

SESSION TITLE

Interplay between the AI Act and the Cyber Resilience Act: overlapping requirements

Chatzopoulou Argyro, APIROPLUS Services Ltd.



Co-funded by the
European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



curium-project.eu

Conformity assessment for high-risk systems - The role of
testing © 2026 by APIROPLUS Services is licensed under



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.

AI Act

Article 15

Accuracy, robustness and cybersecurity

High-risk AI systems shall be designed and developed in such a way that they **achieve an appropriate level of accuracy, robustness, and cybersecurity**, and that they perform consistently in those respects throughout their lifecycle. High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities. The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

Cyber Resilience Act

(CSA - REGULATION (EU) 2024/2847)

Article 6 Requirements for products with digital elements

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

- (a) 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
- (b) the **processes put in place by the manufacturer comply with the essential cybersecurity requirements** set out in Part II of Annex I.

KEY CONCEPT

'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 - CRA

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 (PDE)



AI System for Access and Admission to Educational & Vocational Institutions

Intelligent. Fair. Transparent. Inclusive.

Using AI to evaluate applicants and recommend the most suitable educational or vocational training opportunities at all levels.



All Levels
Primary, Secondary,
Tertiary, Vocational



All Pathways
Academic, Technical,
Vocational



For Everyone
Equal Opportunity
for All

What is this product?

1. INPUT DATA



Personal Information
Identity, Age, Location



Academic Records
Grades, Transcripts,
Certificates



Aptitude & Skills
Test Scores, Assessments,
Competencies



Interests & Preferences
Career Interests, Programs
Preferred Learning Modes



Socioeconomic Factors
Background, Access,
Disadvantage Indicators



Institution Data
Programs Offered, Capacity,
Admission Criteria

2. AI PROCESSING & ANALYSIS



Data
Integration



AI Model
Evaluation



Fit & Potential
Analysis



Ranking &
Recommendation



Rank and Bias
Control



Predicts Academic
Success Potential



Matches Applicants
with Suitable Programs



Considers Multiple
Factors Holistically



AI



Ensures Fairness
& Non-Discrimination



Supports Inclusive
Access & Equity



Continuously Learns
& Improves

3. DECISIONS & OUTPUTS



Admit
Applicant is offered admission
to the most suitable institution
or program.



Waitlist / Conditional
Applicant is considered for
future intake or under
specific conditions.



Recommend Alternative
Suggest other suitable
programs or institutions
that better match the
applicant's profile.



Not Admitted
Applicant does not meet the
requirements for available
options.



Every individual,
every talent,
every opportunity.

4. HUMAN OVERSIGHT & TRANSPARENCY



Human review for final decisions



Applicants can appeal or request review



Clear communication of results and reasons



Compliance with data privacy & protection laws

Applicants & Institutions Benefit



Right opportunity
for every
individual



Better student
fit and higher
success rates



Efficient
process and
resource use



Stronger,
inclusive, future-
ready education

Designed for a Better Future

Empowering education and vocational training systems through responsible AI to build skilled, capable and confident individuals and communities.



Equity



Excellence



Opportunity



Progress

Right Person. Right Program. Right Future. | AI for Education. AI for Inclusion. AI for Impact.

- Products with digital elements classified as high-risk AI systems which fall within the scope of the CRA should comply with the essential cybersecurity requirements set out in the CRA.
- Where those high-risk AI systems fulfil the essential cybersecurity requirements set out in the CRA, they should be deemed to comply with the cybersecurity requirements set out in Article 15 of the AI Act in so far as those requirements are covered by the EU declaration of conformity or parts thereof issued under this Regulation.
- For that purpose, the assessment of the cybersecurity risks associated with this product should take into account risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights.

KEY CONCEPT

‘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 12 - CRA

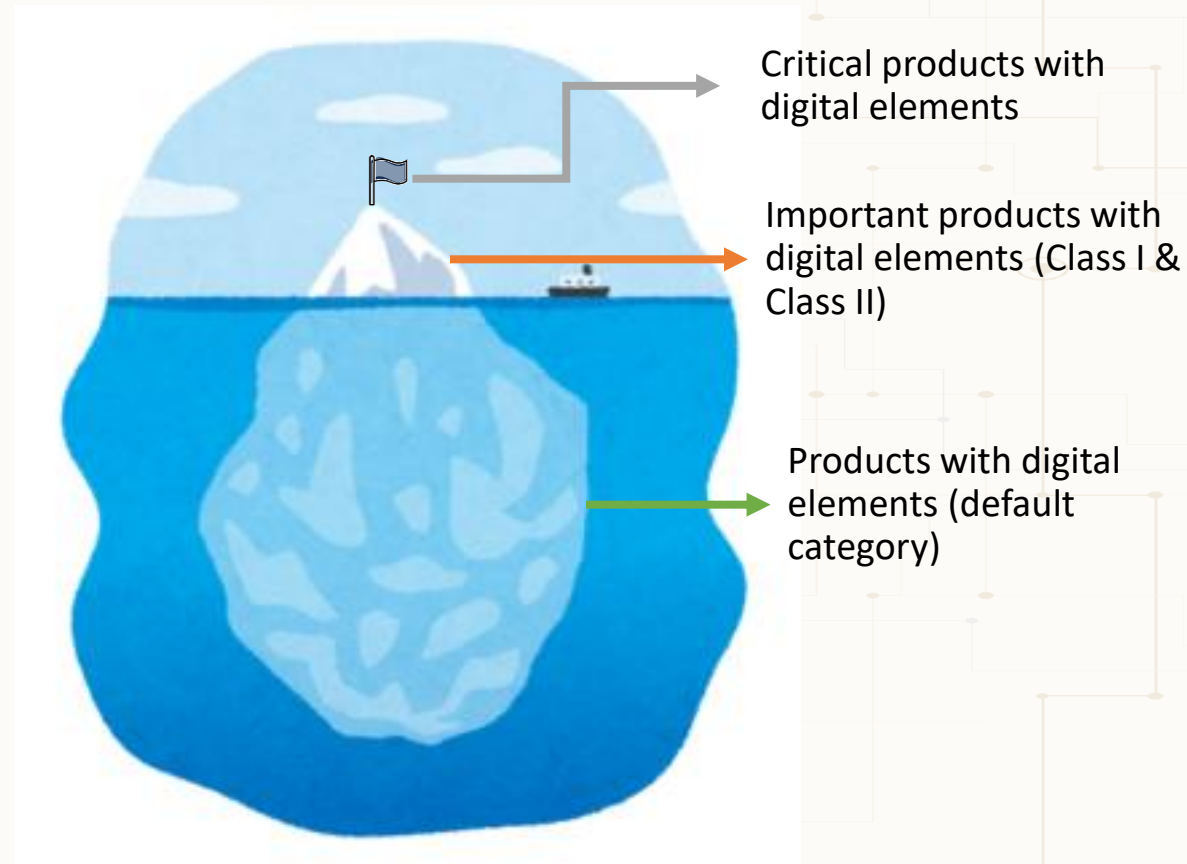
Without prejudice to the requirements relating to accuracy and robustness set out in Article 15 of the AI Act, products with digital elements which fall within the scope of the CRA and which are classified as high-risk AI systems shall be deemed to comply with the cybersecurity requirements (Article 15 AI Act) where:

- (a) those products fulfil the essential cybersecurity requirements set out in Part I of Annex I;
- (b) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I; and
- (c) the achievement of the level of cybersecurity protection required under Article 15 of Regulation (EU) 2024/1689 is demonstrated in the EU declaration of conformity issued under this Regulation.

- For the products with digital elements and cybersecurity requirements the relevant conformity assessment procedure provided for in Article 43 of the AI Act shall apply. For the purposes of that assessment, **notified bodies which are competent to control the conformity of the high-risk AI systems** based on the AI Act **shall also be competent to control the conformity of high-risk AI systems which fall within the scope of the CRA** against the Essential cybersecurity requirements, provided that the compliance of those notified bodies with the requirements of the CRA has been assessed as part of the process of the AI Act.
- **Important products with digital elements**, which are subject to the conformity assessment procedures (internal control procedure and the EU-type examination procedure, a conformity assessment based on full quality assurance or a European cybersecurity certification) and **critical products with digital elements** which are required to obtain a European cybersecurity certificate or, absent that, which are subject to the conformity assessment procedures as above, and which are **classified as high-risk AI systems** and to which the conformity assessment procedure applies, **shall be subject to the conformity assessment procedures provided for in the CRA in so far as the essential cybersecurity requirements set out in the CRA are concerned.**

Classification of Products with Digital Elements

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



Classification of Products with Digital Elements

IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS – CLASS I

2. Standalone and embedded browsers
3. Password managers
4. Software that searches for, removes, or quarantines malicious software
5. Products with digital elements with the function of virtual private network (VPN)
6. Network management systems
7. Security information and event management (SIEM) systems
8. Boot managers

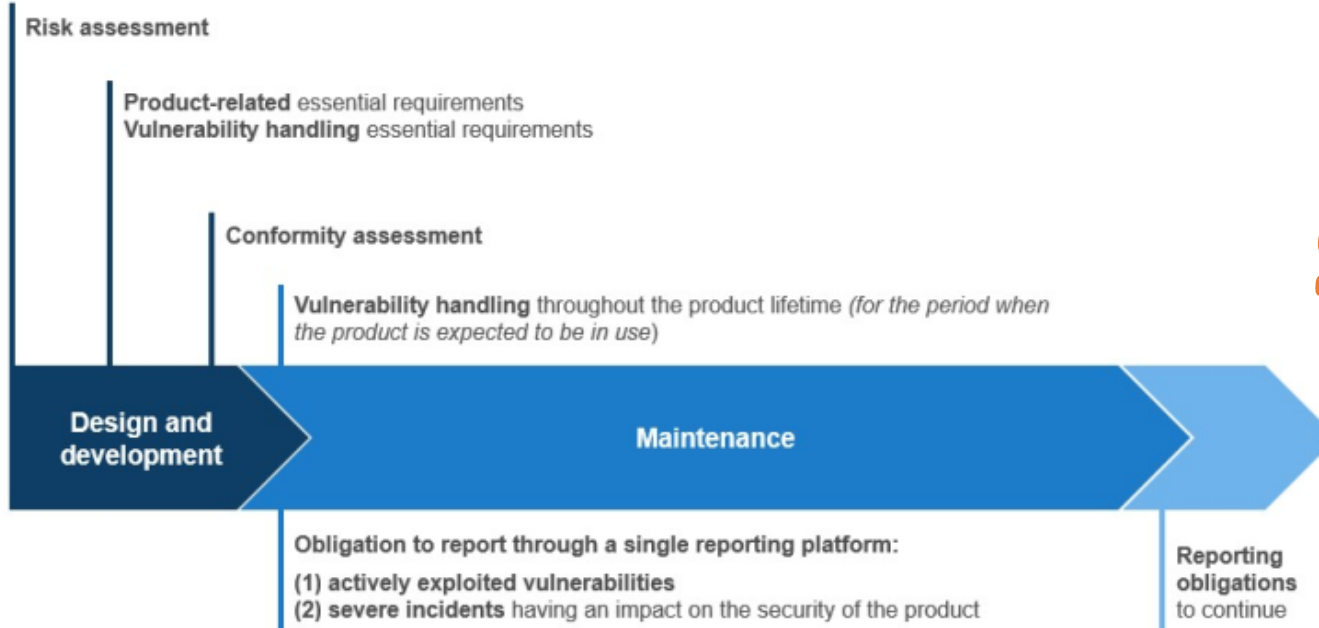
IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS – CLASS II

2. Firewalls, intrusion detection and prevention systems
3. Tamper-resistant microprocessors
4. Tamper-resistant microcontrollers

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

1. Hardware Devices with Security Boxes
2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council ⁽¹⁾ and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements

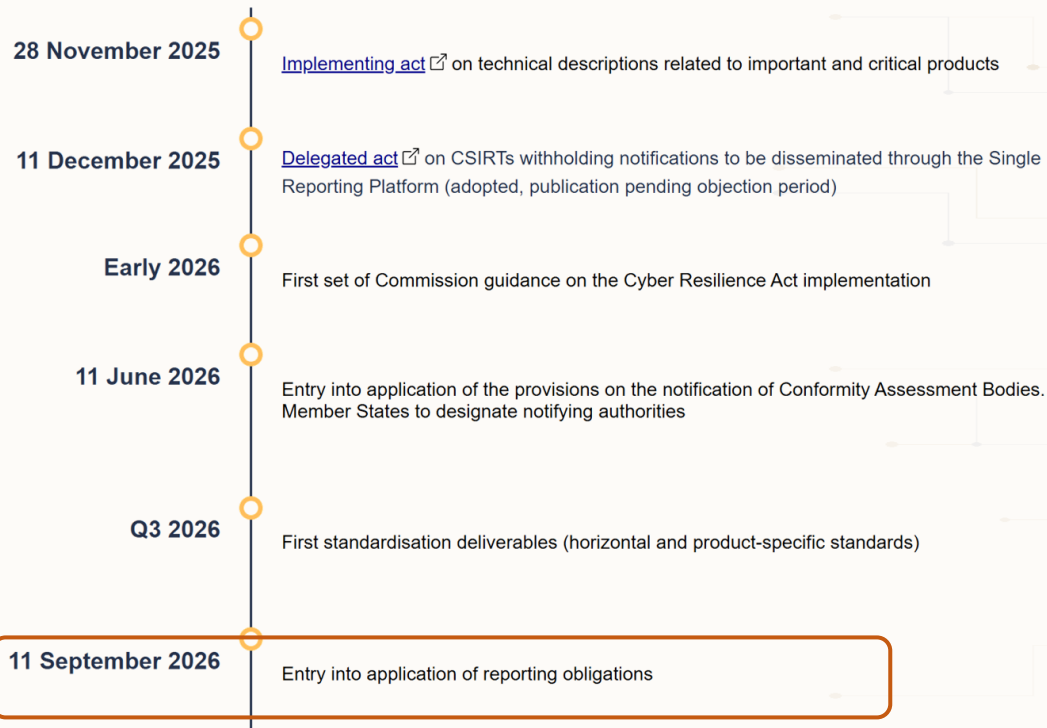
Implementation steps of a manufacturer under the CRA



Conformity assessment under the CRA

	Default	Class I	Class II	Critical
(a) the internal control procedure (based on module A). The manufacturer ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential cybersecurity requirements				
(b) the EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C). Where a notified body examines the technical design and development of a product with digital elements and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential cybersecurity requirements and that the manufacturer meets the essential cybersecurity requirements. EU-type examination shall be carried out by assessing the adequacy of the technical design and development of the product with digital elements through the examination of the technical documentation and supporting evidence referred to in point 3, and the examination of specimens of one or more critical parts of the product (combination of production type and design type).				
(c) a conformity assessment based on full quality assurance (based on module H) The manufacturer operates an approved quality system for the design, development and final product inspection and testing of the products with digital elements concerned and for handling vulnerabilities, maintain its effectiveness throughout the support period, and shall be subject to surveillance.				
(d) where available and applicable, a European cybersecurity certification scheme .				

Timeline

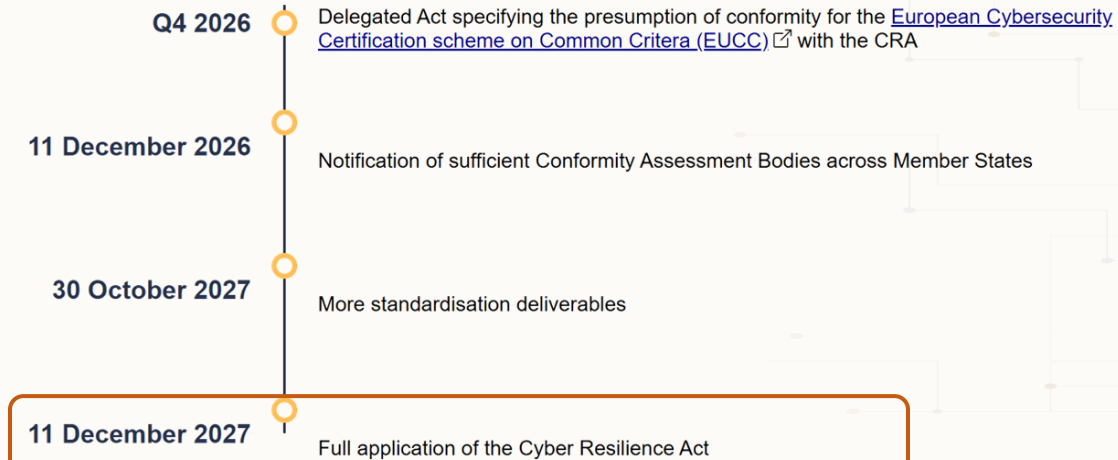


The CRA requires manufacturers to **notify actively exploited vulnerabilities and severe incidents** having an impact on the security of their product with digital elements.

24 hours - early warning
72 hours - a full notification



Timeline



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.

CAC

DPRA

CyReA

PSTVA

DPMA

Penetration Self-Testing and Vulnerability Assessment

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

Training

Digital Product Maturity Assessment

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

Curium Portal

Welcome back! Please sign in to continue.

Username or email

Password

Forgot Password?

☐ Remember me

Sign In

New user? [Register](#)

The CURIUM Continuum products are provided for free.

Would you like to test / use them?

Declare your interest here:



<https://ec.europa.eu/eusurvey/runner/f0d8e5d4-60c4-1cd6-1885-8e9fe8b536c8>

Thank You

We look forward to the conversation.

CONTACT

info@apiroplus.com

www.apiroplus.com



APIROPLUS
SERVICES