The European Cyber Resilience Act explained

What is the European Cyber Resilience Act (the “CRA”)?
When will this regulation come into effect?
What is the impact on your products and activities?
What will you need to do to comply?
These are some of the questions that equipment manufacturers operating in the European Union need answers to. This dossier aims at answering device makers concerns and providing them with a clear path towards cybersecurity compliance.

The Embedded Kit

What is the Cyber Resilience Act?

The Cyber Resilience Act, also known as the “CRA”, is a regulation from the European Parliament and Commission. It defines harmonized rules within the European Union to make sure equipment manufacturers develop and maintain cybersecure hardware and software products.

Validated in March 2024 by the European Parliament, it will prescribe various additional cybersecurity activities to equipment manufacturers for the launch and maintenance of their existing and future products (articles 14 & 54).

It therefore includes:

5,5 trillion €

worldwide annual cost of cyberattacks on hardware and software products in 2021

Why was the CRA introduced?

In 2021, according to the European Commission, the worldwide annual cost of cyberattacks on hardware and software products approximated 5,5 trillion euros.
The causes are multiple:

- The lack of security updates for products on the market
- The lack of information and awareness surrounding cybersecurity best practices and risks

The objectives of the European Union with this regulation are to:

1

Ensure that device makers improve the security of their products **from the conception phase until the end of their lifecycle**.

2

Ensure a **coherent set of rules** within the European borders – not fragmented between the countries of the Union.

3

Improve **transparency** on product security levels.

4

Protect organizations and end-customers.

All this while respecting equipment manufacturers' intellectual property.
The EU estimates that the CRA will help reduce cyber threats and **save more than 180 billion euros each year for organizations by limiting the number of cybersecurity attacks**.

Who must comply with this regulation?

"The proposed Regulation **will apply to all products with digital elements** whose intended, and reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."
(General provisions, chapter 1)

All products with digital elements **From all industries***

Commercialized in the European Union

***Are there any ineligible products?**
Yes, some products are already regulated by specific cybersecurity laws within the European Union, such as medical devices and accessories with the Regulation 2017/745 and in vitro diagnostic medical devices and accessories with Regulation 2017/746.
Additionally, civil aviation products certified under Regulation 2018/1139 and motor vehicles following Regulation 2019/2144 are exempted.

Open source

Equipment manufacturers bear the responsibility of ensuring that the open-source packages they integrate are devoid of security vulnerabilities throughout the entire lifecycle of their product.

Should they come across any vulnerabilities during their maintenance routines, swift notification to the appropriate entity is imperative.

Artificial intelligence

Products incorporating AI fall under the scope of the CRA and must comply with its provisions.

They'll also need to comply with the future AI Act of the European Union which aims to make sure that "AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly."

Proof of Concept (POC)

To foster innovation, POCs and beta versions are exempt from CRA compliance until the launch of the product final version, provided they are solely for testing and iteration with end-users in a limited period of time.

However, these prototypes should only be disseminated after a security risk assessment.

If an OEM discontinues its operations, it can no longer ensure the security of its products on the market. That's why it must notify market surveillance authorities and customers about the situation.

Product categories

The Cyber Resilience Act classifies products in 3 categories with distinct security requirements to meet.

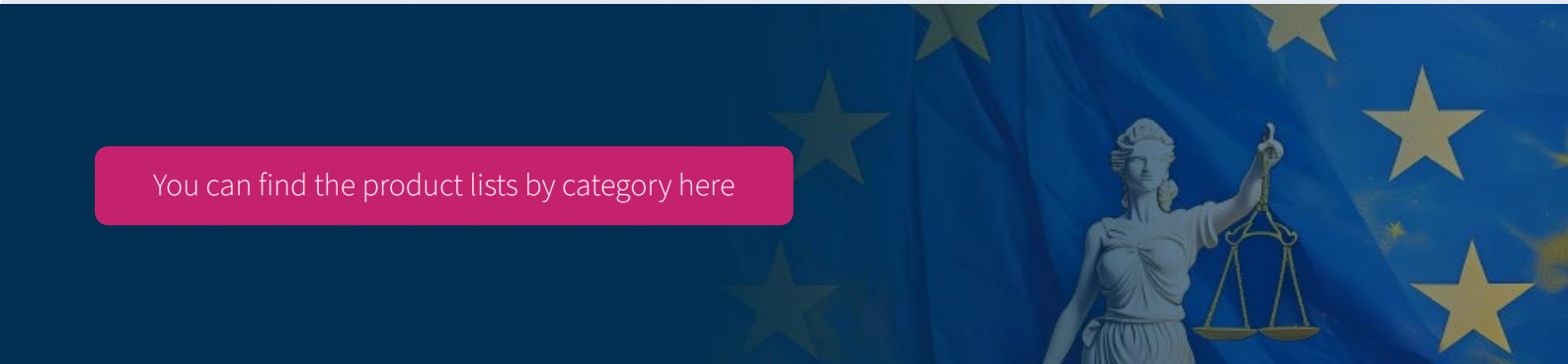
Default	Important		Critical
90% of products			
Self-assessment requirement	**Class I** Self or third-party assessment	**Class II** Third-party assessment	European Common Criteria-based cybersecurity certification
Examples: photo edition, word processing, smart speakers, hard drives, games, etc	*Password manager, OS, routers, virtual assistant...*	*Hypervisors, firewalls, tamper-resistant MPU & MCU...*	*Hardware device with secuity boxes, smartcards including secure elements...*

All products that are not explicitly listed as either important or critical are in this category. It is estimated that this represents around 90% of all products with a digital element.

These are the products that present a higher cybersecurity risk by performing a function which carries a significant risk of adverse effects (in terms of its intensity and ability to damage the health, security, or safety of users of such products) and should undergo a stricter conformity assessment procedure.
The Cyber Resilience Act classes important products in two categories depending on their level of criticality: class I and class II. Class II products hold a higher level of criticality and are thus subject to more stringent compliance measures, including assessment by external third parties.

These products have a cybersecurity-related functionality and perform a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or damage many other products with digital elements through direct manipulation.

You can find the product lists by category here



Key activities to comply with theCyber Resilience Act

1 - Cybersecurity risk assessments

The CRA requires device makers to do **comprehensive security assessments of their products**. Equipment manufacturers must indeed integrate cybersecurity considerations into the design, development, and manufacturing processes, conducting thorough evaluations at each phase to mitigate potential vulnerabilities.

This risk assessment **should appear in the product technical documentation**.

What should be included in the security assessment?

- **A thorough examination of cybersecurity risks** based on the intended purpose and foreseeable usage of the product. Utilizing attack trees can effectively delineate potential attack paths and align each with a corresponding security objective.
- **Evaluation of how the dev team implements the general requirements outlined in the CRA**, including secure development practices and procedures for handling vulnerabilities within their system.
- Providing a **clear rationale when** certain essential requirements are deemed inapplicable.

This risk evaluation process **should be regularly revisited** to adapt to evolving cybersecurity threats and the discovery of new vulnerabilities, at minimum throughout the product support period.

Witekio

Regardless of your product category, you have the option to conduct the risk assessment independently. However, **numerous consulting firms** specialize in providing assistance for such analyses, both at the outset and throughout the product's lifecycle. One such partner is **Witekio**.

Witekio benefits from being developers first and foremost:

- ☑ Witekio can initiate a cybersecurity risk analysis at the project inception and maintain it throughout the development process for ongoing relevance.
- ☑ Witekio has access to a diverse pool of experts with cybersecurity experts you can consult for support.
- ☑ Witekio offers pragmatic and effective security solutions, integrated throughout the development process.

2 - Integrate security from the conception phase

"On the basis of the cybersecurity risk assessment and where applicable, products with digital elements shall be made available on the market without known exploitable vulnerabilities." (annex I, section 1)

Building *secure by design* systems

Security must be integrated from the very conception phase of products containing digital elements.

This includes:

- delivering products with **default security configurations**,
- ensuring protection against unauthorized access through appropriate **control mechanisms** such as authentication and identity management systems,
- safeguarding the **confidentiality and integrity** of stored, transmitted, or processed data,
- **minimizing data processing** to what is strictly necessary,
- and basic functions through **mitigation measures** against denial-of-service attacks,
- limiting attack surfaces, including external interfaces (by closing external ports for example),
- **recording and monitoring** relevant internal activity with an opt-out mechanism for the user

Furthermore, device makers must protect products essential functions' availability, mitigate their negative impacts on other devices or networks, limit attack surfaces, reduce incident consequences through appropriate mechanisms, and provide security-related information through activity monitoring and update notifications. That's why security assessments are also required by the CRA.

Read our article: How to build secure by design Linux-based products

Existing solutions to streamline security developments

Solutions like Welma Yocto Linux can significantly expedite your development process for embedded Linux systems by pre-integrating essential security requirements for the CRA. These include features such as minimization, secure boot, read-only configurations, OTA update mechanisms, comprehensive cybersecurity documentation, and more. Additionally, Welma Yocto Linux supports long-term maintenance through vulnerability monitoring and integration into CI pipelines, ensuring your system remains secure by design throughout its lifecycle.

Discover more about Welma Yocto Linux

WELMA
YOCTO LINUX

3 - Vulnerability monitoring & patching during the whole product lifecycle

Generating a Software Bill of Materials

Manufacturers are urged to meticulously **list and document the components present in their products**. Having this comprehensive software inventory, called Software Bill of Materials (SBOM) not only facilitates vulnerability analysis but also enhances understanding of the supply chain dynamics.

"Manufacturers of products with digital elements shall identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products." (Annex I, section 2)

Monitoring product vulnerabilities

Manufacturers are required by the Cyber Resilience Act to diligently manage and address security vulnerabilities in their products. This involves systematically identifying and documenting vulnerabilities and software components, promptly managing and correcting identified vulnerabilities through security updates, and subjecting products to regular and effective security tests and assessments.
See our article on how to monitor your vulnerabilities

Communicating vulnerabilities information among stakeholders

Additionally, device makers must publicly disclose information about corrected vulnerabilities, including their severity and potential consequences, to ensure users are informed and able to take appropriate actions. A coordinated vulnerability disclosure policy must be established, along with mechanisms for facilitating the sharing of vulnerability information among stakeholders.

Applying regular security updates

Secure distribution mechanisms for updates are crucial to swiftly address exploitable vulnerabilities, ensuring that patches and security updates are disseminated promptly and accompanied by clear instructions for users. Read our article on OTA update definition & best practices

Software composition analysis (SCA) & vulnerability management tools

Vigiles timesys
cve-check yocto
CVE SCAN VULNERABILITY MONITORING

Numerous SCA tools, such as **CVE Scan**, are available to **help generate hardware (HSBOM) ad software (SBOM) component lists**. These tools also assist in regularly identifying and **monitoring vulnerabilities** within your embedded system when integrated to your CI pipelines.

When selecting a tool, it's crucial to consider:

- **results accuracy** to minimize the time spent on maintenance activities
- **ownership on your vulnerabilities data**

Consult our tools comparison

4 - Documentation

Product technical documentation will serve as a vector of information on security activities for verification authorities and end-customers.

Equipment manufacturers should **methodically document cybersecurity risks** associated with their products, encompassing known vulnerabilities and pertinent data from external sources. This documentation not only aids in internal decision-making processes but also fosters transparency and accountability in adherence to regulatory requirements. As mandated by regulations, manufacturers must include vulnerabilities list, third-party information, and periodic risk assessments.

Furthermore, manufacturers are obligated to **maintain technical documentation and EU conformity declarations for a period of ten years** following the product's market introduction, ensuring accessibility to market surveillance authorities.

"Ensuring thorough documentation within user guides or integration manuals is essential. It's crucial that this documentation clearly outlines the requirements for securely utilizing the product's security functionalities. This aspect is particularly critical for products destined for integration into larger systems, where the integration guide also serves as a security manual. It meticulously details the essential points necessary to maintain security integrity without compromise. **By providing comprehensive documentation, users can navigate the product's security features confidently, thereby minimizing the risk of inadvertently compromising system security.**"

Julien BERNET, Cybersecurity leader

5 - Reporting

Transparent reporting mechanisms are also essential for effective cybersecurity governance. Equipment manufacturers must establish clear protocols for reporting cybersecurity incidents, both internally and to relevant stakeholders. This transparent approach enables swift responses to cyber threats, minimizing potential damage and enhancing trust among customers and regulatory authorities.

Notifying the European Union Agency for Cybersecurity (ENISA) about actively exploited vulnerabilities

Notifying the European Union Agency for Cybersecurity (ENISA) about actively exploited vulnerabilities is imperative and must occur within 24 hours of becoming aware of the vulnerability. This notification should include detailed information about the exploit and any measures taken to address or mitigate its effects.

About the ENISA, the European Union Agency for Cybersecurity: In the context of the CRA, the ENISA organization is tasked with receiving notifications from OEMs regarding actively exploited vulnerabilities in their products as well as incidents impacting the security of these products. It should transmit these notifications to relevant European & States authorities.

Notifying users

Additionally, OEMs should promptly inform users of any security incidents affecting their products, along with any corrective measures that users can implement to mitigate the impact. This proactive communication ensures that users can respond swiftly to security incidents, whether through published information on the manufacturer's website or direct outreach from the manufacturer. Equipment manufacturers ought to autonomously establish the appropriate timing for notifying users, encompassing both patch releases and vulnerability identification. This schedule should align seamlessly with the outcomes of the risk assessment they have performed.

6 - Conformity assessment & declaration

Conformity assessment objectives

Before launching a new product on the market - or if there is a substantial update of the product -, equipment manufacturers must conduct a conformity assessment to validate that the CRA requirements have been taken into account and that the product does not present any known and exploitable vulnerability.

What is a substantial update of the product? *"a product with digital elements should be considered as substantially modified by a software change where the software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed, or the level of risk has increased because of the software update. For example, this could be the case where a new input element is added to an application, requiring the manufacturer to ensure adequate input validation" (article 39).*
Therefore, not all updates lead to a substantial modification of the product.

Manufacturers carry the responsibility for conducting these assessments under their own supervision. However, they have the flexibility to engage third-party entities for evaluation if necessary. Given the heightened cybersecurity risks associated with critical Class II devices, third-party intervention is essential during the conformity assessment process.
Note that the list of organizations authorized to help you with your conformity assessment is defined by the country you are living in. Consult your government page to know more.

Conformity assessment procedures

There are three primary procedures for conformity assessment:

- **Internal control procedure**: The manufacturer assumes responsibility for ensuring product compliance with all essential requirements and processes. This includes establishing technical documentation, ensuring adherence to design, development, production, and vulnerability management processes, affixing the CE marking on compliant products, and providing a written EU declaration of conformity for each product.
- **EU type examination**: In this procedure, a notified body examines the technical aspects of the product's design, development, and vulnerability management processes to ensure compliance with essential requirements. The manufacturer submits documentation and evidence of compliance to a single notified body (the ANSSI in France for instance), which then evaluates the product and issues an EU type examination certificate if requirements of the article 39 are met.
- **Conformity based on internal production control**: Here, the manufacturer ensures that production processes guarantee conformity with the approved type and essential requirements. This involves affixing the CE marking on compliant products, establishing a written declaration of conformity for each product model, and maintaining technical documentation for ten years after market placement.

CE marking

Once the assessment is done, device makers can submit an EU conformity declaration. Once validated they will be able to put the CE marking on their product.

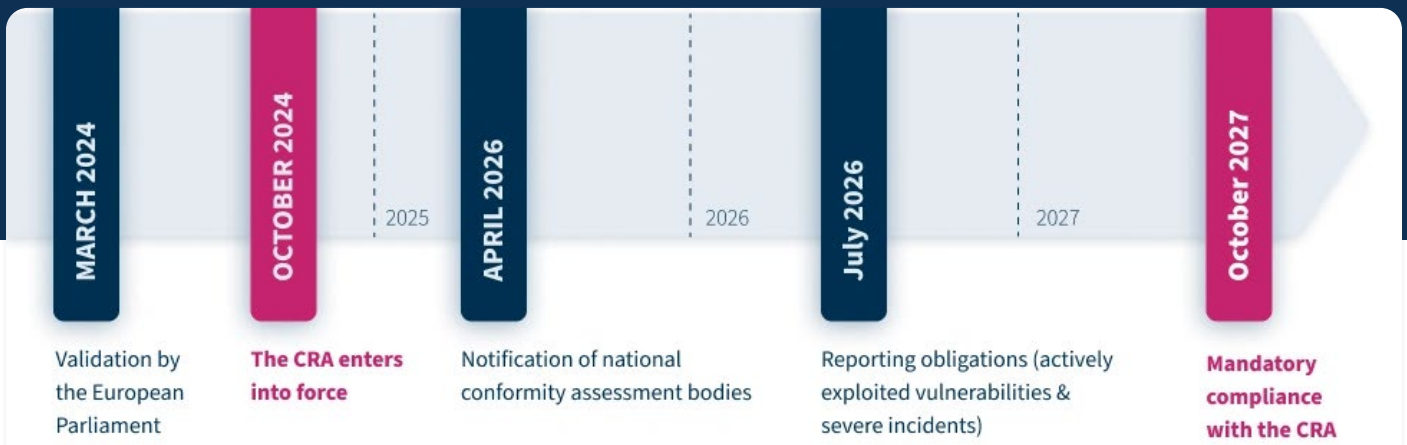
The CE marking is a crucial **indication of product compliance to the Cyber Resilience Act**. It is the visible result of the comprehensive process of conformity assessment and allows products free movement within the internal European market. The CE marking must be affixed in a visible, legible, and indelible manner on the product, its packaging, its EU Declaration of Conformity, and/or on the product's website. Its height can be less than 5 mm, as long as it remains visible and legible. **The CE marking is affixed before the product is placed on the market** and is followed by the identification number of the notified body, when this body participates in the conformity assessment procedure based on full quality assurance.

Get help from external providers

Equipment manufacturers may appoint mandates to help them perform certain tasks:

- Maintain the EU declaration of conformity and technical documentation for ten years from the product's market placement, making it available to market surveillance authorities.
- Cooperate with market surveillance authorities upon request regarding any measures taken to eliminate risks posed by a product.

Timeline



To let manufacturers the time to adapt to the new regulation, they have **36 months** from the regulation entry into force (planned in September/October 2024) to organize themselves and make the necessary adjustments.

However, reporting obligations for actively exploited vulnerabilities and incidents will begin 21 months after the regulation takes effect, and declarations to national conformity assessment bodies will be required 18 months after the regulation's start date.

Risks of non-compliance

Non-compliance with the Cyber Resilience Act carries significant consequences for manufacturers. The directive 85/374/CEE complements this regulation by establishing rules on liability for defective products, ensuring that victims can seek redress for damages caused by such products. Manufacturers are held strictly liable for damages resulting from security flaws in their products. Failure to provide necessary security updates post-market release could therefore lead to liability for manufacturers.

Financial penalties

Failure to meet cybersecurity requirements may result in **administrative fines of up to €15,000,000 or 2.5% of the company's total annual worldwide turnover for the previous fiscal year**.
Providing inaccurate, incomplete, or misleading information to notified bodies and market surveillance authorities in response to inquiries may incur fines of up to €5,000,000 or 1% of the company's total annual worldwide turnover for the previous fiscal year.
The amount of the fine will depend on the nature, severity, and duration of the violation and its consequences, whether administrative fines have been previously imposed by other market surveillance authorities on the same operator for a similar offense, and the size and market share of the operator committing the violation.

Product recalls

If products do not adhere to the regulation, the Commission may request an assessment by ENISA. Based on this evaluation, the Commission may adopt corrective or restrictive measures at the Union level, including product recalls, within a reasonable timeframe proportional to the risk. However, this action is exceptional when competent authorities fail to address the situation effectively.

The Embedded Kit

theembeddedkit.io