NewTec Services

Creating safety.
With passion.

NewTec

The Cyber Resilience Act (CRA) is in force.

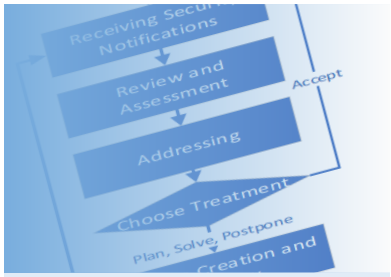
CRA: The requirements are now binding. What obligations do you have as a manufacturer?

The Cyber Resilience Act (CRA) aims at the cybersecurity of networkable products to a high and uniform level both across the EU and across products. Moreover, it aims at improving the transparency of security features. It is a cross-sectoral regulation which covers not only all areas of cybersecurity but also all products which are able to establish a data connection to a network or another product.

Manufacturers must carry out a cybersecurity-related risk assessment for every product "with digital elements". Furthermore, manufacturers must take 'the result of this assessment into account in the planning, design, development, manufacturing, supply and maintenance phases of the product' (Art. 10 para. 2). The requirements therefore apply to the entire life cycle. In addition, manufacturers must implement risk management and effective vulnerability management. Reporting obligations with tight deadlines apply to actively exploited vulnerabilities and serious security incidents. They must also provide updates and patches to fix the vulnerabilities (Annex I, Part I, para. 2c).

When does the Cyber Resilience Act apply?

At the end of 2023, the European Commission, the European Parliament and the Council of the European Union agreed on the final text of the Cyber Resilience Act. It was published in the Official Journal of the EU on 20 November 2024 and came into force on 10 December 2024. However, in order to give companies time for the transition, the requirements do not have to be implemented with immediate effect. From 11 June 2026, the conformity assessment bodies will be authorised to assess CRA conformity. From 11 September 2026, manufacturers will be subject to the obligation to report vulnerabilities and incidents. From 11 November 2027, all requirements will apply in full.



Regulations & Standards

We assist in fulfilling CRA-conformity on the basis of these standards:

- ISA/IEC 62443 – Industrie
- ETSI EN 303 645 – Consumer IoT
- EN ISO/IEC 27xxx – IT-Security
- IEC 63452 – Railway
- etc.

NT SECURITY SOLUTIONS

NewTec GmbH Buchenweg 3 89284 Pfaffenhofen a.d. Roth Tel.: + 49 7302 9611-0 info@newtec.de **www.newtec.de**

Phases of security product development according to CRA

Managing the CRA: NewTec services to fulfill the legal requirements

NewTec supports manufacturers in the CRA-compliant development of products with digital elements - for example with a threat and risk analysis in accordance with the Cyber Resilience Act, the integration of security measures or the implementation of secure update processes as well as comprehensive security testing. Our experts work with you to assess your current situation, provide help with classification and support the introduction of necessary processes and secure operation.

Enablement of your organisation:

- **CRA GAP analysis:** Maturity assessment of the development and support processes
- Implementation of **CRA-compliant processes**
- **Documentation** in accordance with CRA
- **Workshops and trainings** to build up security awareness and know-how

CRA-compliant product development

- **Product classification**
- Creation of a **cyber security management plan**
- **Development and documentation** in accordance with CRA
- **Risk analyses** during the entire product life cycle (TARA, IRA, DRA)
- Development of **secure update strategies**
- Consultancy and support with **CRA compliance testing**

Secure operation/ incident management

- Automated **vulnerability monitoring**
- **Vulnerability management**
- **Update management**
- Support in the form of a customised **Product Security Incident Response Team (PSIRT)**
- Provision of a **public key infrastructure (PKI)**

NewTec GmbH Buchenweg 3 89284 Pfaffenhofen a.d. Roth Tel.: + 49 7302 9611-0 info@newtec.de **www.newtec.de**

MKT094TE_0325