

EU Cyber Resilience Act

The **EU Cyber Resilience Act** sets **mandatory cybersecurity standards** for all products with digital elements like software, IoT devices, and connected systems sold in the EU. It covers the entire product lifecycle to prevent vulnerabilities and ensures ongoing protection against cyber threats.

Who must comply?

Any business placing **"products with digital elements"** on the EU market, including **hardware, software, networked systems** in vehicles, appliances, or critical infrastructure and even **open-source** or **free products** with digital functions.



SECURE DESIGN & DEVELOPMENT



DEFAULT SECURITY



TRANSPARENCY



VULNERABILITY HANDLING

OBLIGATIONS TIMELINE

IN FORCE
DECEMBER 11
2024

REPORTING
SEPTEMBER 11
2026

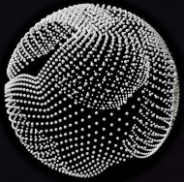
COMPLIANCE
OCTOBER 11
2026
TYPE A,B,C

FULL RULES
DECEMBER 11
2027



IMPACT ASSESSMENT & ROADMAP

We will map CRA requirements to your environment including supply chain to identify high-risk areas early. Our experts will then develop a tailored roadmap with clear milestones, timelines, and priorities to achieve compliance efficiently while supporting your growth objectives.



SUPPORT IN READINESS & CERTIFICATION

We will conduct a thorough gap analysis against CRA, helping you build detailed documentation. Our team will guide and support you through every step of the process, from self-evaluation to third-party audits, vulnerability management, preparing your products for successful certification and ongoing surveillance readiness.



GOVERNANCE INTEGRATION

We will design and implement CRA-aligned security policies, technical controls, and processes that integrate seamlessly into your daily operations. Additionally, we will strengthen vendor management frameworks and incident response plans to handle vulnerabilities proactively and maintain long-term compliance across your organization.

CONTACT US

If you want to understand how the **Cyber Resilience Act** affects your organisation, or if you need a structured approach to **compliance readiness**, do not hesitate to get in touch and discuss how we can support your organisation.



Ratko Drca,
Director
rdrc@deloittece.com



Donika Dimov,
Senior Manager
ddimov@deloittece.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTL and each DTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTL), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTL and each of its member firms, and their related entities, are legally separate and independent entities.