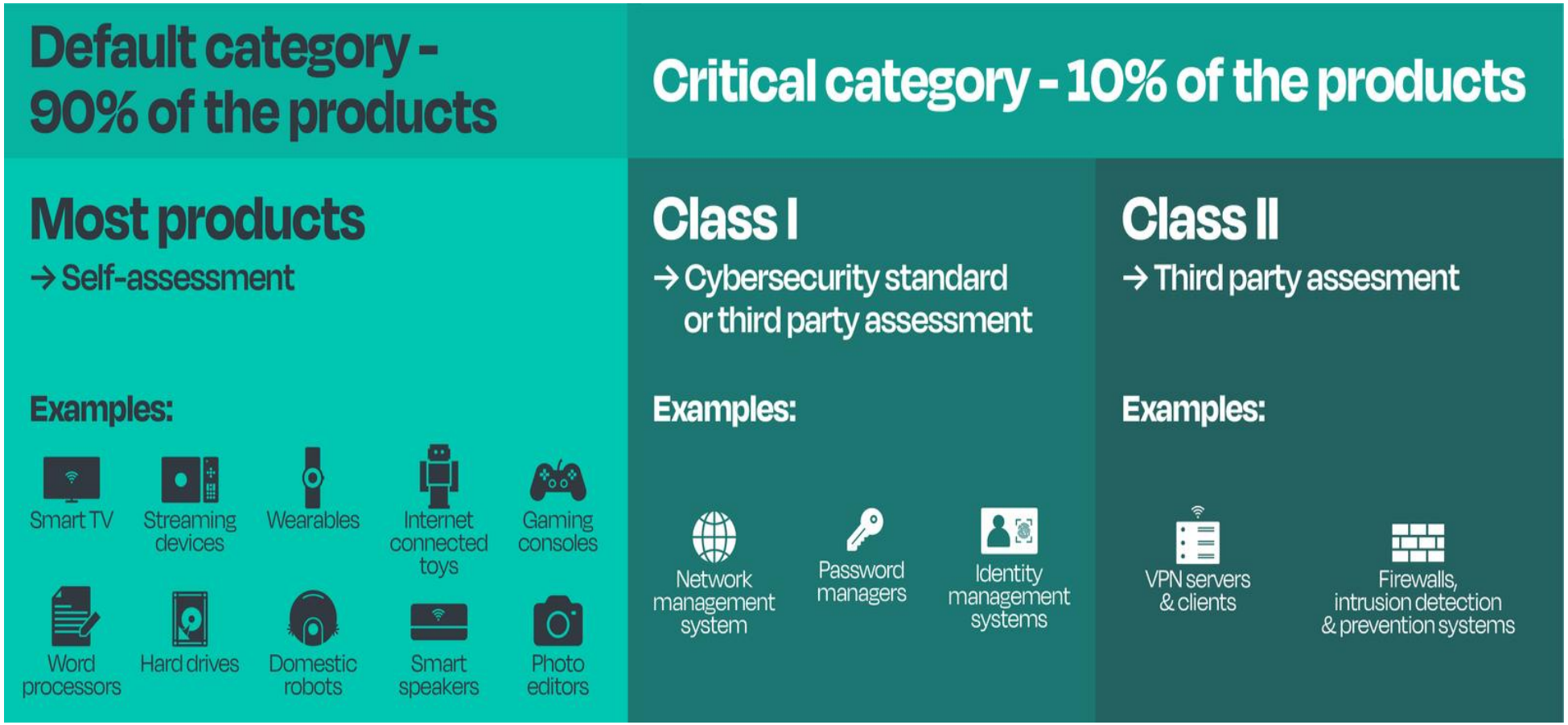
Standalone and embedded browsers, Password managers, Software that searches for, removes, or quarantines malicious software, products with digital elements with the function of virtual private network (VPN), Network management systems, security information and event management (SIEM) systems, boot managers, firewalls, intrusion detection and prevention systems…

Default class

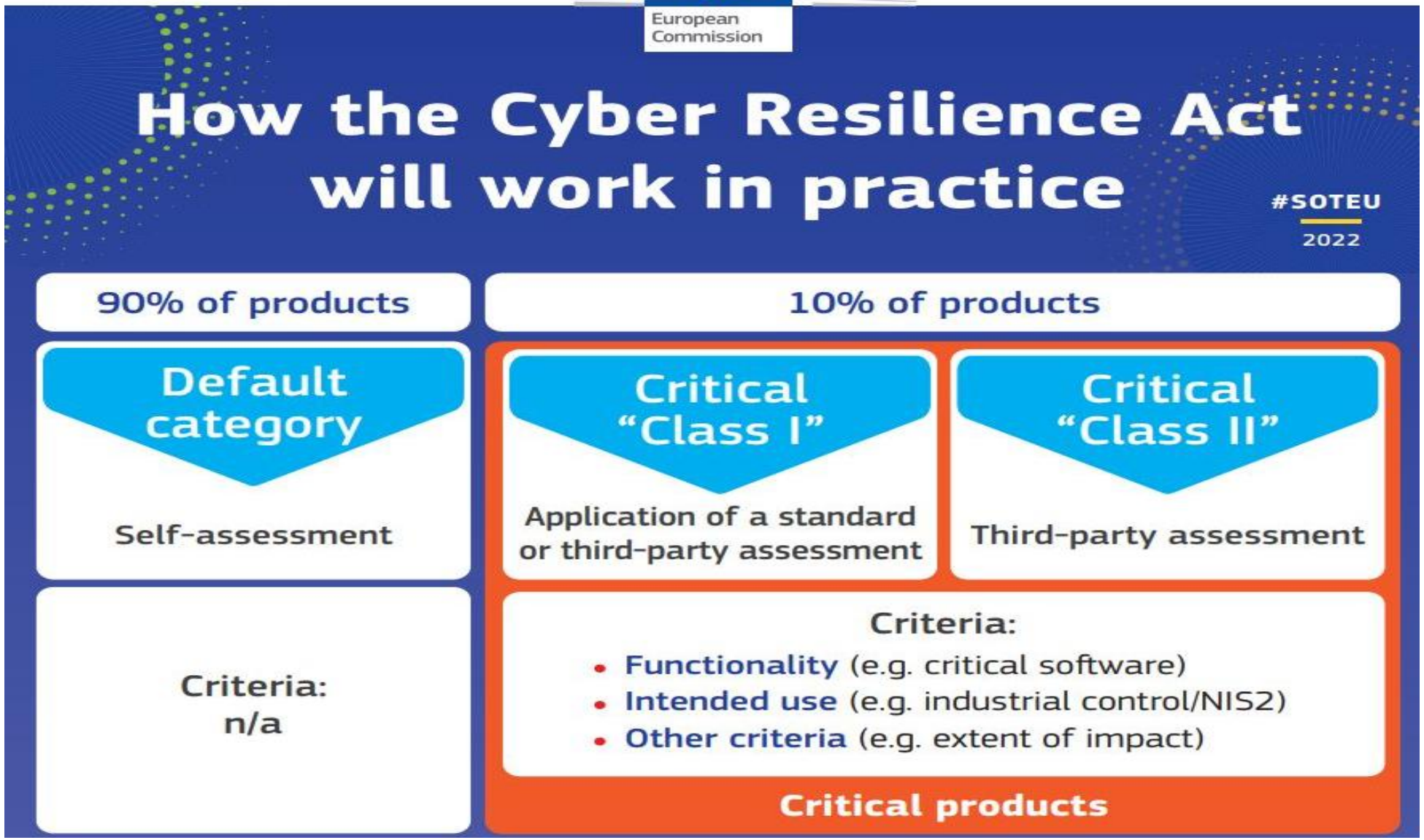
Critical products with digital elements

Hardware Devices with Security Boxes, Smart meter gateways within smart metering systems, Smartcards or similar devices, including secure elements…

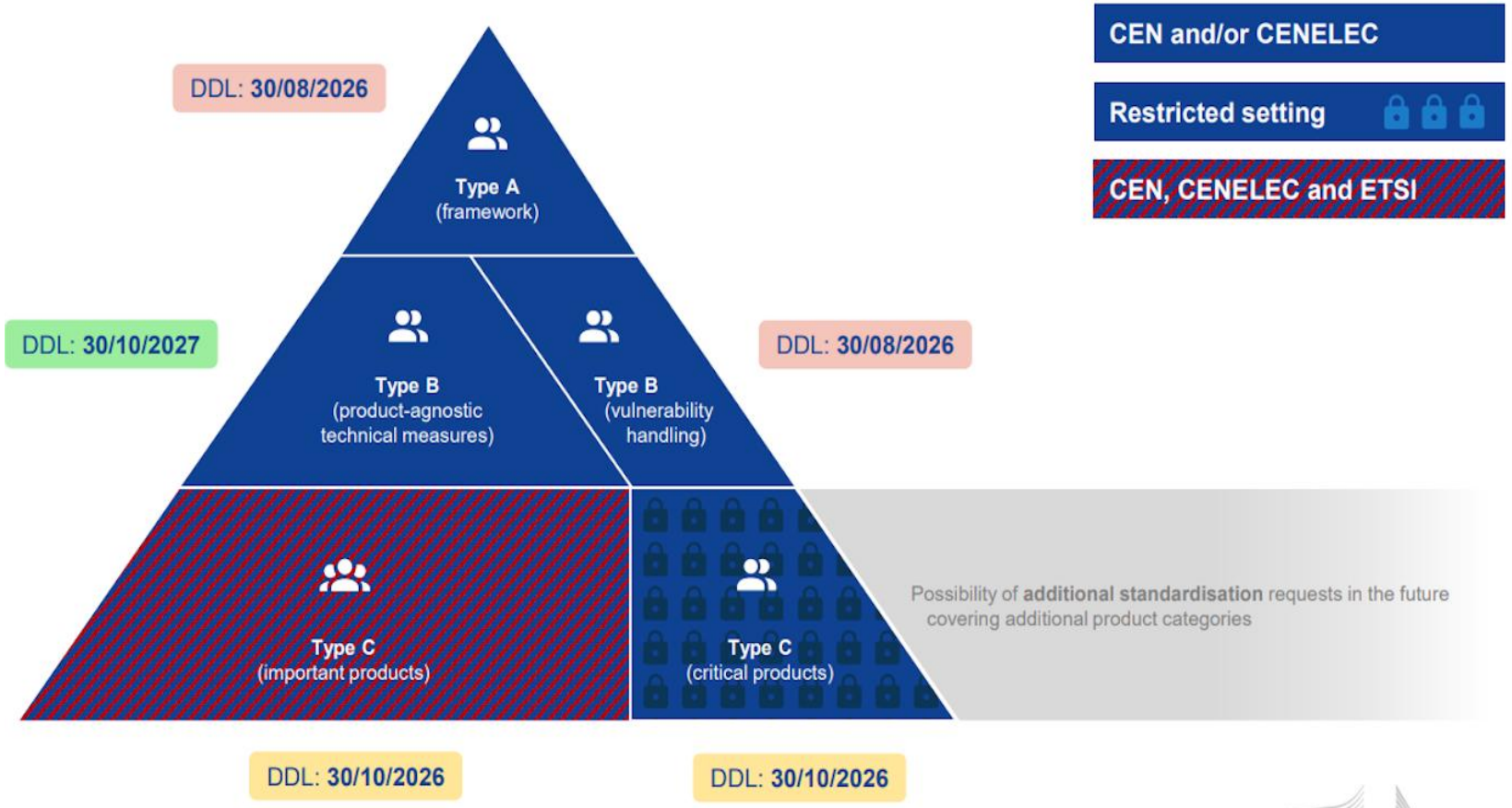
Differences per category



https://www.exein.io/blog/cyber-resilience-act-what-manufacturers-need-to-know


European Commission
How the Cyber Resilience Act will work in practice
#SOTEU 2022
90% of products
10% of products
Default category
Self-assessment
Critical "Class I"
Application of a standard or third-party assessment
Critical "Class II"
Third-party assessment
Criteria:
n/a
Criteria:
Functionality (e.g. critical software)
Intended use (e.g. industrial control/NIS2)
Other criteria (e.g. extent of impact)
Critical products

Standardization request



On April 3, 2025, the Standardization Request for the Cyber Resilience Act (CRA) was officially accepted by CEN, CENELEC and ETSI. These European standardization organizations have committed to delivering harmonized standards ahead of the regulatory deadlines.

Standardization request

The development of these standards is led by several technical committees, which play a central role in defining harmonized European Standards aligned with the essential cybersecurity requirements defined in the CRA. There are three categories of standards in development:

Type A standard on cyber resilience principles: covers the first sentence from Annex I: “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.” It is expected to be published by August 2026

Type B horizontal standards: include product-agnostic cybersecurity requirements and vulnerability handling standards. The generic requirements standard is anticipated by October 2027, while the vulnerability handling standard, based on existing ISO/IEC standards, is due by August 2026. Both cover phases like discovery, triage and remediation

Type C vertical standards for products: specific requirements tailored to certain digital product categories. These standards specify CRA requirements providing presumption of conformity, if followed. They must align with Type A and B principles and are targeted for publication by October 2026

https://www.sgs.com/en/news/2025/09/safeguards-13125-update-on-developments-relating-to-the-eu-cyber-resilience-act

The countdown

11 June 2026

Requirements for conformity assessment bodies (institutions that check compliance with safety standards) come into force.

278	12	28	41
Days	Hours	Minutes	Seconds

30 August 2026

Release of horizontal framework (general principles). Horizontal standard on vulnerability handling.

343	12	28	44
Days	Hours	Minutes	Seconds

11 September 2026

Obligations to report vulnerabilities and security incidents come into effect for actively exploited vulnerabilities & severe incidents for all products.

355	12	29	35
Days	Hours	Minutes	Seconds

https://reliableembeddedsystems.com/blog/countdown-to-the-cyber-resilience-act-cra/

The countdown

https://reliableembeddedsystems.com/blog/countdown-to-the-cyber-resilience-act-cra/

30 October 2026

Release of Vertical standards for important/critical products. Broad vertical standard for OT based on ISA/IEC 62443-4-1, -4-2, 3-3.

404	12	28	28
Days	Hours	Minutes	Seconds

30 October 2027

Release of Horizontal standard on generic cybersecurity requirements (based on EN 18031).

769	12	28	54
Days	Hours	Minutes	Seconds

11 December 2027

Every provision of the CRA comes into effect. Products cannot be sold on EU markets if they don't comply with the CRA.

811	13	28	36
Days	Hours	Minutes	Seconds

Thank you!

Chatzopoulou Argyro

Co-founder, Senior Cybersecurity Policy Advisor, APIROPLUS Services

ac@apiroplus.solutions