Overview

The Cyber Resilience Act (CRA)

The future of cybersecurity for digital products

Find out more about

- Definition of the Cyber Resilience Act (CRA)
- Who does it affect?
- When will the CRA be implemented?
- Implementation of the CRA at Phoenix Contact
- Further information
- Contact

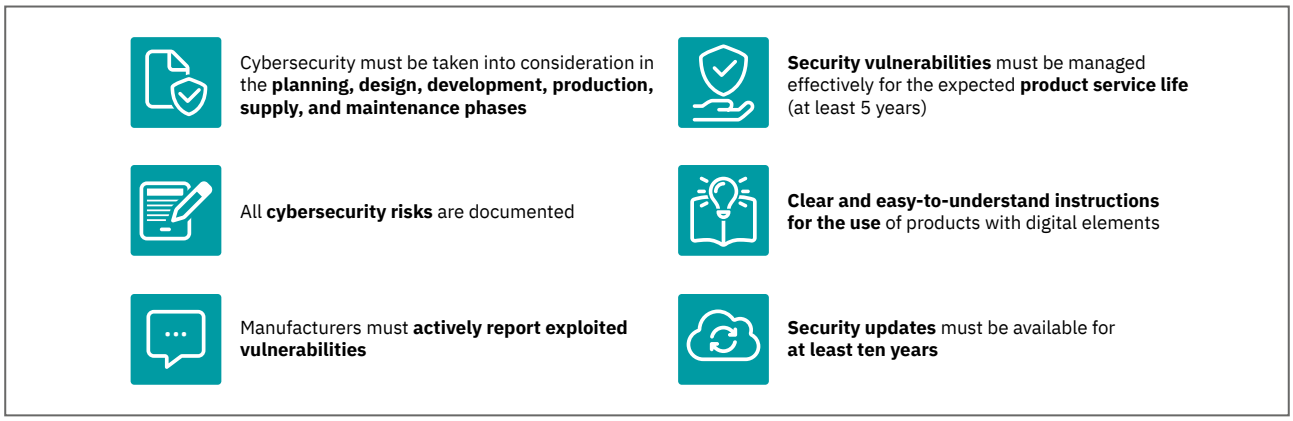
The Cyber Resilience Act (CRA) represents a groundbreaking development in the field of cybersecurity. It defines clear obligations for manufacturers of digital products, in particular with regard to the implementation of security-by-design.

This document takes a look at the challenges and opportunities that the CRA presents for manufacturers, considers the role of the IEC 62443 international security standard as a key player in this context, and describes how Phoenix Contact will meet the requirements of the CRA in the future.

Definition of the Cyber Resilience Act (CRA)

The European Cyber Resilience Act (CRA) requires manufacturers to develop products in accordance with security standards. In the future, products subject to the CRA will no longer receive CE marking or be made available on the market unless they comply with the legal regulations.

The legal text places particular emphasis on aspects such as access protection, confidentiality, integrity, and availability, which must be integrated into the entire development process. It is the first regulation worldwide to define security requirements for products as a barrier to market entry.



Requirements of the Cyber Resilience Act

Who does it affect?

The Cyber Resilience Act (CRA) applies to all manufacturers, importers, and distributors of “products with digital elements” and is mandatory for CE marking. “Product with digital elements” refers to both hardware and software that has communication capabilities.

Conversely, this means that non-compliant products are not allowed to be placed on the market. The supplier must also withdraw from the market any existing products that do not meet the cybersecurity requirements.

The Cyber Resilience Act categorizes products with digital elements into four risk classes depending on their function, intended use, and criteria such as the extent of potential impact.

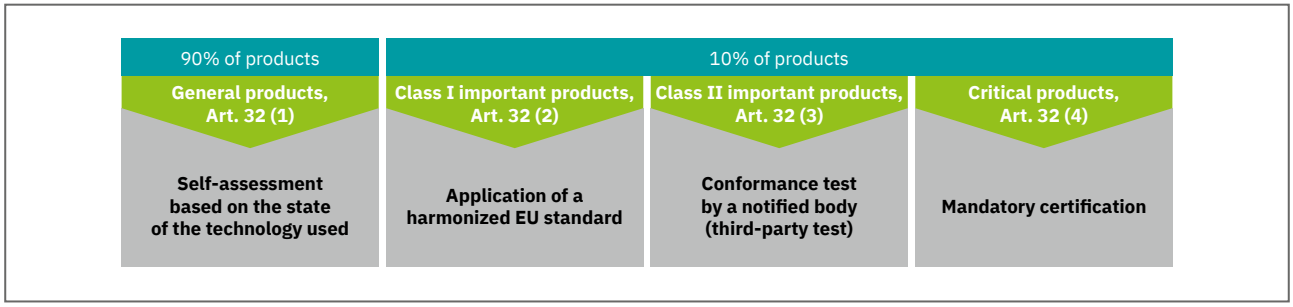
- **Non-critical products** such as storage media and graphics programs
- **Class I critical products** such as browsers or password managers
- **Class II critical products** such as routers, IoT devices, or firewalls for industrial use
- **Highly critical products** affect the resilience of the entire supply chain, such as smart cards or smart meter gateways.

Certain legal requirements apply to each category: While self-declaration based on the state of the technology will be sufficient for non-critical products in the future, harmonized European standards must be applied for Class I products. If this is not the case or if the product is categorized as Class II, a notified body must be involved.

The European Commission estimates that around 90% of products fall into the non-critical category. Market surveillance authorities are monitoring the expected implementation. In Germany, the Federal Office for Information Security (BSI) is responsible for this task.

For users, the CRA means that all available products will meet higher security standards and pose fewer risks from hackers, security vulnerabilities, or other threats.

Manufacturers are also required to maintain the products throughout their entire lifecycle and to provide automatic security updates. Users can therefore rely on the cybersecurity guarantees of CE-marked products.



The CRA categorizes products with digital elements into four risk classes

When will the CRA be implemented?

The first draft text of the CRA was published in September 2022. On March 12, 2024, the European Parliament approved the provisional text (517 votes in favor, 12 against, 78 abstentions). And the European Council also gave its approval for the CRA on October 10, 2024. The agreement will come into force after a transitional period of 36 months.

When the CRA comes into force, it will apply with immediate effect in all EU member states. As an EU act, it does not have to be transposed into national law. Manufacturers must therefore meet the requirements of the CRA from late 2027.

Implementation of the CRA at Phoenix Contact

Although the CRA grants manufacturers a transition period of 36 months, when you consider the complexity of security standards or laws, it quickly becomes clear that there is an immediate need for action. Cybersecurity is no longer an option, but a necessity.

To ensure compliance with these high requirements, such as the implementation of a secure development process, it is helpful to use international standards as a basis. One such example is the IEC 62443 series of international standards. It is the leading standard for implementing security-by-design in products and systems. And fundamental requirements, as defined by the CRA, are covered by the secure development process in accordance with IEC 62443-4-1 along with the functional specifications in accordance with IEC 62443-4-2.

Phoenix Contact began implementing IEC 62443 in 2017. We use a comprehensive 360° security concept, which implements the guiding principle “Security is anchored in the entire lifecycle of our products and solutions”.

Our products will be CRA-compliant by the deadline. Where possible, conformity shall be achieved by means of new firmware. If conformity cannot be achieved, we will offer new, compatible products wherever possible.

Comprehensive protection thanks to our 360° security concept

Secure products are already being developed in accordance with the IEC 62443-4-1 standard, while also satisfying the requirements for security functions in accordance with IEC 62443-4-2.

The Product Security Incident Response Team (PSIRT) is responsible for the effective handling of vulnerabilities. This strategy has meant that Phoenix Contact is well positioned to meet the new legal requirements.

Our 360° security concept has all the relevant IEC 62443 certifications. We offer our customers secure products and certified development processes, certified solutions, services, and selected partners.

Further information

Further information on our 360° security concept:
phoenixcontact.com/cybersecurity

Further information on the CRA:
phoe.co/CRA

Contact

Lutz Jänicke
Corporate Product & Solution Security Officer
ljaenicke@phoenixcontact.com

phoenixcontact.com

2024-09-10/00
3012107875