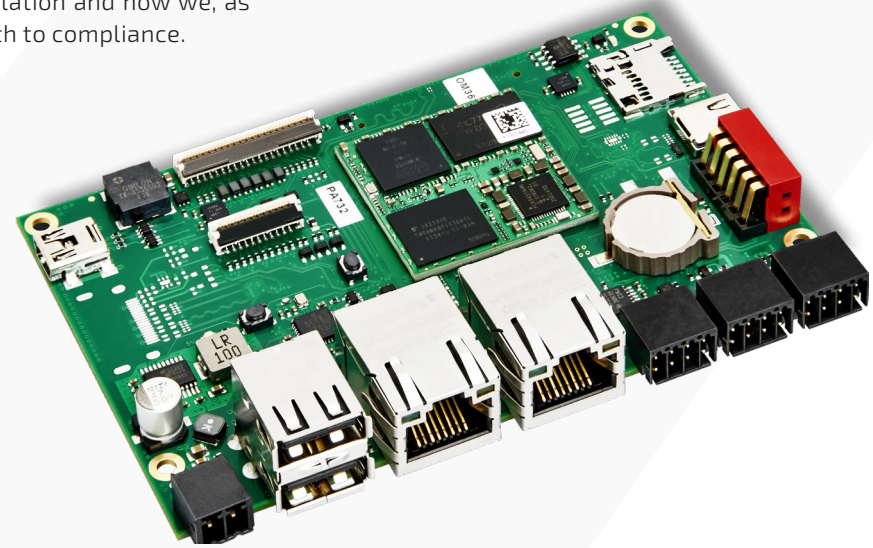
Whitepaper

Cyber Resilience Act (CRA)

What companies need to know and do now

Your guide to the EU Cybersecurity Regulation and how we, as an IoT specialist, support you on your path to compliance.



15 MILLION EUR

› maximum fine for non-compliance

DEC. 2027

› Full applicability

> 90%

› of all digital products affected

kontron

The Power of IoT

Executive Summary

The Cyber Resilience Act (CRA) is the first EU-wide regulation to establish binding cybersecurity requirements for all products with digital elements. It applies equally to manufacturers, importers, and distributors.

At a glance: Key facts about the CRA

- Applies to all products with digital elements placed on the EU market
- Manufacturers must ensure cybersecurity throughout the entire product lifecycle
- Fines of up to EUR 15 million or 2.5% of the previous year's global annual turnover
- Full applicability from December 2027
- Now is the time to act!

1. Background: Why the CRA?

Ransomware, supply chain attacks, and vulnerabilities in connected devices cause billions in damage every year. At the same time, there has been no consistent EU-wide standard to ensure that products are secure when placed on the market.

The CRA closes this gap. It complements existing regulations such as the NIS2 Directive and establishes a binding framework for product cybersecurity.

1.1 What is the Cyber Resilience Act?

The Cyber Resilience Act was published in the Official Journal of the EU in October 2024 and entered into force in December 2024. It establishes harmonized cybersecurity requirements for products with digital elements for the first time. These range from smart home devices and industrial control systems to software.

1.2 Who is affected by the CRA?

The CRA generally applies to all economic operators within the supply chain:

MANUFACTURERS	Bear primary responsibility, including conformity assessment, CE marking, technical documentation, and vulnerability management.
IMPORTERS	Ensure that only compliant products are placed on the EU market.
DISTRIBUTORS	Verify that products comply with CRA requirements before being made available on the market.
OPEN-SOURCE DEVELOPERS	Largely exempt, provided there is no commercial activity involved.

2. Timeline & Key Milestones

Companies should begin implementation now, as conformity assessments and technical documentation require significant lead time.

DATE	MILESTONE	DESCRIPTION
DEC. 2024	Entry into force	CRA officially enters into force
SEP. 2026	Reporting obligations	Reporting obligations for actively exploited vulnerabilities apply
DEZ. 2027	Full applicability	All requirements become fully applicable

Although full applicability only takes effect in December 2027, companies should begin implementation no later than mid-2026, as conformity assessment procedures can take several months.

Products placed on the market before December 2027 may be treated under transitional provisions, subject to certain conditions.

3. Key Requirements at a Glance

The CRA defines fundamental cybersecurity requirements in Annex I and Annexes II–IV. These can be grouped into three main areas:

3.1 Security by Design

Manufacturers must ensure that products are designed and developed with an adequate level of cybersecurity. This includes:

- Reduction of the attack surface
- Protection against unauthorized access, including authentication mechanisms
- Encryption of sensitive data both in transit and at rest
- Secure default configurations
- No known exploitable vulnerabilities at the time of market entry
- Minimization of dependencies on third-party components (including open source)

3.2 Vulnerability Management Across the Lifecycle

Manufacturers are required to provide security updates for at least five years (or the expected product lifetime). This specifically includes:

- Reporting actively exploited vulnerabilities to ENISA and national authorities within 24 hours
- Sharing relevant information with affected users
- Provision of security updates

3.3 Transparency & Documentation

Manufacturers must create comprehensive technical documentation and maintain a Software Bill of Materials (SBOM):

- Software Bill of Materials (SBOM) covering all components, libraries, and dependencies
- Technical documentation in accordance with Annex VII of the CRA
- EU Declaration of Conformity and CE marking
- Clear user information on cybersecurity features and updates

4. Product Categories & Risk Classification

The CRA distinguishes between standard products and critical products. The higher the risk class, the stricter the conformity assessment:

CATEGORY	EXAMPLES	CONFORMITY ASSESSMENT PROCEDURE
STANDARD PRODUCTS (DEFAULT)	Smart TVs, printers, smart home devices	Manufacturer self-assessment
CRITICAL CLASS I	Password managers, firewalls, routers	Harmonized standards or third-party assessment
CRITICAL CLASS II	Industrial SCADA, PKI, hardware security modules (HSM)	Certification by an accredited body

5. Penalties & Consequences of Non-Compliance

The CRA provides for significant sanctions. Market surveillance authorities can withdraw non-compliant products from the market and impose substantial fines:

INFRINGEMENT	MAXIMUM FINE
Violations of essential cybersecurity requirements	EUR 15 MILLION OR 2.5% OF TOTAL WORLDWIDE ANNUAL TURNOVER
Violations of other obligations (e.g. reporting obligations)	EUR 10 MILLION OR 2% OF TOTAL WORLDWIDE ANNUAL TURNOVER
Providing false or misleading information to authorities	EUR 5 MILLION OR 1% OF TOTAL WORLDWIDE ANNUAL TURNOVER

6. What Companies Need to Do Now

CRA compliance is not a one-time project, but an ongoing process. We recommend the following structured approach:

Step 1: Inventory & Gap Analysis (start immediately)

- Identify all digital products and components
- Determine the CRA risk classification for each product
- Assess existing security measures against CRA requirements
- Identify missing documentation (SBOM, technical documentation)

Step 2: Organizational Measures

- Establish internal vulnerability reporting processes (24-hour reporting chain)
- Clearly define responsibilities for product security
- Conduct training for development and compliance teams

Step 3: Technical Implementation

- Integrate security by design into development processes
- Implement SBOM tooling and create a complete inventory of all software dependencies
- Establish patch and update management processes
- Conduct penetration testing and security assessments

Step 4: Conformity Assessment & Certification (from Q3 2026)

- Prepare technical documentation in accordance with Annex VII
- Issue the EU Declaration of Conformity
- Affix the CE marking
- Engage an external certification body if required (for Class I/II)

7. How We Support as an IoT Specialist

We offer our customers and partners a comprehensive portfolio of support services:

SERVICE	DETAILS
SECURE HARDWARE BY DESIGN	Tamper-resistant modules, secure boot, HSM integration
PATCH & UPDATE MANAGEMENT	Signed firmware updates, remote management capabilities
TRANSPARENCY & DOCUMENTATION	SBOM support, CE documentation, technical documentation
VULNERABILITY MANAGEMENT	Coordinated disclosure, 24-hour reporting support, hotfix processes
CERTIFICATION & COMPLIANCE	Preparation for EU conformity assessment, audit support
TRAINING & CONSULTING	CRA readiness workshops, gap analysis, roadmap development

7.1 Secure Hardware as the Foundation of Your Compliance

Cybersecurity starts at the hardware level. Our products are designed from the ground up according to the principle of "security by design" and provide the following security-relevant features:

Hardware Security Features

- Secure boot & Trusted Platform Module (TPM)
- Hardware security module (HSM) integration
- Tamper detection & physical protection
- Isolated security zones (TrustZone)
- Hardware acceleration for cryptographic applications

Software & Update Infrastructure

- Signed firmware & over-the-air (OTA) updates
- Rollback protection & version management
- Remote device management
- Secure storage of keys
- Automated security checks within the build process

7.2 Transparency & SBOM Support

The Software Bill of Materials (SBOM) is one of the key requirements of the CRA. We support you in establishing a complete and up-to-date SBOM:

- Delivery of our products with a complete component SBOM in SPDX or CycloneDX format
- Regular SBOM updates for changes in firmware or software
- Support in setting up your own SBOM processes within your supply chain

7.3 Vulnerability Management & Reporting Processes

Our vulnerability management supports you in complying with the strict reporting requirements of the CRA:

- Proactive notification of newly identified vulnerabilities in our products
- Prioritized provision of security patches for critical vulnerabilities
- Support in communication with ENISA and national authorities

About Kontron

Kontron AG is a leading IoT technology company. For more than 20 years, Kontron has been supporting companies from a wide range of industries to achieve their business goals with intelligent solutions. From automated industrial operations, smarter and safer transport to advanced communications, connectivity, medical, and energy solutions, the company delivers technologies that add value for its customers. With the acquisition of Katek SE in early 2024, Kontron significantly strengthens its portfolio with the new GreenTec division, focusing on solar energy and eMobility, and grows to around 8,000 employees in over 20 countries worldwide. Kontron is listed on the SDAX® and TecDAX® of the German Stock Exchange.

For more information, please visit: **www.kontron.com**

About Kontron Electronics

Kontron Electronics GmbH is a full-service provider in the field of electronics, development and manufacturing services. Our business portfolio includes proprietary and client-specific products, development and design services for complex electronics components, modules and systems, as well as production and assembly services for entire devices. The company is part of the technology corporation Kontron AG.

For more Information please visit: **www.kontron-electronics.com**

Your Contact

Kontron Electronics GmbH

Max-Planck-Straße 6
72636 Frickenhausen, Germany
Tel.: +49 7022 4057-0
info@kontron-electronics.de

www.kontron-electronics.com

Global Headquarters

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: +49 821 4086-0
info@kontron.com

www.kontron.com

kontron
The Power of IoT