

CYNERGY 2026

Advancing Europe's digital resilience through research,
innovation and cross-sector collaboration

An SME's guide to cybersecurity compliance the who, what, how and when of the CSA and CRA

Argyro Chatzopoulou, Senior Advisor, APIROPLUS Solutions;

A little bit of history ...

On 13 September 2017, in his annual State of the Union Address, **President Jean-Claude Juncker** stated:

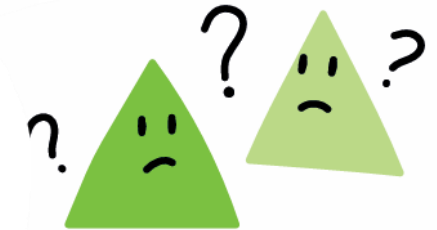
"In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."

‘Cybersecurity’: the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.

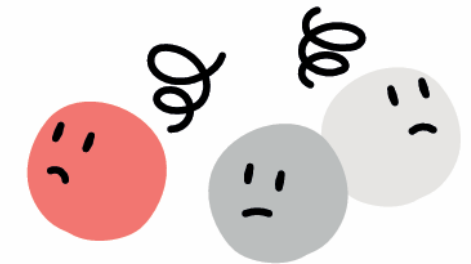


The problem...

IN TODAY'S ICT MARKET, HOW IS IT POSSIBLE TO COMPARE THE LEVEL OF SECURITY OF SOLUTIONS?

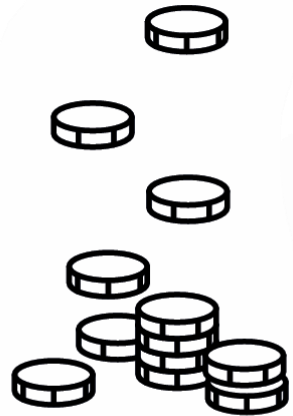


THIS LEAVES ICT CONSUMERS WITH **COMPLICATED CHOICES**.



DEVELOPERS AND SERVICE PROVIDERS ENTERING NEW MARKETS NEED TO COMPLY WITH **NUMEROUS SECURITY REQUIREMENTS**.

SOME OF THESE SOLUTIONS CALL THEMSELVES CYBER SECURE AND TRUSTWORTHY, WHILE OTHERS CARRY VARIOUS LABELS.

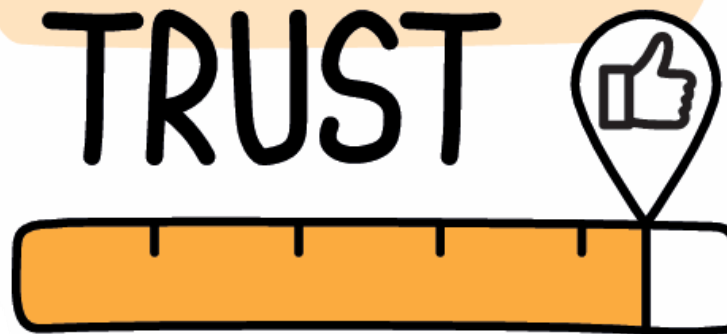


THIS LACK OF HARMONISATION RESULTS IN **HIGH COSTS**.

Source: ENISA - <https://certification.enisa.europa.eu/>

What are we doing about this?

TO ADDRESS THIS CHALLENGE,
THE EUROPEAN UNION IS DEVELOPING
EU CYBERSECURITY CERTIFICATION
TO PROVE COMPLIANCE
TO A GIVEN LEVEL OF



Source: ENISA - <https://certification.enisa.europa.eu/>

The solution: Certification; but is it working?

The cybersecurity certification landscape was fragmented in 2017



5.14	Standards and schemes for IoT device vendors
5.14.1	BITAG Internet of Things (IoT) Security and Privacy Recommendations
5.14.2	Future-proofing the Connected World
5.14.3	GSMA IoT Security Guidelines
5.14.4	Industrial Internet of Things Security Framework
5.14.5	IoT Security Compliance Framework
5.14.6	Online Trust Alliance IoT Trust Framework
5.14.7	OWASP Internet of Things Project
5.14.8	Strategic Principles for Securing the Internet of Things (IoT)

<https://ecs-org.eu/ecso-uploads/2022/10/5a60b8bf83f7c.pdf>

	Finland	Singapore	German
	Cybersecurity label	Cybersecurity labeling scheme	IT security label
Reference	ESTI 303 645	ESTI 303 645	ESTI 303 645

<https://innovation.consumerreports.org/interpreting-iot-labels-from-around-the-globe/>

CYBERSECURITY ASSESSMENTS Version1.0 |
January 2024

2.9 IOT LABELS

2.9.1 IoT Label – Germany

2.9.2 IoT Label – Finland

2.9.3 IoT Label – Singapore

2.9.4 PSA Certified

2.9.5 ioXt

2.9.6 Matter

2.9.7 Global Platform TEE

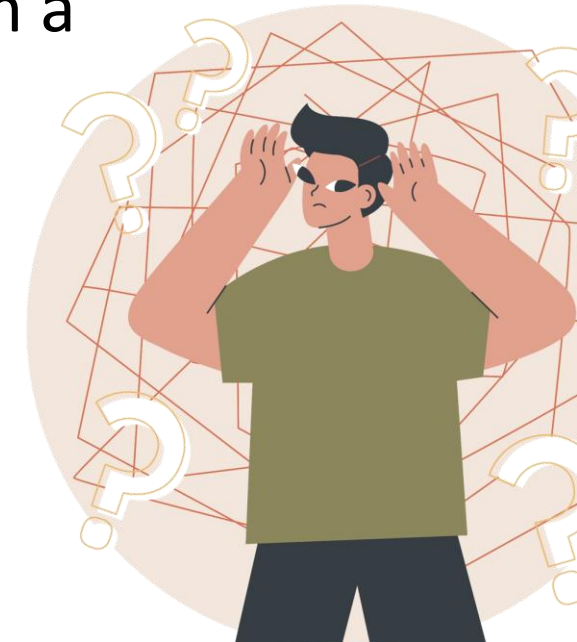
2.9.8 Global Platform SESIP

https://certification.enisa.europa.eu/document/download/b6616304-a50f-41fd-a1bc-dcf8bb11f4b5_en?filename=Cybersecurity%20Certification%20Statistics%20Report%202018-2022.pdf

Wait , wait... a lot of unknown words...

‘Certification’: the **procedure** resulting in the issuance of a certificate.

‘European cybersecurity certificate’: a **document** issued by a relevant body, attesting that a given **ICT product, ICT service or ICT process or Managed Security Service** has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme.



The EU Cybersecurity Act

TITLE I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down:

(a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and

(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes and managed security services in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

REGULATION (EU)
2025/37 (amendment)

The framework referred to in point (b) of the first subparagraph applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.

2. This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law.

The EU Cybersecurity Act

Proposal for a Regulation for the EU Cybersecurity Act, 2026

Article 1

Subject matter and scope

This Regulation lays down:

- (a) the mission, objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA);
- (b) a framework for establishing European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, managed security services or the cybersecurity posture of entities in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union; and
- (c) a trusted ICT supply chain framework.

In preparation

Call for evidence

Public consultation

Feedback and consultation period

11 April 2025 - 20 June 2025

Feedback: Closed

Commission adoption

05 February 2026 - 12 May 2026

Feedback: Closed

Cybersecurity certification scheme you said?

‘European cybersecurity certification scheme’: a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes or Managed Security Services;



European Certification Scheme



ENISA, the European Union Agency for Cybersecurity is developing and maintaining the EU Cyber certification Schemes on ICT solutions:

EUCC

The European Common Criteria-based cybersecurity certification scheme

EUCS

European Union Cybersecurity Certification Scheme on Cloud Services

EU5G

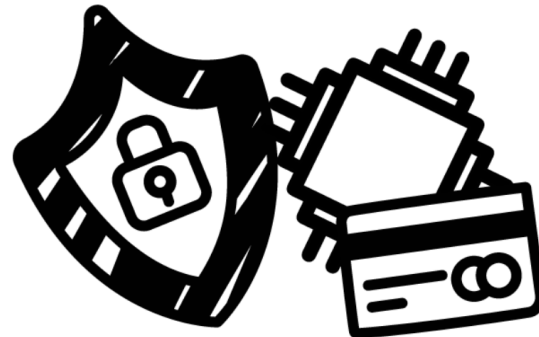
The European Cybersecurity Certification Scheme for 5G

EUDI Wallet

EU MSS

The European Cybersecurity Scheme on Common Criteria

The EUCC scheme allows ICT suppliers who wish to showcase proof of assurance to go through an EU commonly understood assessment process to certify ICT products such as technological components (chips, smartcards), hardware and software.

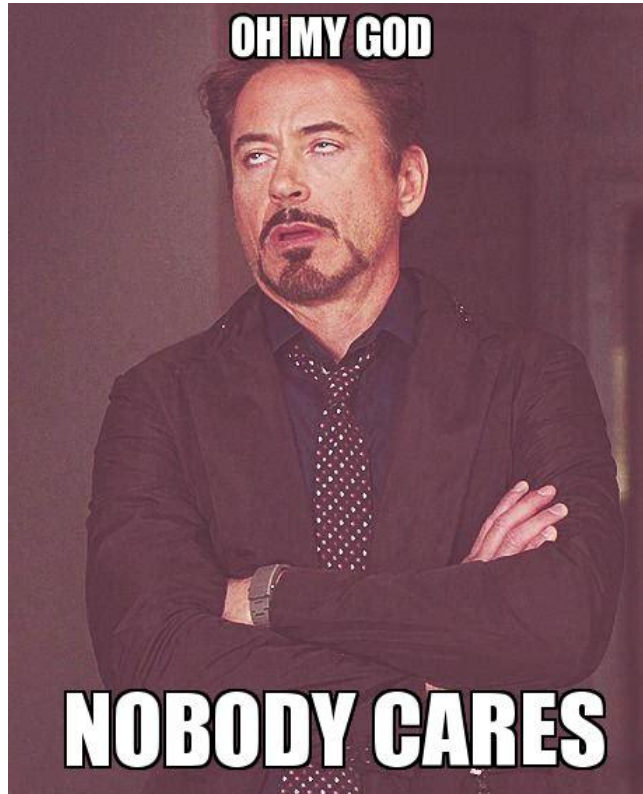


European Cybersecurity certification

The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.



OMG! Who cares?



Reality check*:

Sammy Azdoufal hooked up his DJI Romo vacuum cleaner to his PS5 controller. He found that not only could he control his own robot, but that he had gained access to data from other robot vacuum cleaners.

What kind of data? Live camera feeds, microphone audio, maps from nearly 7,000 devices across 24 countries.

The accidental hacker: how one man gained control of 7,000 robots

When Sammy Azdoufal found he had access to data from robot vacuum cleaners around the world, he told a tech publication. But the implications could be mind-boggling



Clean sweep ... Sammy Azdoufal accessed live camera feeds with the DJI vacuum cleaner. Photograph: Sipa US/Alamy Stock Photo/Alamy Live News

*<https://www.theguardian.com/lifeandstyle/2026/feb/24/accidental-hacker-how-one-man-gained-control-robots->

And then.... the CRA!

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

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

The CRA – the basics

- ✓ **Cybersecurity rules** for the making available on the market of hardware and software
- ✓ **Obligations** for manufacturers, importers and distributors
- ✓ Cybersecurity **essential requirements** across the life cycle
- ✓ **Conformity assessment** – differentiated by product category
- ✓ **Reporting** obligations
- ✓ **Market surveillance and enforcement**
- ✓ **Entry into application:** 11 December 2027
except for reporting obligations: 11 September 2026

What?

‘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

In simpler terms, a product with digital elements is:

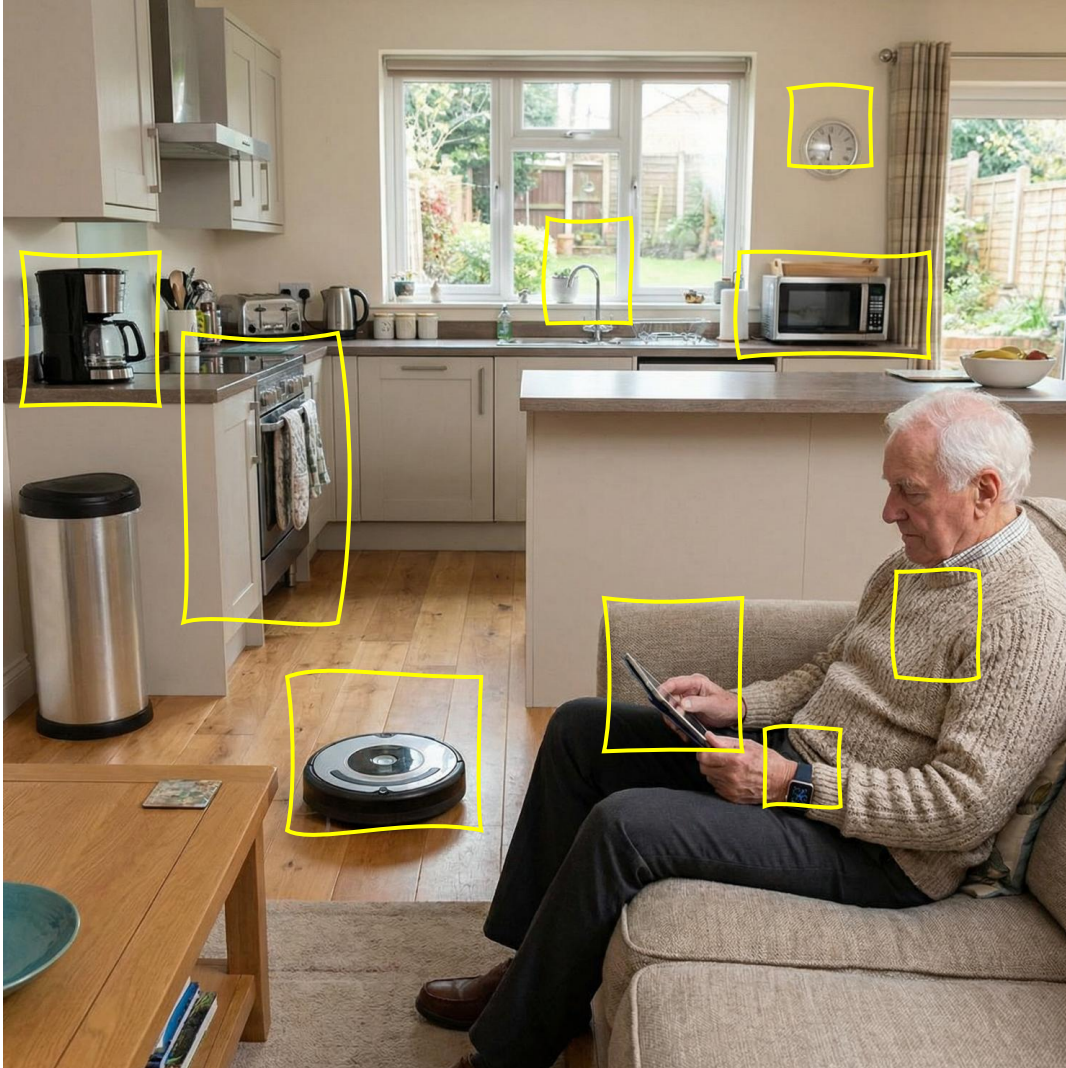
- Software that has or is able to have a data or network connection during use. (accounting software, mobile gaming apps, software firewalls, security information and event management (SIEM))
- Hardware that has or is able to have a data or network connection during use. (smartphones, laptops, home cameras, 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)



Can you identify any products with digital elements?



Can you identify any products with digital elements?

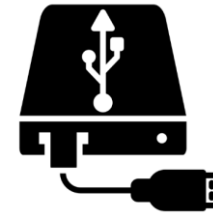


- Coffee maker
- Kitchen appliance
- Microwave
- Vacuum cleaner
- Wall clock
- Water tap
- Tablet
- Health tracker – watch
- Pacemaker

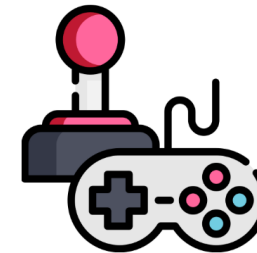
Not all IT products are products with digital elements! 😄

CUSTODIES

CURIUM



Backup

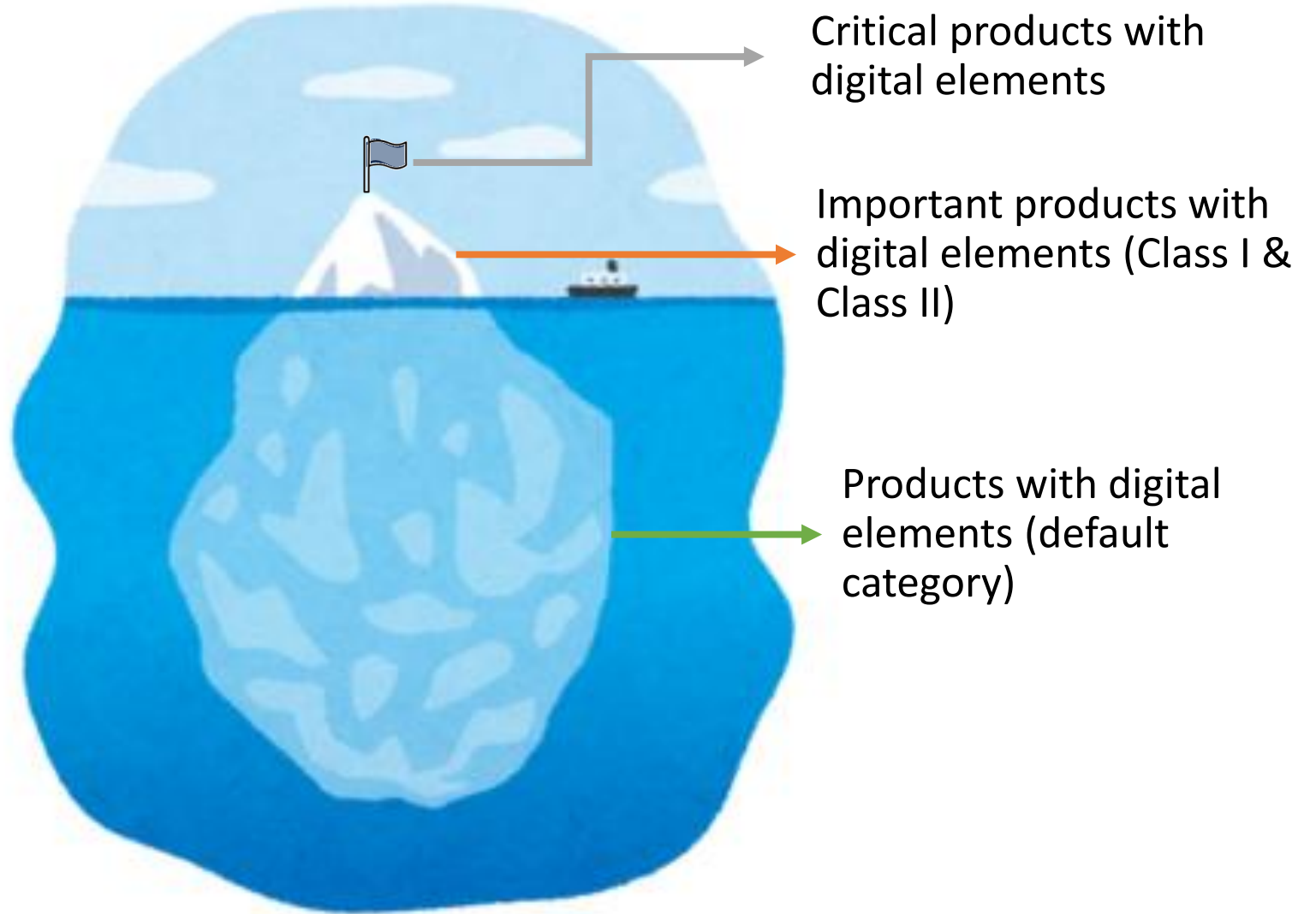


Games

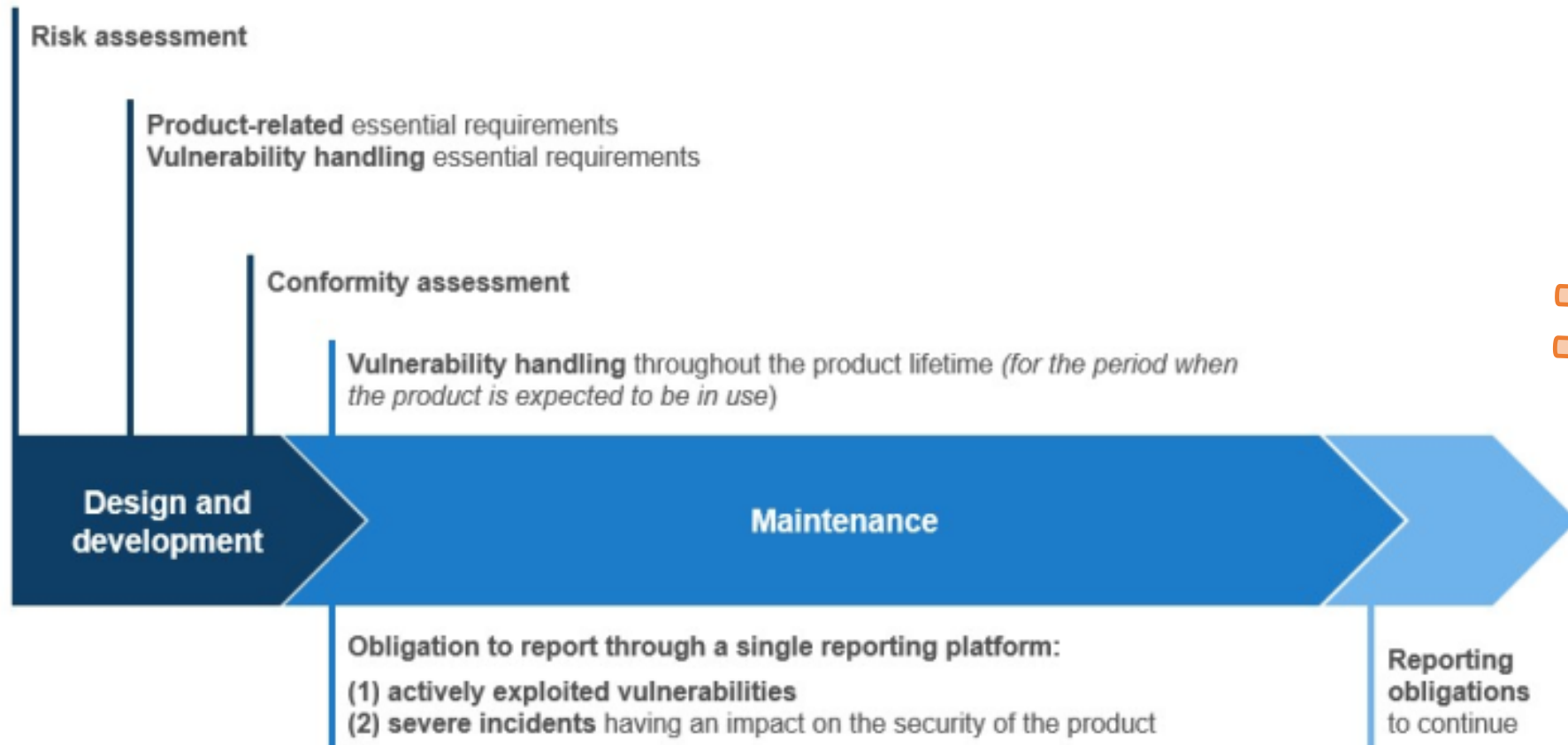


Classification of products with digital elements

a manufacturer should look at the **core functionality of its product** with digital elements to determine classification



Implementation steps of a manufacturer under the CRA



<https://digital-strategy.ec.europa.eu/en/policies/cra-manufacturers>

Conformity Assessment



Default category — self-assessment

(memory chips, mobile apps, smart speakers, computer games...)



Important products — application of standards/third-party assessment

(operating systems, anti-virus, routers, firewalls...)



Critical products — third party assessment (in the future potentially certification)

(smart cards, secure elements, smart meter gateways...)



FOSS — self-assessment (unless categorized as “critical products”)

(web development frameworks, operating systems, database management systems...)

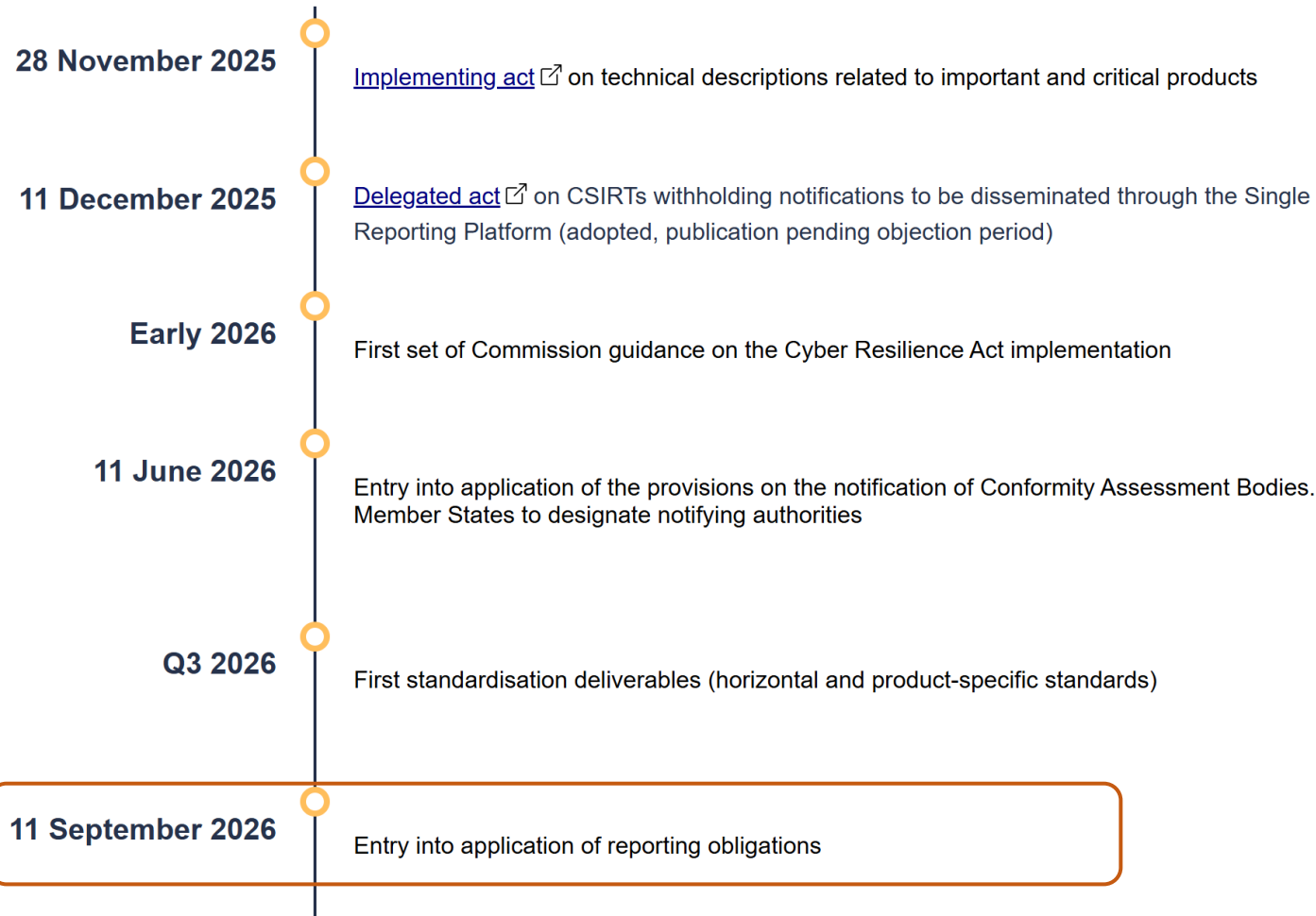
The manufacturer
has to prove and
assume
responsibility

At placement on the market

At the end of the process, the manufacturer can **affix the CE marking** and attach a **declaration of conformity** to its products.

Furthermore, the manufacturer needs to indicate the **support period**, i.e. how long the product will be supported, and provide **information and instructions** for the use of the product.

When?

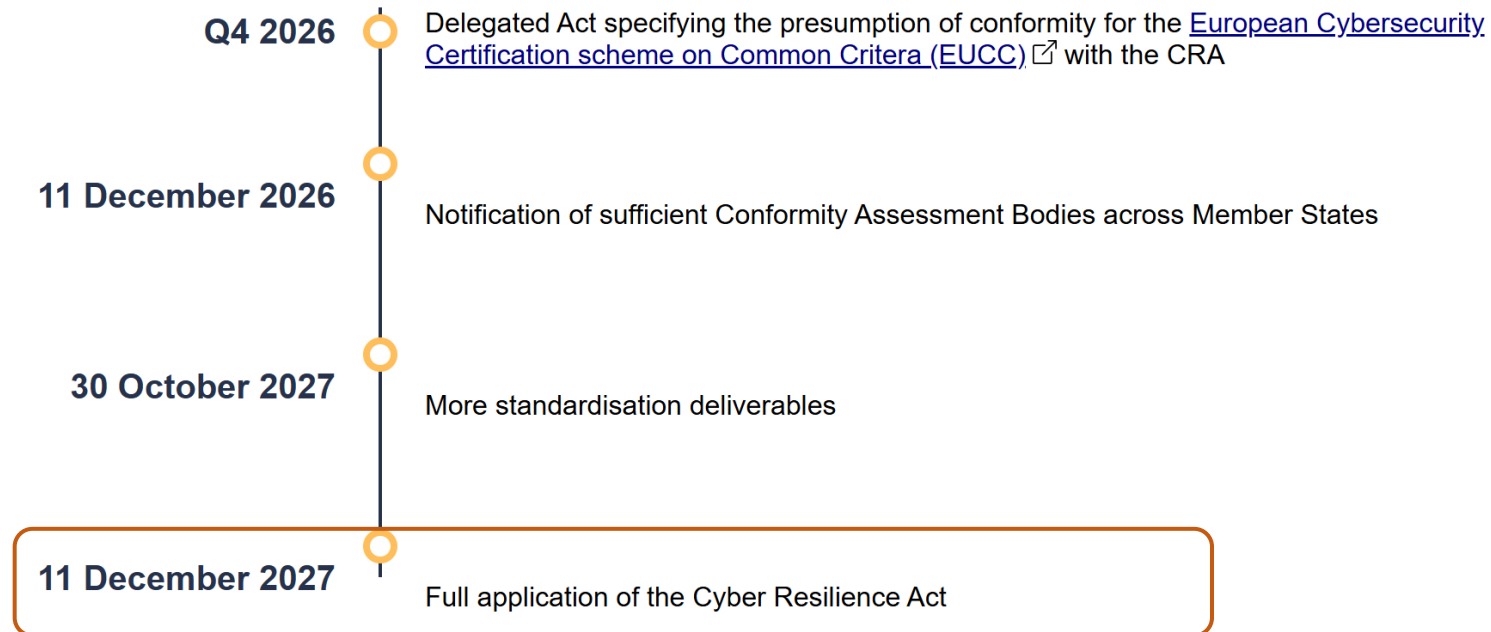


The CRA requires manufacturers to **notify actively exploited vulnerabilities and severe incidents** having an impact on the security of their product with digital elements.

24 hours - early warning
72 hours - a full notification



When????



Are you still confused? CSA vs CRA vs EUCC



Feeling a bit overwhelmed?



CURIUM

Here to Help!

CUSTODES

The CURIUM Continuum

Conformity Assessment and Compliance

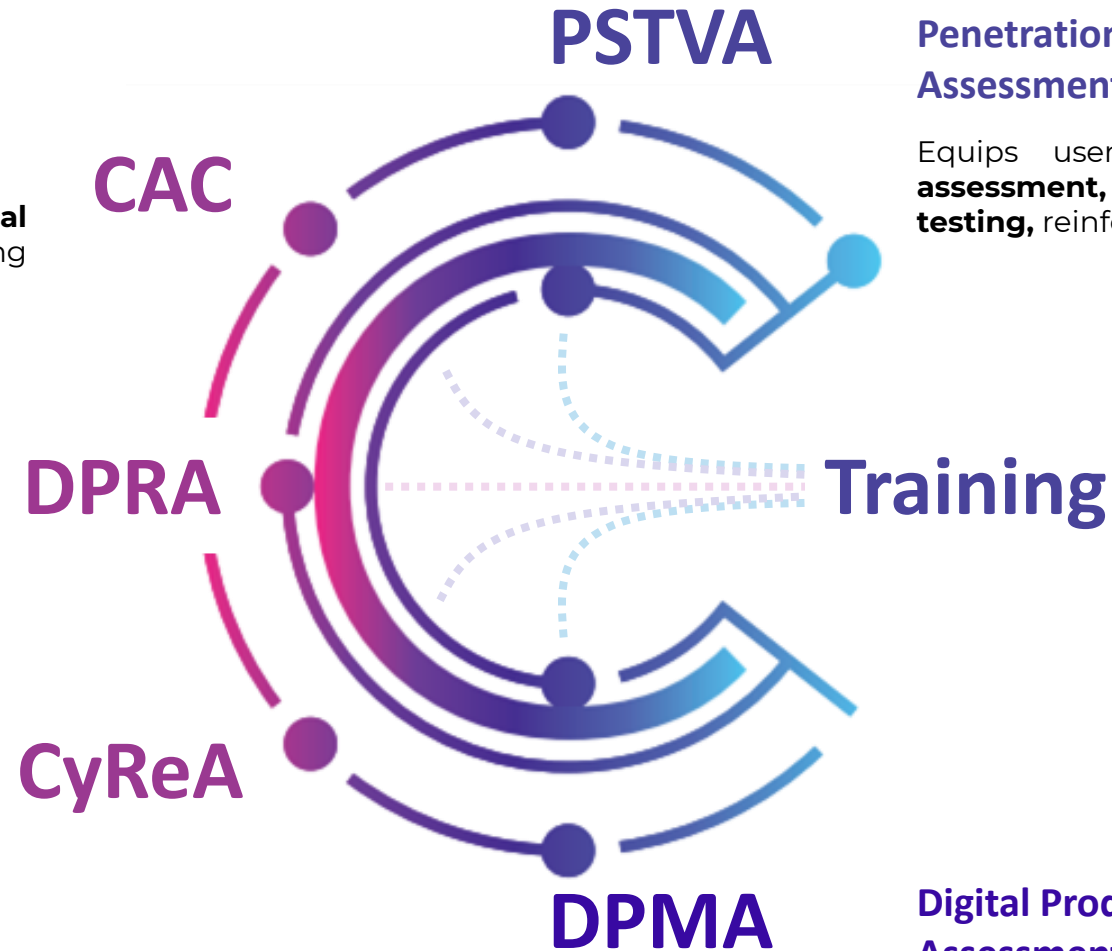
Provides a guided approach to **technical documentation and self-gap analysis**, ensuring alignment with CRA requirements.

Digital Product Risk management

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

Cyber Resilience Assessment

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



Penetration Self-Testing and Vulnerability Assessment

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

Digital Product Maturity Assessment

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

CURIUM exploitation options





Organizational Profile

[Dashboard](#) | [Organizational Profile](#) | [Product](#) | **Product details**



Inventory

- Assets
- Components
- Vulnerabilities
- Threats

Service Management

- Products**
- Certified Products



business webpage

Technical Evaluation
Report :

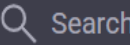


Request Declaration of
Conformity:



Certification
Status : **InProgress**

Assets 5 Security Objectives 4 Security Requirements 18 Assessment 71 Certification Sharing



Search



Add Asset

Name	Risk Score	Controls	Version	
▼ webserver	0.0%	3	1	⋮
▼ home computer OS	0.0%	4	1	⋮
▼ home router firmware	0.0%	1	1	⋮
▼ home computer	0.0%	6	1	⋮
▼ home router	0.0%	3	1	⋮

About

Created At: Feb 26, 2026

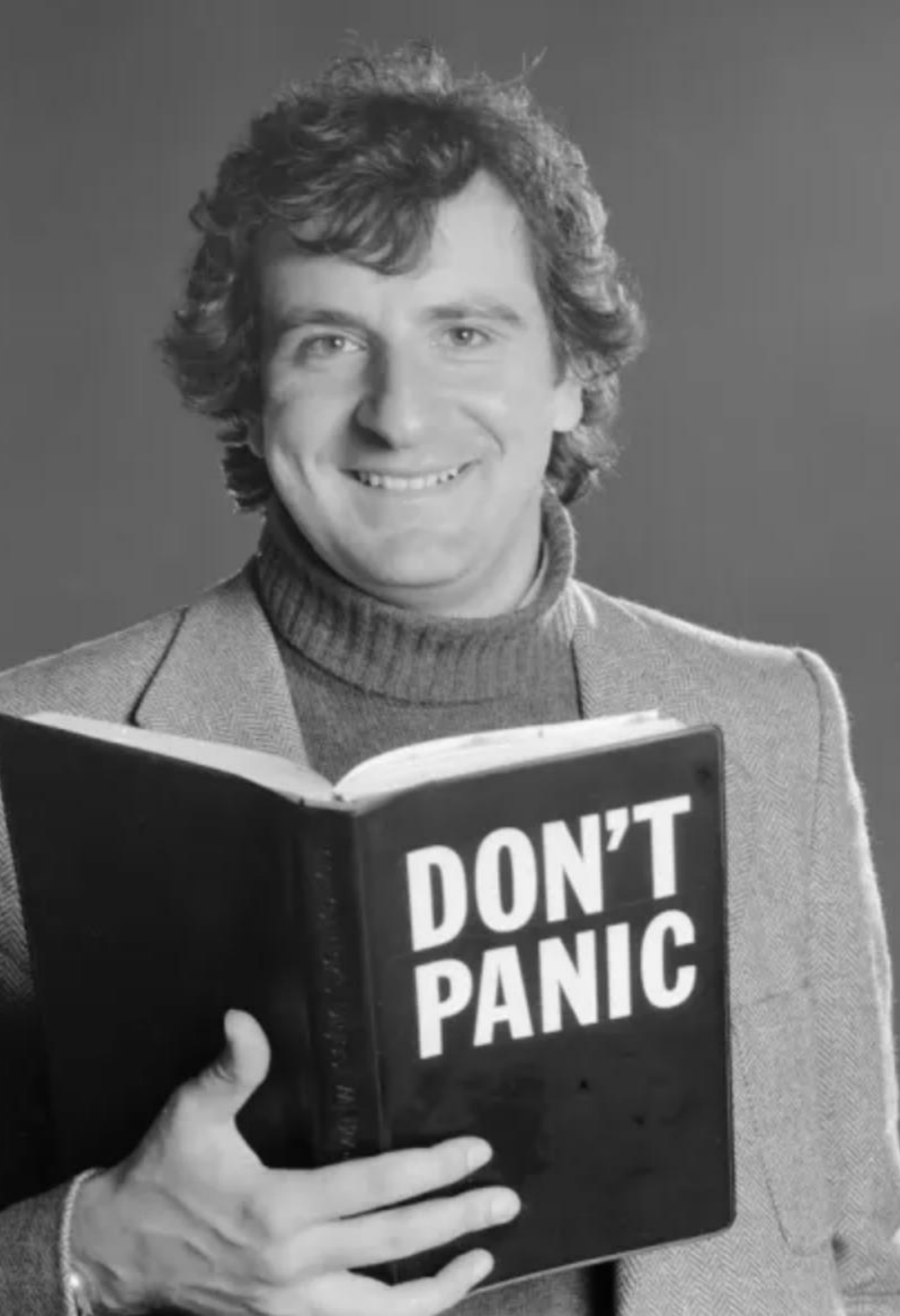
Modified At: Feb 26, 2026

Assurance
Level: EAL3:
Methodically
Tested and
Checked

Vulnerability
Analysis Level: AVA_VAN.2:
Vulnerability
analysis

Vulnerability
Analysis
Description: Assessment
against simple,
low-skill
attacks.
Ensures basic
protection
measures are
in place

Attack
Potential: Basic



Thank you very much!

Don't panic! DON'T PANIC!!

Douglas Adams, The Hitchhiker's Guide to the Galaxy

An SME's guide to cybersecurity compliance

31

Argyro Chatzopoulou, Senior Advisor, APIROPLUS Solutions;
Konstantinos Lampropoulos, Senior Cybersecurity Researcher,
p-NET Competence Centre