



Cyber Resilience Act (CRA) Deloitte Cyber Regulatory Compliance

For companies **selling products with digital components in the EU**, the CRA brings **new obligations** related to managing **cybersecurity risks**, detecting and addressing vulnerabilities, securing the supply chain, and reporting incidents. A wide range of products are affected, including:



**IoT
Devices**



**Network
Components**



**Remote Data
Processing
Solutions**



**Specialized
Industrial Systems**

With the introduction of the CRA, businesses are now required to meet **stricter security standards**, and failing to comply could lead to significant consequences.

The CRA is a regulation proposed by the European Union to ensure that **products with digital components** – such as software, smart devices, and connected equipment – are **secure by design** and **secure by default**. It applies to **importers, manufacturers, and distributors operating in the EU market**.

Who does it affect?

- › **Manufacturers of software and hardware**
- › **Importers & distributors** placing digital products on the EU market
- › **Organizations integrating third-party components** into product they place on the EU market
- › **Open-source** software stewards

Non-compliance risks

- › Fines of up to **€15 million** or **2.5% of global annual turnover**
- › **Product recalls or bans**
- › **Reputational damage** and legal liability

Key requirements



Security by Design

Cybersecurity features at every development stage, SBOM and mandatory support period



Vulnerability Management

Ongoing monitoring, testing, and patching



Transparency

Clear instructions for use, maintenance, and risk mitigation



Vulnerability & Incident Reporting

Notify CSIRTs and ENISA of vulnerabilities and exploited vulnerabilities



Conformity Assessment

Important and Critical products require third-party evaluation

Key milestones

September 2026 – Mandatory reporting of incidents and vulnerabilities will begin

December 2027 – Full implementation of the CRA, all products must meet the requirements

Given these timelines, it is crucial to start preparing **as soon as possible** to implement relevant processes and necessary security measures.

Our team of **experts in cybersecurity, regulatory compliance, law, and risk management** will help you **meet all CRA requirements**.



Product Portfolio Analysis

We assess your offerings to pinpoint CRA-regulated digital products



Conformity Assessment & Documentation

We support technical documentation and preparation for CRA conformity assessment



CRA Readiness & Gap Analysis

We benchmark your current state against CRA requirements



Vulnerability & Update Management

We help you manage security updates and handle vulnerability disclosures effectively



Corrective Actions

We propose clear, prioritized steps to close compliance and security gaps



Supply Chain & Third-Party Security

We implement security standards across suppliers and external partners



Implementation Support

We guide you in applying Security by Design and by Default principles



Expert Guidance & Methodology

We provide ongoing expert support throughout the CRA compliance process

Contact Us

Jakub Höll, Partner
jholl@deloittece.com



Marek Fišer, Manager
mfisher@deloittece.com

