CRA Cybersecurity

Guidance on the classification and implementation of products containing digital elements

Context, requirements and specific steps to be taken

steinel

Cybersecurity for connected products

Cybersecurity is one of the key challenges facing the European Union.

The number and variety of connected devices is growing steadily, increasing the attack surface for cyber risks.

At the same time, cyberattacks, vulnerabilities and a lack of security updates pose significant risks, both to businesses and to the security and stability of infrastructure and society.

The Cyber Resilience Act (CRA) addresses this development and establishes a binding regulatory framework for products with digital elements within the European Union.

For the first time, manufacturers are obliged to systematically ensure cybersecurity throughout the entire product lifecycle, from development and operation through to ongoing maintenance and updating.

The CRA thus fundamentally changes the way products are developed, operated and placed on the market. Companies are faced with the task of adapting their existing products, processes and responsibilities accordingly.

This white paper provides a structured overview of the key requirements and highlights the relevant aspects throughout the entire process.

A structured approach to the topic of CRA

The CRA's requirements cover a range of areas, from product classification to compliance.

A structured approach includes, in particular:

- Product classification
- Manufacturers' obligations
- Reporting obligations
- Compliance and documentation
- Identification of specific measures

The following sections address these topics individually.

Product classification according to the CRA

The Cyber Resilience Act introduces an EU-wide harmonised classification system for products containing digital elements.

The aim is to ensure that cybersecurity requirements are risk-based and proportionate.

An overview of the four product categories:

Standard products (default) (approx. 90% of products)
e.g. smart home devices, IoT sensors or consumer software

Key products – Class I
e.g. products posing an increased cyber security risk, such as operating systems, browsers, routers or password managers

Key products – Class II
e.g. firewalls or container runtime systems

Critical products
e.g. hardware security modules or smart meter gateways.

Different requirements and conformity assessment procedures apply depending on the category.

Conformity assessment:

Internal assessment is possible for standard and, in some cases, Class I products – external assessment (by a notified body) is required for Class II and critical products.

→ Correct classification is the first and crucial step and has a direct impact on effort, costs and time to market.

steinel

Manufacturers' obligations

The CRA requires manufacturers to systematically ensure cyber security throughout the entire product life cycle.

Key responsibilities:

- Security by Design & by Default right from the development and design stage
- Mandatory cybersecurity risk assessment
- Active vulnerability management
- Provision of security updates
- Consideration of third-party and open-source components
- Transparency towards users
- Technical documentation, conformity assessment and CE marking

→ Cybersecurity thus becomes an ongoing responsibility for manufacturers throughout the entire life cycle.

An overview of reporting obligations

The CRA requires manufacturers to report safety issues in an active and structured manner.

The following are subject to reporting requirements:

- actively exploited vulnerabilities
- serious security incidents, e.g. involving data loss, disruption of functionality or malicious code

Registration procedure:

within 24 hours: Early warning → **within 72 hours: detailed report** → **in accordance with defined deadlines: Final report**

The report must be submitted via the standard EU reporting platform to:

- the relevant CSIRT and
- ENISA

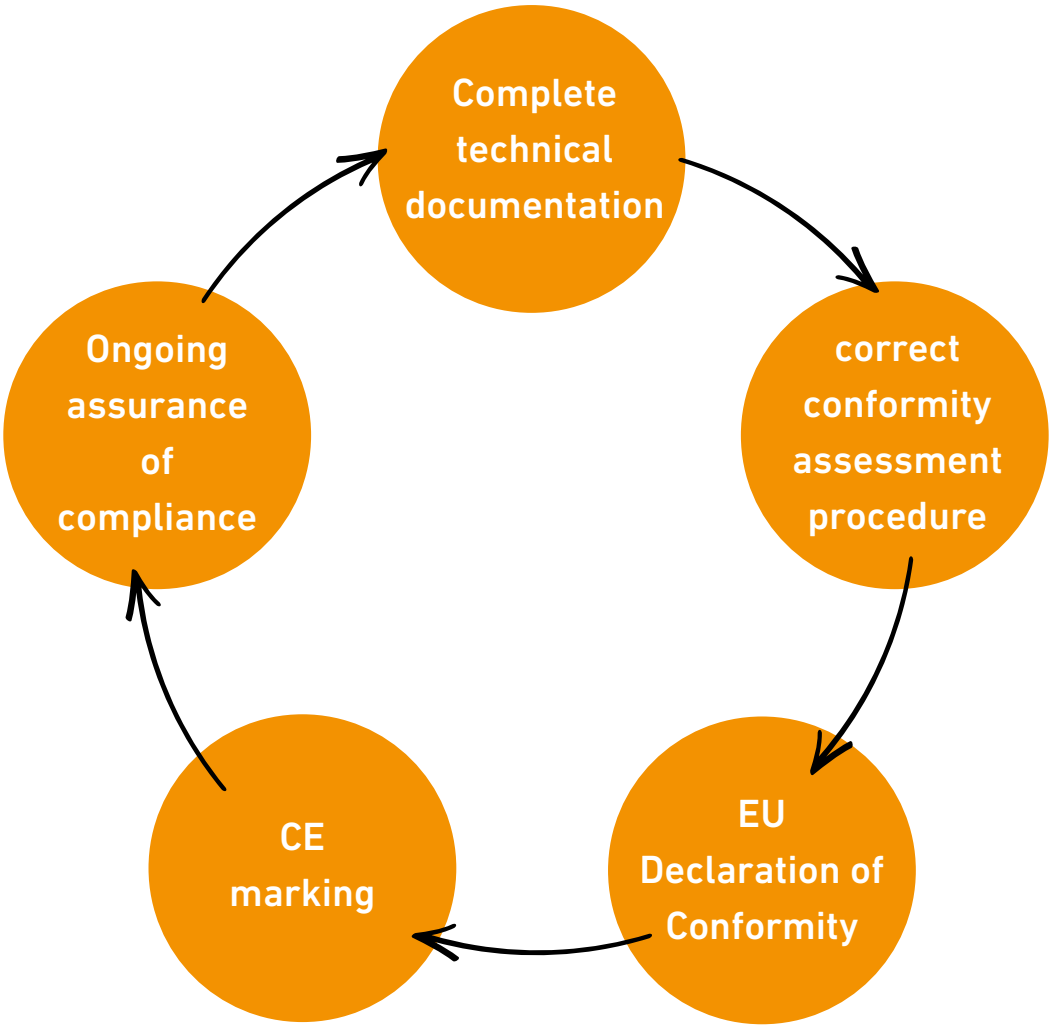
In addition, there is a duty to inform users.

→ Security incidents are therefore no longer an internal matter, but form part of regulatory requirements.

Product conformity

A product may only be placed on the market in the EU if it can be demonstrated that it meets the requirements of the CRA.

These include:



Changes to products, processes or standards must be taken into account on an ongoing basis.

Market surveillance authorities may order corrective measures, recalls or market restrictions in the event of non-compliance.

Conclusion & next steps

The Cyber Resilience Act makes cybersecurity a mandatory obligation for manufacturers.

Even though full implementation will not begin until 11 December 2027, the preparations made today will determine the future viability of products and processes.

What businesses should be doing now:

- Check products and portfolios for CRA relevance
- Carry out product classification
- Appoint an authorised representative where necessary
- Assess and establish security and development processes
- Define responsibilities and reporting lines (by September 2026)
- Establish documentation and evidence of compliance at an early stage

→ Getting started early reduces risks, costs and regulatory pressure.

Recommended approach in light of the phased roll-out of the CRA

NOW

Carry out an inventory: Which products fall under the CRA? Carry out a check and classify the products into the appropriate categories.

Define internal responsibilities. Review authorised representatives and appoint them where necessary. Keep track of compliance bodies.

until Sept. 2026

Preparing for reporting obligations:
Define and implement internal processes for identifying and reporting vulnerabilities.

until Dec. 2027

Produce technical documentation. Draft a declaration of conformity and finalise the CE marking. Carry out a conformity assessment and implement a policy for vulnerability management.

Ongoing

from Dec. 2027

Continuously monitor the support period (at least 5 years). Provide security updates free of charge. Comply with reporting requirements and keep documentation up to date at all times.

steinel

Q&A

Who does the CRA apply to?

For manufacturers and suppliers of products with digital elements in the EU.

Which products are affected?

The Regulation applies to all products with digital elements that are made available on the market and whose intended purpose or foreseeable use involves a direct or indirect data connection to other devices or networks.

A ‘product with digital elements’ is defined as a software or hardware product, including associated data-processing solutions, as well as individual components that may be placed on the market separately.

My device isn’t connected to the internet – does the CRA still apply?

Yes, locally operated devices may also fall within the scope of the CRA.

Is there a duty to report?

Yes, for actively exploited vulnerabilities and serious security incidents.

Q&A

Are harmonised standards already in place? (As at June 2026)

They are currently being drawn up and are important for practical implementation.

Do I have to do anything at all while there are no standards in place?

Yes. If you wait for the standards to be published, implementation will be very stressful. Many of the requirements are already clear, so companies can start preparing in a targeted manner right now.

Do I need to add information about CRA requirements for my product?

Yes. Manufacturers must provide relevant information on cyber security and the safe use of the product. This includes, in particular, guidance on security features, updates and how to deal with vulnerabilities; this information must be accessible to customers in a way they can understand.

Any questions left?

Individual questions often remain unanswered, particularly when it comes to the specific classification of products or the implementation of requirements.

This is exactly where we can help you.

We can help you with the following:

- assessing your specific situation
- identifying initial areas for action
- determining the next sensible steps

Arrange a no-obligation initial consultation and receive an initial assessment of your product in the context of CRA.

Arrange an initial consultation now

steinel