TÜVIT

CRA

Guidance: A Product Manufacturer's Path to Comply with the Cyber Resilience Act

TÜV®

TÜVNORDGROUP

Table of contents

1. Time to Act 3

2. Cyber Resilience Act at a Glance 3

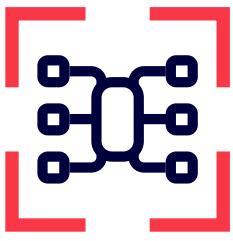
3. Deadlines You Need to Know 4

4. CRA Essential Requirements 4

5. Mapping Manufacturers' Obligations to Related TÜVIT Services 5

6. Product Classes 6

7. Conformity Assessment Procedures of the CRA 7



1. Time to Act

The EU Cyber Resilience Act (CRA), which came into force at the end of 2024, poses significant challenges for almost all parties involved. This is particularly true for manufacturers of products with digital elements (PwDE) who wish to place their developments on the EU market from the end of 2027 onwards or already do so. While fixed deadlines for proving compliance reduce the preparation time for manufacturers on a weekly basis, testing and certification bodies also still need to adapt to their new role. In addition, harmonized evaluation standards for certain product classes are still under development. This dynamic increases overall complexity. But how can manufacturers deal with this and still prepare themselves?

In our guide, we provide a brief overview of the truly essential content of the new legislation. At the heart of the document is a mapping of requirements from the CRA and corresponding modular service components with which TÜVIT can help affected manufacturers to prepare and achieve CRA compliance as well as to meet relevant deadlines.

The right time to start fulfilling the CRA obligations is now. Contact us as a trusted IT security service provider and start your pathway to compliance.

2. Cyber Resilience Act at a Glance

The Regulation (EU) 2024/2847 known as the Cyber Resilience Act will be mandatory for EU type examination procedures from 12 November 2027 onwards. It establishes essential cybersecurity requirements (ESR) that manufacturers must comply with during the design, development and production of their products with digital elements. These requirements also apply during the operational phase, i.e., while products are in use.

The CRA entered into force on 10 December 2024 and will be fully applicable as of 11 December 2027. The CRA defines “products with digital elements” (PwDE) broadly, ranging from consumer IoT to professional IT systems, and industrial control systems used in critical infrastructure and essential services as defined in NIS-2. Before placing the product on the market, the manufacturer must carry out conformity assessment procedures in accordance with their classification, then draw up the EU declaration of conformity and affix the CE marking to its product.

The CRA is directly linked to further directives such as EU NIS-2 Directive, the European framework for entities and operators of critical infrastructures, and the Radio Equipment Directive (RED) 2014/53/EU, in areas covered by the CRA in December 2027.

3. Deadlines You Need to Know

11 September 2026

Manufacturers must report vulnerabilities that are actively exploited and serious security incidents on the the central CRA reporting platform.

Applies to:
All products with digital elements (PwDE) without exception, including pure software products.

11 December 2027

Manufacturers must comply fully with the CRA.

Applies to:
- All PwDE placed on the market for the first time after this date.
- All PwDE that were already available before the CRA came into force and have been substantially modified after this date.

4. CRA Essential Requirements

The CRA sets a range of essential requirements (ESRs) which should be understood as minimum security requirements for products to be secure during use and operation. These requirements address product design as well as operational requirements before placing the product on the market.

Most products, such as household appliances, computer games, and mobile applications will be subject to a self-assessment by the manufacturer. However, for certain products deemed important or critical, manufacturers will have to apply harmonized standards and/or undergo an assessment by a third party called a notified body (a conformity assessment body that is notified under the CRA). Harmonized standards under the CRA will be published progressively before 2027 and are not yet available. However, these standards will be largely based on existing and commonly accepted standards.

The CRA Annex III and IV list essential and critical products with digital elements based on their definitions in Articles 7 and 8. The CRA requires a risk assessment that will help categorize the product and associated requirements. High-risk ones are those whose failure or compromise could endanger critical infrastructure and essential services.

Adopt currently available standards. Harmonized standards under the CRA will be published progressively before 2027. Companies already aligned with ETSI EN 303 645 and IEC 62443, or already operating under EUCC-related conformity assessment schemes, will typically only require minor adjustments to achieve CRA alignment.

5. Mapping Manufacturers' Obligations to Related TÜVIT Services

	OBLIGATIONS:	TÜVIT SERVICE-MODULES:
1. PRE-MARKET OBLIGATIONS	**Product Categorization** CRA Annex III and IV based on definitions in Article 7 and 8	▪ **CRA Scoping Workshop for Starters** CRA insights and guidance on embarking on the right path to achieve and demonstrate conformity ▪ **Seminar: Cyber Resilience Act (CRA)** TÜV NORD Akademie
	Risk Analysis	▪ **Enabling Workshop "Threat & Risk Analysis"** Enabling manufacturers for self risk and threat assessments of their PwDE ▪ **3rd-Party Threat & Risk Analysis** Bundling the relevant set of PwDE-specific security requirements as a basis for the implementation of suitable security measures
	Implementation of Security Measures CRA Annex I based on definitions in Article 13 and 14	▪ **Gap Analysis** Ascertain the maturity level of your implementations and advise on closing the gaps before starting the certification phase ▪ **Pre-Penetration Testing as Technical Quality Gate for Self Assessment** Reliable security expert report of an independent testing lab
	Demonstration of Conformity CRA Annex VIII based on definitions a. o. in Article 32	▪ **Evaluation of important PwDE Class I and II** Certification readiness based on an evaluation of a notified evaluation body (TÜVIT) according to EUCC or dedicated harmonised Standards (hEN) currently under development based on e.g. IEC 62443, ETSI EN 303 645. Certification by TÜV NORD ▪ **Evaluation of Critical PwDE** Certification readiness based on an evaluation of a notified evaluation body (TÜVIT) according to EUCC or dedicated harmonised EU Standards (hEN). Certification by TÜV NORD
	CRA Compliance Readiness	
2. POST-MARKET OBLIGATIONS	**Continuous Compliance with Requirements Throughout the Entire Support Period**	▪ **Re-Evaluation of important PwDE Class I and II** Comply with the Post-Market Obligations, in case of your certificate expires, in the event of significant changes of PwDE or, if necessary, after security vulnera-bilities have been eliminated. Re-Certification by TÜV NORD ▪ **Re-Evaluation of Critical PwDE** Comply to the Post-Market Obligations, in case your certificate expires, in the event of significant changes to PwDE or, if necessary, after security vulnerabilities have been eliminated. Re-Certification by TÜV NORD
3. REPORTING OBLIGATIONS	**Reporting Vulnerabilities and Security Incidents** a. o. in Article 14	▪ **Vulnerability Management** Cyclical security checks such as penetration tests, darknet and SBOM monitoring to detect vulnerabilities after market launch
	CRA Compliance	

Pathway to CRA Compliance Readiness

Pathway to CRA Compliance

6. Product Classes

Default Products

- TVs
- Network printers
- Bluetooth speakers
- Media player software applications

Important Products Class I

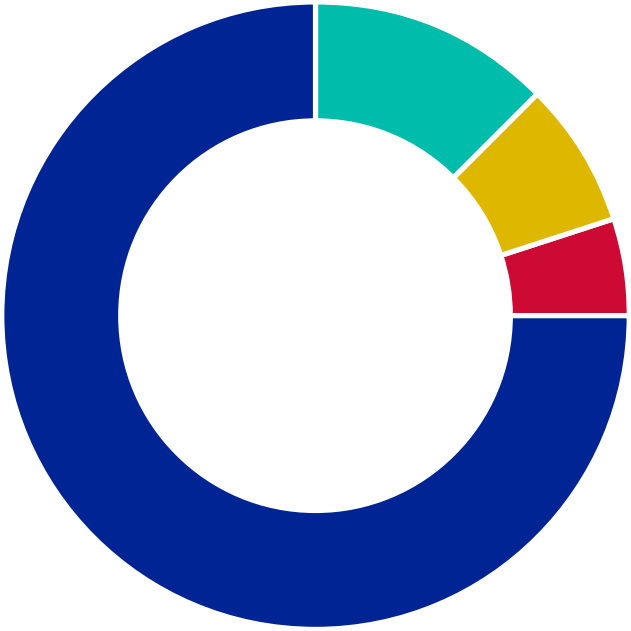
- Identity management systems
- Privileged access management software/hardware
- Standalone/embedded browsers
- Password managers
- Anti-malware software
- VPN products
- Network management systems
- Operating systems
- Routers, modems, and switches
- Microprocessors/microcontrollers with security-related functions
- Smart home products with security features
- Internet-connected toys
- Personal wearable devices

Important Products Class II

- Hypervisors
- Container runtime systems
- Firewalls
- Intrusion detection and prevention systems
- Tamper-resistant microprocessors
- Tamper-resistant microcontrollers

Critical Products

- Hardware security modules
- Smart meter gateways
- Smart cards
- Secure elements and other devices for advanced security purposes, including crypto-processing



Note: This is a selection of products that may also be assigned to a different product class depending on the criticality of the use case.

Talk to existing and prospective customers to understand their cybersecurity risk assessment approach based on zones and conduits in which your product will be deployed. This will help validate the required security levels for your products.

7. Conformity Assessment Procedures of the CRA

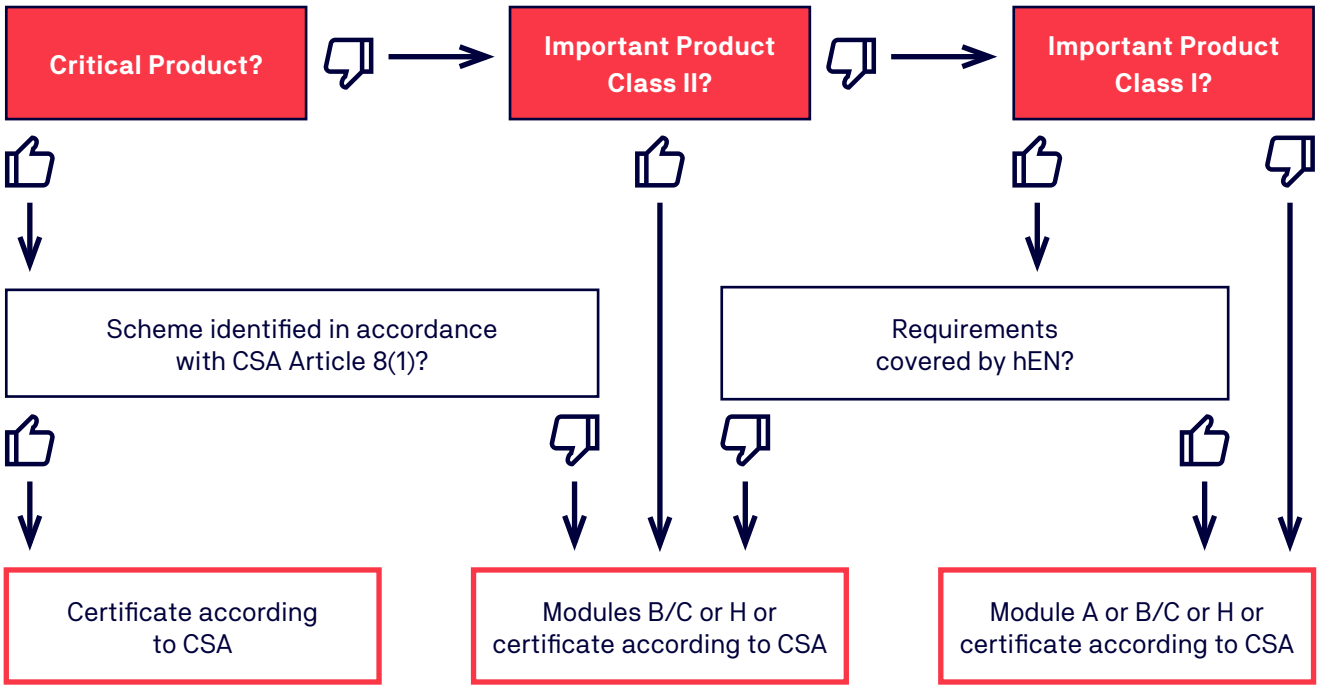
Modularization is the Key

In the context of the Cyber Resilience Act, conformity assessments and EU declarations of conformity are carried out on the basis of clearly defined conformity assessment modules. These modules specify the procedures by which manufacturers demonstrate that products with digital elements comply with the essential cybersecurity requirements of the CRA.

Depending on the product category, the following modules are applied: Module A (Internal Production Control), which is based on the manufacturer's self-assessment; Module B (EU-type examination) in combination with Module C (Conformity to type based on internal production control); and Module H (Conformity based on full quality assurance).

The selection of the applicable module determines whether conformity is demonstrated solely by the manufacturer or requires the involvement of a notified body, thereby ensuring a risk-based and proportionate conformity assessment approach.

In addition, the CRA allows conformity to be demonstrated by using a European cybersecurity certification scheme under the Cybersecurity Act (CSA). Where a relevant and appropriate CSA certification scheme exists, a certificate issued under such a scheme may be used as a means to demonstrate compliance with the corresponding CRA requirements.

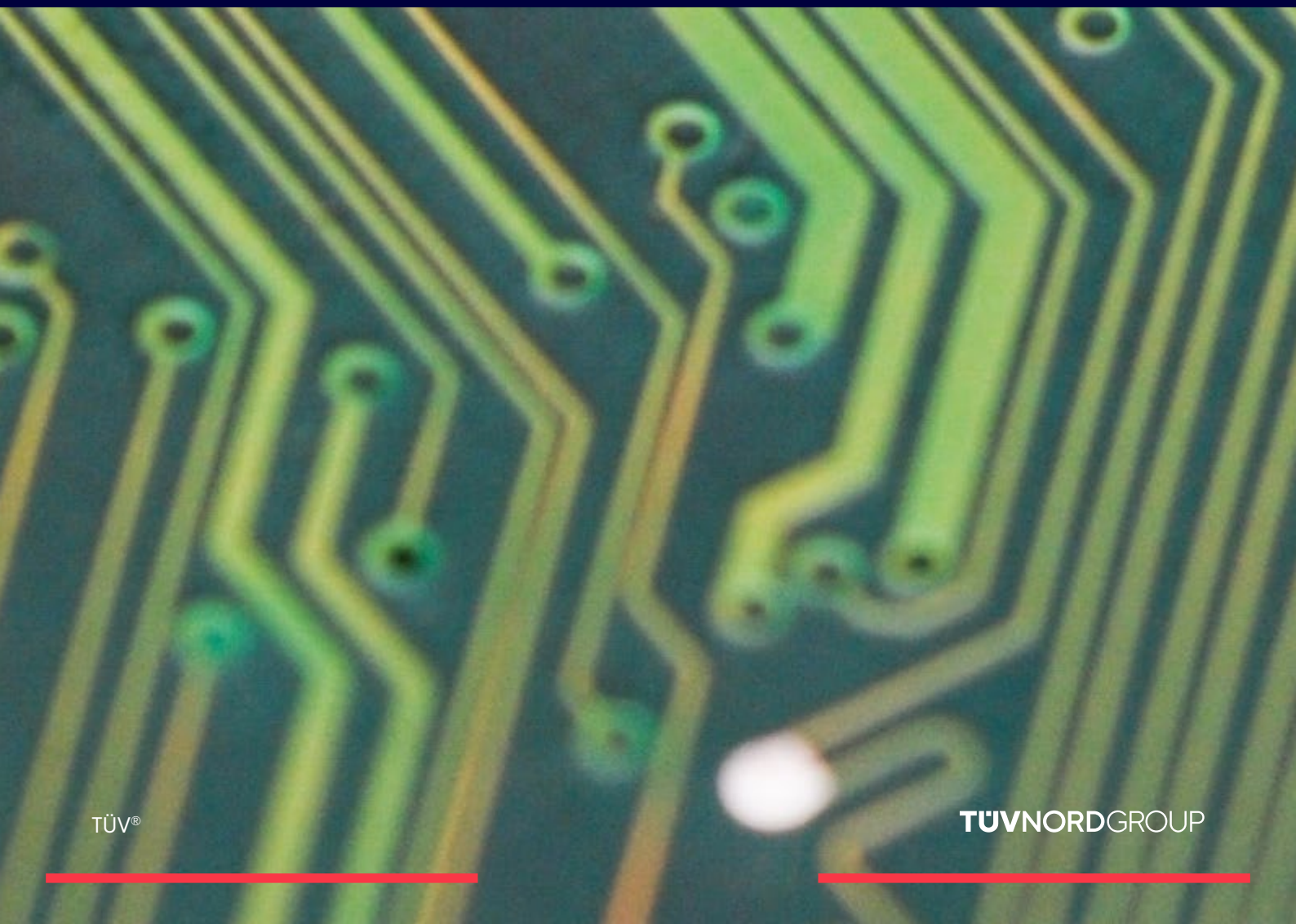


Inspired by Knowledge

TÜVIT

Contact

Eric Behrendt
T +49 30 2007700 66
M +49 160 8880296
E e.behrendt@tuvit.de

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Am TÜV 1
45307 Essen

tuvit.de/en