THE CYBER RESILIENCE ACT

New mandatory cyber security requirements for CE compliance

Who is affected?

Manufacturers, distributors, and importers of products with digital elements

Which products are affected?

Software and hardware products with direct or indirect data connection to another device or network

Which penalties apply?

Up to 15 Mio € or 2.5% of annual turnover

+ potential product recalls

2024 → **2025** → **2026** → **2027**

CRA entry into force
Dec. 2024

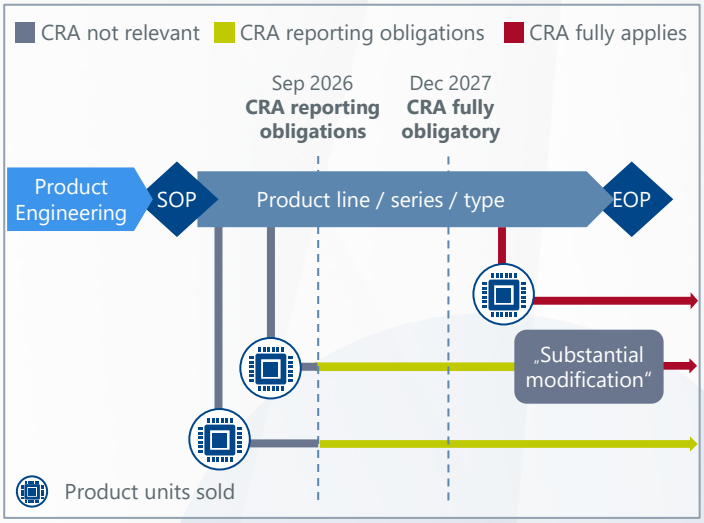
CRA reporting obligations
(Article 14)
11.09.2026

CRA fully obligatory
11.12.2027

Main obligations

- **Risk assessment** of the product
- Implementation of appropriate measures to address the risks & **essential CRA requirements**
- **Vulnerability monitoring & security updates** AFTER product was placed on the market for a time period that is also based on user-expectation
- **Reporting obligations** to CSIRT & ENISA for severe incidents and actively exploited vulnerabilities
- **Documentation requirements** & compliance to sweeps of market surveillance authorities

What about existing products?



Excluded sectors

- Medical devices (MDR)
- Road vehicles (UN R155)
- Aviation & marine equipment
- National security & military
- Non-commercial OSS
- XaaS / cloud services (→ NIS2)

itk ENGINEERING

ITK Engineering GmbH
Headquarters Ruelzheim
Im Speyerer Tal 6
76761 Rülzheim, Germany

Tel.: +49 (0)72727703-0
cybersecurity@itk-engineering.de

www.itk-engineering.com

Follow us on:

ITK's CRA SERVICES

Experience-based, pragmatic & tailored to your needs

From SMEs to large companies: We have already helped customers of various sizes and with different challenges to find customized solutions that hit the sweet spot in terms of pragmatism, required effort, structure, and consistency.

CYBER SECURITY ENGINEERING FOR CRA

Risk assessments
Determine the „appropriate level" of cyber security for your product and only invest where it counts.

Cyber security concepts
Select appropriate countermeasures and meet the essential requirements of the CRA.

Cyber security development
Have experts help you with cyber security technologies (e.g. cryptography, secure booting, secure updates, etc.).

Penetration testing
View the product from the attacker's point-of-view and satisfy CRA testing obligations.

CYBER SECURITY CONSULTING FOR CRA

CRA gap analysis & roadmap
Identify what's missing for CRA compliance and how to get there.

Program management
Align all relevant stakeholders: from C-level cyber security policy to supplier management, engineering and production.

Supplier management
Coordinate cyber security requirements with your suppliers and ensure they help you meet your CRA obligations.

SBOM & vulnerability management
Create SBOMs and continuous monitor / triage for vulnerabilities (e.g., via CVE).

Reporting obligations & incident management
Setup and align processes that allow you to react fast once it counts.

Trainings
Everything we consult, we can develop – or train! Let us coach your teams in presence, interactive or on-the-job.

LEARN MORE ABOUT OUR SERVICES AND CUSTOMER REFERENCES.

itk ENGINEERING

ITK Engineering GmbH
Headquarters Ruelzheim
Im Speyerer Tal 6
76761 Rülzheim, Germany

Tel.: +49 (0)72727703-0
cybersecurity@itk-engineering.de

www.itk-engineering.com

Follow us on: