

Are your products ready for the EU's Cyber Resilience Act?



EU cybersecurity regulation is moving beyond organisational resilience and into product accountability.

The Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, marks a fundamental shift in EU cybersecurity regulation. CRA introduces the first horizontal, mandatory cybersecurity requirement for all products with digital elements, placing responsibility on manufacturers, authorised representatives, importers and distributors throughout the product lifecycle. Organisations placing products on the EU market will need to demonstrate secure design, vulnerability management, reporting capabilities and ongoing compliance to maintain market access.



Products in scope — illustrative examples¹:

- Default products are in-scope products that are not specifically classified as important or critical.
- Important products (Class I) such as identity and access management solutions, operating systems, routers, modems, smart home security products and (Class II) such as firewalls, intrusion detection and prevention systems
- Critical products such as hardware devices with security boxes, smartcards.

Timeline

11 JUN 2026



Conformity assessment bodies: designation & notification

11 SEP 2026



Incident & vulnerability reporting obligations for manufacturers

11 DEC 2027



Regulation fully applicable

¹. CRA applicability depends on the product's intended purpose, direct or indirect connectivity, EU market placement and any relevant exclusion. A case-by-case assessment may still be required. Final classification depends on the product's functionality and the applicable CRA provisions.

Reporting obligations for manufacturers are already in force:

Since 11 September 2026, manufacturers must report actively exploited vulnerabilities (where reliable evidence shows a malicious actor has exploited them) and severe incidents impacting product security. Notifications are submitted through ENISA's Single Reporting Platform and, where the manufacturer is established in Cyprus, to CSIRT-CY, the CSIRT designated as coordinator by the Digital Security Authority (DSA).

≤24-hour early warning: Notify without undue delay and no later than 24 hours after awareness; the first report serves as an early warning.

≤72-hour follow-up: Provide a more detailed notification and updates.

Final report: For an actively exploited vulnerability due ≤14 days after a corrective or mitigating measure becomes available, while for severe incidents having an impact on the security of products with digital elements due ≤1 month after the 72-hour report submission.

User notification: After becoming aware, manufacturers must also inform impacted users (and where appropriate all users) of the vulnerability or incident and any mitigating or corrective measures, where possible in a structured, machine-readable format.

Implication: The deadline requires a functioning reporting process to be in place before an incident occurs. Parallel reporting obligations may still apply under the Network and Information Security Directive (NIS2), the General Data Protection Regulation (GDPR) or the Digital Operational Resilience Act (DORA).

Overall compliance requirements effective by 11 Dec 2027:

Secure products by design and by default

- Manufacturers must ensure products are designed, developed and produced with cybersecurity integrated from the outset and configured with secure default settings.
- Products must be placed on the market without known exploitable vulnerabilities.
- Protect confidentiality, integrity and availability of data.

Lifecycle vulnerability management

- Manufacturers must continuously identify, assess, remediate and communicate vulnerabilities throughout the support period of products.
- Requirements include managing third-party dependencies and maintaining Software Bills of Materials (SBOMs) where appropriate.

In most cases, product support obligations must be for at least five years unless the product's expected lifetime is shorter. For certain categories of products, support periods may need to extend beyond this minimum threshold.



**PRIORITY
NOW**

Although the full Regulation does not apply until December 2027, compliance preparation should already be underway.

Compliance with the CRA will require organisations to assess product scope, strengthen governance and cybersecurity practices, develop robust vulnerability management processes, and build the documentation necessary to support regulatory compliance.

How KPMG in Cyprus can help



CRA Quick Scan: High-level applicability assessment and initial gap identification.



CRA Applicability & Product Classification: Product-by-product scope assessment, identification of important and critical products and conformity assessment route determination.



CRA Readiness Assessment: Review against requirements to identify gaps and relevant prioritisation roadmap.



Training and Awareness: Targeted awareness and capability-building initiatives.

With reporting obligations already commencing in 2026 and full compliance approaching in 2027, organisations that begin their readiness journey now will be better positioned to manage regulatory expectations, strengthen customer trust and reduce future compliance burdens.

Contact KPMG in Cyprus to discuss how the Cyber Resilience Act may affect your products, services and compliance roadmap.

Main Contacts

Gerasimos Ntouskas

Board Member

IT Consulting

T: +357 22209041

E: gerasimos.ntouskas@kpmg.com.cy

Christoforos Evlavis

Board Member

Risk Consulting

T: +357 22209046

E: Christoforos.Evlavis@kpmg.com.cy

Chloe Karacosta

Senior Manager

Risk Consulting

T: +357 22207475

E: Chloe.Karacosta@kpmg.com.cy

Konstantinos Agathangelou

Manager

IT Consulting

T: +35 722207456

E: konstantinos.agathangelou@kpmg.com.cy

Sandra Zreik

Assistant Manager

IT Consulting

T: +357 22209378

E: Sandra.Zreik@kpmg.com.cy

Iakovos Ellinas

Team member

IT Consulting

T: +357 22207459

E: iellinas@kpmg.com.cy

Christos Georgiou

Team member

IT Consulting

T: +357 22207486

E: chrgeorgiou@kpmg.com.cy

kpmg.com.cy

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

©2026 KPMG Limited, a Cyprus limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.