

Cyber Resilience Act

Strengthening cybersecurity, securing supply chains and innovation

With the Cyber Resilience Act (CRA), the EU is creating a horizontal legal framework for the cybersecurity of connected products – so-called products with digital elements. The electrical and digital industry explicitly supports this goal. With its foundation in the New Legislative Framework (NLF) and its risk-based approach, the CRA is in principle a good step towards a cyber-resilient and trustworthy European economy. From December 2027, every single connected product – including models already on the market – must be placed on the market in compliance with the CRA.

However, with its very broad scope and comprehensive design, documentation, reporting and security requirements, the CRA partially goes beyond the initial regulatory objective. A comprehensive redesign of the entire relevant product portfolio by this date is not technically or economically feasible for many manufacturers. If the legal framework remains unchanged, there is a risk of serious supply chain disruptions, particularly in the field of microelectronics. This would result in production interruptions, product discontinuations and a potential relocation of production facilities.

Our positions

Exemption of "non-critical products" without cybersecurity risk from the CRA

Many connected products – such as DAB radios, bike computers, radio clocks, barcode scanners, analog-to-digital converters or integrated microchips – do not pose a relevant cybersecurity risk. Although they transmit data and are therefore covered by the CRA, this data is exclusively trivial and often processed within a single device. If, for example, only audio data and simple operating and status information are transmitted without access to other IT systems or security-relevant functions, this does not create a relevant attack surface in cyberspace. The same applies to most microelectronic components. Many integrated microchips only transmit control and status information within a device (e.g. on/off, speed, temperature, fill level), usually via simple internal interfaces. Due to their installation situation and limited capabilities, they simply do not pose a cybersecurity risk.

Manufacturers have developed these non-critical products and components without taking CRA into account and would now have to adapt their entire portfolio. A complete redesign by 2027 is practically impossible for many companies. This would result in product discontinuations, particularly in the semiconductor industry, with serious consequences for supply chains.

Practical example: A large international semiconductor manufacturer states that its product portfolio consists of around 80,000 models; a complete redesign is not realistic. Exceptions for "non-critical" products with digital elements would significantly ease the burden here: according to estimates, around 60,000 models in this portfolio – i.e. 75 percent – could fall under this category.

Removing these non-critical products from the scope of the CRA would significantly reduce the risk of bottlenecks for important components such as microchips while maintaining a high level of security. At the same time, it would also make it significantly easier to place end products such as simple DAB radios or radio clocks on the market.

A blueprint for such an approach can be found in the Electromagnetic Compatibility (EMC) Directive (Recital 12), which stipulates that it "...should not regulate equipment which is inherently benign in terms of electromagnetic compatibility".

A similar reference to products with digital elements that "are inherently benign in terms of cybersecurity risks" would be appropriate and sensible in the context of the CRA.

Simplified technical documentation for products in the "basic category" (without increased cybersecurity risk)

Under the CRA, manufacturers must, regardless of the risk class of the product, comprehensively describe in their technical documentation what function the product fulfils, how it is technically constructed, what cybersecurity risks may exist and what measures they use to control these risks. Article 33(5) of the CRA allows micro and small enterprises to submit this technical documentation in a simplified format. This simplification should be extended to all manufacturers for basic category products (not listed in Annexes III & IV). This category covers the majority of the CRA's scope. Especially digital consumer products (connected coffee machines, smart light bulbs, etc.) would benefit from this. According to a recent ZVEI survey, this would significantly facilitate the placing on the market of around 65% of the connected products of our member companies.

Clarification that CRA compliance is possible for fully developed product models

The CRA requires manufacturers to design and manufacture products with digital elements in such a way that they ensure an appropriate level of cybersecurity in view of the risks (Annex I, Part I, Number 1). This requirement must be interpreted in such a way that it is possible to re-qualify previously developed product models. Models of products with digital elements that are already available on the market must continue to be allowed to be placed on the market if it can be shown that they meet the essential technical cybersecurity requirements, even if no process taking into account the CRA legal text was applied during their original development. There are product models on the market, for example in the semiconductor and railway industries, that have been developed over decades. They are needed by society and cannot be redesigned by December 2027 for purely technical reasons. It must therefore be clarified and stated that CRA compliance is possible for fully developed product models as long as they guarantee an appropriate level of cybersecurity. This clarification can be provided, for example, in guidelines.

Realistic, technically feasible timelines for the development of harmonised European standards

Manufacturers must have sufficient time to incorporate the legal requirements specified in the standards into their development and production processes. There should be at least 36 months between the publication of the relevant harmonised standards in the Official Journal of the EU and the end of the CRA transition period – especially in the case of vertical, product-specific standards that trigger a presumption of conformity. If these standards are not available in time, so-called "important" class I products – such as routers, operating systems or microprocessors with security-related functionalities – would have to be certified by an external conformity assessment body. This affects around 21% of digital products in the electrical and digital industry. If an extension of the deadlines is not feasible, manufacturers of this product category should, in the interim, be able to demonstrate the conformity of their products with the CRA on their own responsibility (NLF Module A of internal production control), until the vertical standards are available. Even then, once a vertical standard is available, an adequate transition period should be specified before it is applied. Otherwise, there is a risk of massive bottlenecks in placing products on the market, as was previously the case with the Medical Devices Regulation.

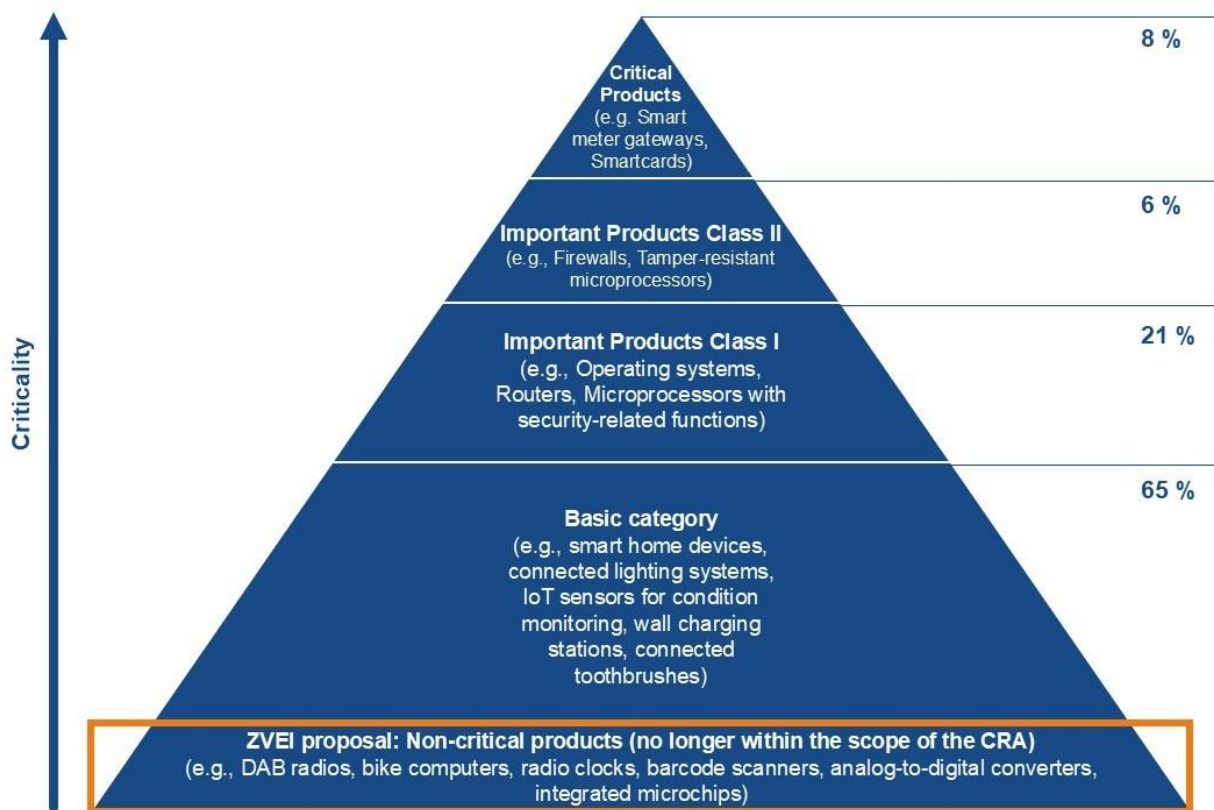
Separation between physical and digital lifetimes when determining the support period in the B2B sector

During the support period for their products with digital elements, manufacturers are required to provide security updates free of charge. The length of this period is generally determined by the manufacturer itself, although it must take other relevant EU legislation into account. This leads to considerable challenges. Regulations such as the Ecodesign Regulation require manufacturers to define the expected lifetime of products. Many industrial products have a physical lifespan of more than ten years, while their digital components are subject to much shorter innovation and support cycles. The CRA requirement could mean that the support period must not deviate significantly from the lifespan predicted under other regulations and that manufacturers must provide free security updates until the end of a product's physical usability. This is a massive intervention in common practice in the B2B sector. In order to enable risk-based and economically viable support obligations, we therefore propose a clear regulatory distinction between the physical and digital lifetimes of products with digital elements within the framework of the CRA.

Background

Scope of the CRA

- The CRA applies to all products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network. Every communicating product is therefore affected by the requirements. It makes no difference whether the product is sold to "normal" consumers (B2C) or to business customers (B2B). The CRA therefore follows an extremely broad, horizontal scope of application, with various products ranging from simple household appliances to complex industrial system components.
- The CRA currently distinguishes four categories of products with digital elements, with increasing levels of risk and correspondingly stricter conformity assessment procedures (see Fig. 1):
 1. Basic category: All products that are not explicitly listed as "important" or "critical";
 2. Important products (Annex III):
 - a. Class I: Products with increased cybersecurity risk;
 - b. Class II: Products with higher cybersecurity risk;
 3. Critical products (Annex IV): Products with high security relevance.



1) Product categories in the CRA and their share of the ZVEI membership's product portfolio consisting of products with digital elements

Manufacturer obligations

- Manufacturers must carry out a risk assessment for each product and implement the CRA's cybersecurity requirements based on this assessment. The category to which the product belongs is irrelevant in this regard. The four categories only specify the conformity assessment procedure relevant to the product. Depending on the respective risk, manufacturers must comply with comprehensive design and protection requirements, ensure active vulnerability management throughout the entire life cycle, report exploited vulnerabilities and cybersecurity incidents, prepare technical documentation and carry out conformity assessment procedures.
- Every single product with digital elements placed on the market in the EU from December 2027 onwards will be subject to the full CRA obligations. If the integration of purchased components is carried out outside the EU, these obligations only apply to the manufacturer of the imported end product.
- The concept of placing on the market refers to each individual product instance (see Blue Guide, Chapter 2.3). Manufacturers have developed their products with digital elements in the past without taking CRA

into account and must now adapt their entire relevant portfolio. A complete redesign by 2027 is practically impossible for many. This would result in product discontinuations, which, especially in the context of the semiconductor industry, would have serious consequences for supply chains.

- With its extensive requirements for manufacturers to ensure a high level of cybersecurity throughout the entire life cycle of a product with digital elements, the implementation of the CRA ties up scarce skilled personnel in companies. They are often faced with a choice: meet the requirements or make new investments in R&D. Easing the documentation requirements and granting exemptions for "non-critical" products with digital elements would remedy this situation.

Facts, numbers and data

- According to forecasts, the number of connected devices (Internet of Things, IoT) in Europe will rise from around 4.3 billion (2025) to around 6.7 billion (2030). In addition, the CRA also covers standalone software and other products with digital elements, meaning that the actual number of products affected is significantly higher.¹
- While the electrical and digital industry (EDI) is not immune to attacks, its products are secure: around 60% of EDI companies have been the target of a cyberattack in the last 24 months. Nevertheless, only around 1.5% of the companies' products placed on the market have been affected by cyberattacks in the last 24 months (e.g. in terms of their function, security or integrity).
- Companies in the digital and electrical industry estimate the total financial cost of implementing cybersecurity regulations (mainly CRA and NIS 2 Directive) until 2030 at around 1.4% of planned turnover.
- Around 65% of the connected products in our member companies' product portfolios fall into the so-called "basic category" and would therefore benefit significantly from simplified documentation requirements.
- 67% of ZVEI members rate the CRA, ahead of the NIS 2 Directive, as the most burdensome cybersecurity regulation.
- Over half (61%) of EU companies have great difficulty filling vacant cybersecurity positions with qualified candidates. The most common recruitment challenges cited are "difficulty finding qualified candidates" (45%) and "lack of applicants" (44%).²

Contact

Lennard Kreißl • Manager Digital Policy (focus on cybersecurity) • Department of Digital and Innovation Policy • Division of Digitalisation & Law
Tel.: +49 30 306960-582 • Mobile: +49 162 2664-941 • Email: lennard.kreissl@zvei.org

Imprint

ZVEI e. V. • Electro and Digital Industry Association • Charlottenstr. 35/36 • 10117 Berlin
Lobby register no.: R002101 • EU Transparency Register ID: 94770746469-09 • www.zvei.org

Date: 19.01.2026

¹ Statista (2024): Number of Internet of Things (IoT) connected devices from 2020 to 2033 (in millions), by region, <https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/>.

² European Commission (2024): Flash Eurobarometer 547 – Cyberskills., <https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=93514>.