

Navigating the Cyber Resilience Act

Organizational Compliance,
Oversight, Challenges, and Impact on
Stakeholders

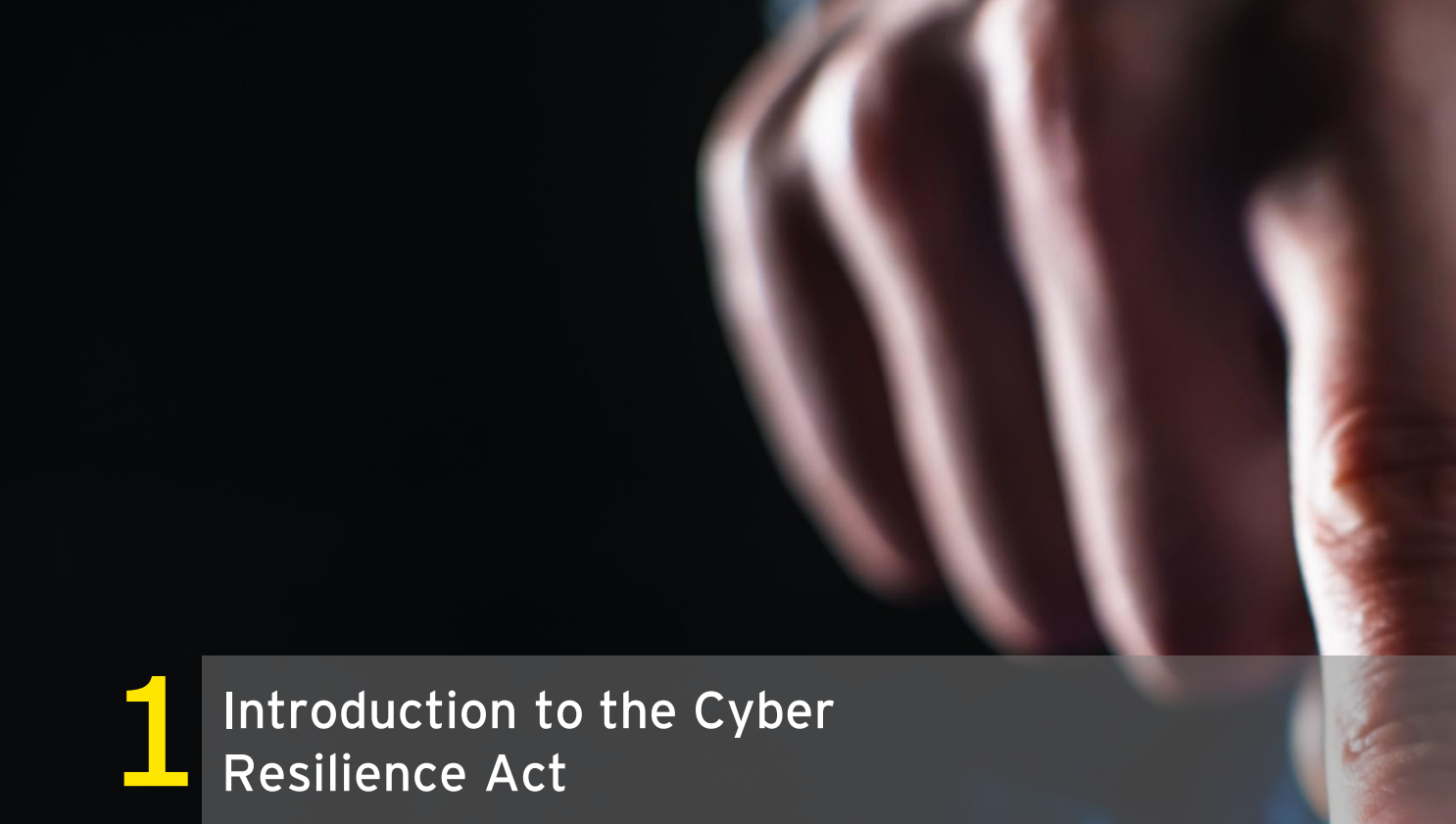
July 2024



INDEX

1.	Introduction to the Cyber Resilience Act	5
2.	Compliance obligations for organizations	11
3.	Compliance and oversight of the implementation of the CRA by organizations	13
4.	Criticisms and challenges identified in the elaboration of the CRA	15
5.	Potential impacts for organizations	17
6.	Potential impacts for consumers	19
7.	Procedures for CRA compliance	21
8.	Conclusions	23





1 Introduction to the Cyber Resilience Act

What is the Cyber Resilience Act?

In an era where cyberattacks are on the rise, with reports predicting an attack every 2 seconds by 2031, possibly costing over €251 billion annually¹, it has become increasingly critical to enhance cybersecurity and mitigate vulnerabilities in digital products.

The proliferation of connected and smart products, with Internet of Things (IoT) connected devices potentially reaching 34.7 billion by 2028², magnifies this risk where a single cybersecurity incident can have cascading effects across entire supply chains, potentially causing widespread disruption to economic and social activities, and even posing threats to public safety.

A fundamental issue is the inadequate cybersecurity in many products, coupled with manufacturers' reluctance to issue updates to fix vulnerabilities, often leaving consumers and businesses to deal with the consequences.

This situation is aggravated by the information gap that exists where both businesses and consumers lack the necessary knowledge to identify and configure secure products and the fact that the burden of security lapses is mostly felt by users, not manufacturers, reducing the latter's motivation to focus on secure design and post-sale support.


The CRA is a legislative initiative designed to ensure that hardware and software products containing digital elements meet essential cybersecurity requirements before they are allowed to be made available on the market.

This legislation was approved by the European Parliament on 12 March 2024³ after the Council's agreement in December 2023, and mandates that manufacturers incorporate cybersecurity considerations

1 [Global Ransomware Damage Costs Predicted To Exceed \\$265 Billion By 2031 \(cybersecurityventures.com\)](https://www.cybersecurityventures.com)

2 [Ericsson Mobility Report June 2023](#)

3 [Cyber Resilience Act: MEPs adopt plans to boost security of digital products | News | European Parliament \(europa.eu\)](#)



into the design and development processes of their products⁴. The final version of the Regulation is expected to be published in 2024.

Under the new regulation of the CRA, stringent cybersecurity standards are established to safeguard against potential threats and vulnerabilities associated with digital systems. By requiring manufacturers to prioritize cybersecurity during product design and development, the CRA aims to enhance the resilience of digital products against cyber threats and foster consumer confidence and transparency in the security of digital technologies⁵.

Framework and relationship with other regulations

The European Parliament expressed its support for the European Commission's move to address the *"risk of fragmentation of the single market due to national regulations on*

*cyber-security and the lack of horizontal legislation regarding essential cyber-security requirements for hardware and software, including connected products and applications"*⁶. This initiative marks a pivotal step as the first legislation of its kind to introduce mandatory cybersecurity requirements for products with digital elements across their entire lifecycle.

The legislative proposal of the CRA was announced by the President of the European Commission, Ursula von der Leyen, in her September 2021 State of the European Union address⁷ and is framed within two strategic pillars: the EU Cybersecurity Strategy⁸ and the 2020 EU Security Union Strategy⁹. This act is part of a broader regulatory genealogy that aims to enhance cybersecurity across the European Union's digital landscape.

4 [State of the Union: New EU cybersecurity rules \(europa.eu\)](#)

5 [Cyber Resilience Act - Questions and Answers \(europa.eu\)](#)

6 [Texts adopted - The EU's Cybersecurity Strategy for the Digital Decade - Thursday, 10 June 2021 \(europa.eu\)](#)

7 [State of the Union Address by President von der Leyen \(europa.eu\)](#)

8 [The Cybersecurity Strategy | Shaping Europe's digital future \(europa.eu\)](#)

9 [eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN](#)

Currently, the legislative measures present in EU's cybersecurity framework are all specific to particular sectors or products. Beginning with the Directive on Attacks against Information Systems¹⁰ introduced in 2013, aimed to align criminal offenses and sanctions targeting information systems, followed by the Directive on Security of Network and Information Systems across the EU (NIS Directive¹¹), that came in 2016 and enacted to strengthen cybersecurity across the EU through legal measures, particularly concerning critical infrastructure. This directive was subsequently updated to the broader NIS2 Directive¹² in December 2022, that fortifies the measures introduced by its predecessor, with a transposition deadline for member states of October 2024.

Sector-specific legislations like the CER¹³ and DORA¹⁴ impose specialized security and reporting protocols within their respective domains. Moreover, the 2019 EU Cybersecurity Act¹⁵ reinforced ENISA's role and initiated a voluntary certification scheme for ICT products, services, and processes' cybersecurity features.

Despite these efforts, the EU lacks a universal set of cybersecurity requirements for hardware and software products not bound to particular sectors or products. This gap raises the possibility of member states creating their own, potentially mismatched regulations, which could challenge the single market's unity and competitive edge.

The upcoming CRA is designed to address this gap and further fortify the EU's cybersecurity framework. Focusing on enhancing the cybersecurity of products with digital elements

will ease compliance efforts for entities covered by the NIS2 Directive and support and secure the entire supply chain. Through this complementarity¹⁶, the CRA endeavors not only to protect consumers and businesses but also to maintain the integrity and reliability of the broader digital infrastructure that underpins the single market.

According to Articles 66, 67 and 68 of the CRA¹⁷, this regulation is also an amendment to Regulation (EU) 2019/1020¹⁸, which covers market surveillance and compliance of products, Directive (EU) 2020/1828¹⁹ which concerns representative actions for the protection of the collective interests of consumers by increasing digital product safety, and Regulation (EU) No 168/2013²⁰, which governs the approval and market surveillance for two- or three-wheel vehicles and quadricycles, respectively.

Geopolitical framework and feasibility of the CRA

The CRA emerges against a backdrop of a highly interconnected and geopolitically complex global digital landscape²¹. China's pivotal role in the production and supply chain of digital components places it at the heart of the CRA's impact, challenging manufacturers there to align with rigorous EU cybersecurity standards. As the EU intensifies its cybersecurity defenses amid escalating cyber threats and tensions, the implementation of the CRA could lead to

10 [Directive - 2013/40 - EN - EUR-Lex \(europa.eu\)](#)

11 [Directive - 2016/1148 - EN - EUR-Lex \(europa.eu\)](#)

12 [Directive - 2022/2555 - EN - EUR-Lex \(europa.eu\)](#)

13 [Directive - 2022/2557 - EN - CER - EUR-Lex \(europa.eu\)](#)

14 [Regulation - 2022/2554 - EN - DORA - EUR-Lex \(europa.eu\)](#)

15 [Regulation - 2019/881 - EN - EUR-Lex \(europa.eu\)](#)

16 [NIS2, DORA and CRA: 3 upcoming mutations in the cyber landscape - INCYBER NEWS](#)

17 [Texts adopted - Cyber Resilience Act - Tuesday, 12 March 2024 \(europa.eu\)](#)

18 [Regulation - 2019/1020 - EN - EUR-Lex \(europa.eu\)](#)

19 [Directive - 2020/1828 - EN - EUR-Lex \(europa.eu\)](#)

20 [Regulation - 168/2013 - EN - EUR-Lex \(europa.eu\)](#)

21 [9th EU-US Cyber Dialogue in Brussels - press statement | Shaping Europe's digital future \(europa.eu\)](#)

both increased production costs, potentially passed on to consumers, and strained trade relations, as manufacturers worldwide adjust to comply with the EU's stringent cybersecurity requirements.

This regulatory shift, while bolstering security, amplifies discussions on supply chain diversification and market competitiveness.

Main objectives of the CRA

The objectives of the CRA^{22,23} to enhance cybersecurity across the digital landscape and ensure a safe digital environment for its citizens are:

- **Create conditions for the development of secure products with digital elements:** ensuring that products with digital elements are inherently secure by design. Manufacturers are expected to prioritize security in every phase of a product's lifecycle, from initial design to post-market updates. By setting robust security baselines, the CRA aims to mitigate the proliferation of vulnerabilities in digital products, ensuring they are both resilient against cyber-attacks and maintained with consistent security updates.

- **Making users aware of cybersecurity:** the CRA envisions a digital marketplace where users are educated and informed, enabling them to make knowledgeable decisions based on cybersecurity features of the products they purchase and use, and addressing the existing gap in user knowledge and access to cybersecurity information.
- **Ensuring a coherent cybersecurity framework:** including legislative measures designed to create consistency in cybersecurity practices among manufacturers, hence avoiding fragmentation.
- **Raising levels of transparency:** by mandating clear labeling and information dissemination about the security features and practices associated with digital offerings, thus providing end-users with the necessary transparency to make informed decisions on the cybersecurity posture of products.

“

This Regulation lays down:

- (a) rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products;
- (b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity;
- (c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the product is expected to be in use, and obligations for economic operators in relation to those processes;
- (d) rules on market surveillance, including monitoring, and enforcement of the rules and requirements.

Article 1 of the CRA¹⁷

²² [Cyber Resilience Act \(europa.eu\)](https://european-cyber-resilience-act.com/)

²³ [European Cyber Resilience Act \(CRA\) \(european-cyber-resilience-act.com\)](https://european-cyber-resilience-act.com/)

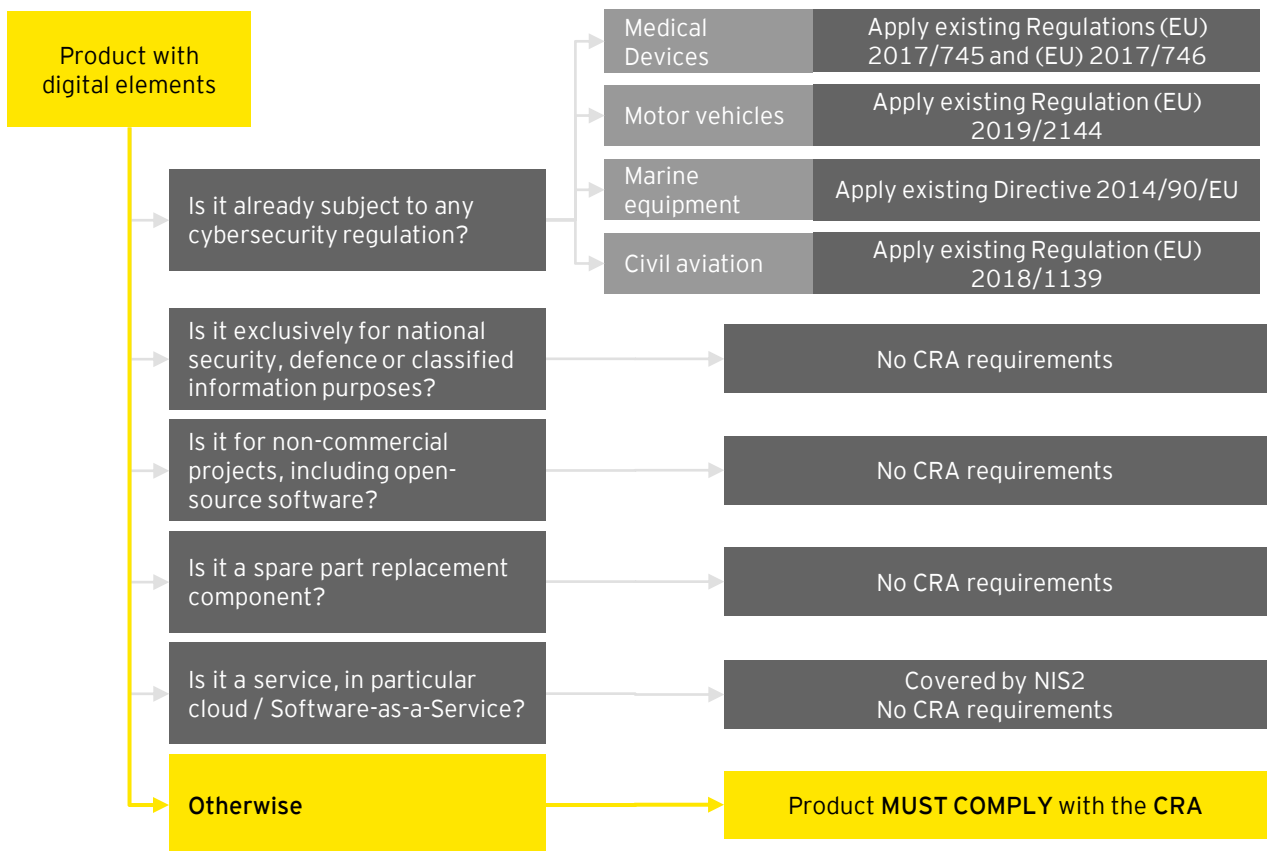
Scope of the CRA

Regarding the scope of this regulation, in Article 2¹⁷ it is said to apply to “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” and Article 3 further explains the definition of products with digital elements as “software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately”.

The covered digital products are classified into two main categories, critical and important, the latter is further divided according to their risk-level²⁴ :

- ▶ **Class I - Lower risk:** e.g., identity management systems and privileged access management software and hardware, password managers, SIEM systems, virtual private networks, routers, smart home products with security functionalities, personal wearable products with health monitoring purposes, etc.
- ▶ **Class II - Higher risk:** e.g., hypervisors and container runtime systems, firewalls, intrusion detection and prevention systems, tamper-resistant microprocessors, etc.

The following page provides additional details regarding the product coverage within the scope of the CRA.²⁵.



²⁴ [EU cyber-resilience act \(europa.eu\)](https://european-council.europa.eu/media/en/press-communications/infographic/infographic_cyber-resilience-act.pdf)

²⁵ [Cyber Resilience Act \(cisa.gov\)](https://www.cisa.gov/cyber-resilience-act)

Important Products With Digital Elements - Class I

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers;
2. Standalone and embedded browsers;
3. Password managers;
4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Security information and event management (SIEM) systems;
8. Boot managers;
9. Public key infrastructure and digital certificate issuance software;
10. Physical and virtual network interfaces;
11. Operating systems;
12. Routers, modems intended for the connection to the internet, and switches;
13. Microprocessors with security-related functionalities;
14. Microcontrollers with security-related functionalities;
15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities;
16. Smart home general purpose virtual assistants;
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems;
18. Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council(45) that have social interactive features (e.g., speaking or filming) or that have location tracking features;
19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or Regulation (EU) 2017/746 do not apply, or personal wearable products that are intended for the use by and for children.

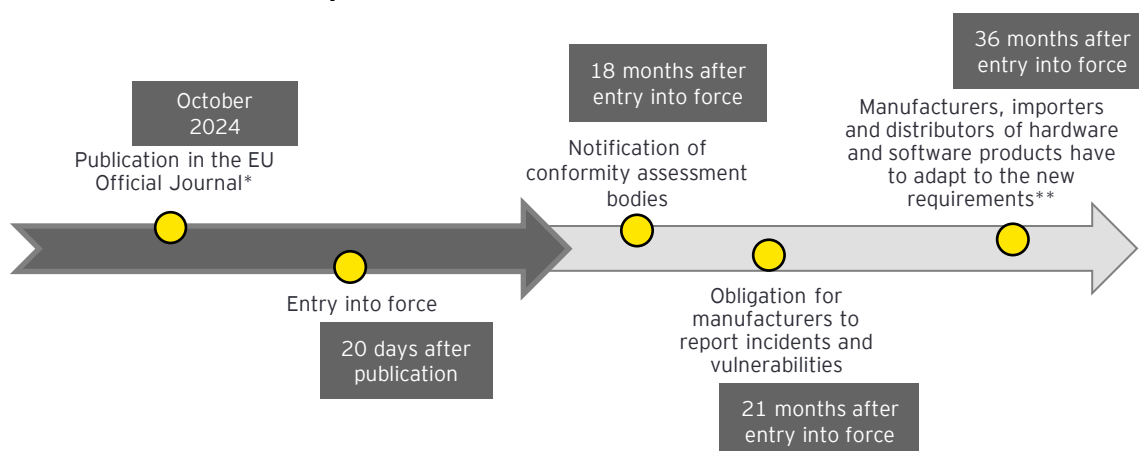
Important Products With Digital Elements - Class II

1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
2. Firewalls, intrusion detection and prevention systems;
3. Tamper-resistant microprocessors;
4. Tamper-resistant microcontrollers.

Critical Products With Digital Elements


1. Hardware Devices with Security Boxes;
2. Smart meter gateways within smart metering systems as defined in Article 2(23) of Directive (EU) 2019/944 of the European Parliament and of the Council(46) and other devices for advanced security purposes, including for secure crypt processing;
3. Smartcards or similar devices, including secure elements.

Timetable for entry into force of the CRA¹⁷



* The publication estimate was postponed to September/ October - [Cyber Resilience Act adopted in plenary with publication postponed to Autumn 2024 \(cece.eu\)](#)

**To simplify the process for manufacturers, to fulfill the essential requirements, the Commission will issue a request for standardization, enabling the European Standardisation Organisations to "develop technical standards for many of the product categories covered by the Cyber Resilience Act".



2 Compliance obligations for organizations

The CRA presents various compliance obligations that organizations must meet to ensure the cybersecurity and integrity of their digitally enabled products within the market²⁶. These obligations can be distinguished by type of entity, as examples:

Manufacturers²⁷:

- ▶ **Compliance with Cybersecurity Requirements:** Manufacturers are responsible for ensuring that digital products meet essential cybersecurity requirements as stipulated in the CRA²⁸ before they are placed on the market.
- ▶ **Conformity Assessment Procedures:** They must carry out or arrange for conformity assessments to be done in accordance with the risk category of the products—either through self-assessment or third-party assessment by a Conformity Assessment Body.
- ▶ **Technical Documentation:** Manufacturers are required to compile and maintain thorough technical documentation demonstrating that the digital products meet the essential requirements of the CRA. They must create a Software Bill of Materials (SBOM) in a widely recognized format that includes at least the primary dependencies of the product. Although there is no obligation for the SBOM to be publicly accessible, it should be part of the technical documentation and made available to market surveillance authorities upon request.
- ▶ **Notification of Cybersecurity Incidents:** They must abide by stringent notification obligations for cybersecurity breaches, reporting them to the appropriate authorities within the timeframe specified by the regulation.
- ▶ **Support:** Manufacturers also need to monitor the digital products through their lifespan and take corrective actions when necessary.

²⁶ [Cyber Resilience Act text, articles \(15.9.2022\) \(european-cyber-resilience-act.com\)](#)

²⁷ [Cyber Resilience Act text, Article 10 \(15.9.2022\) \(european-cyber-resilience-act.com\)](#) (Article 13 in updated version)

²⁸ [Cyber Resilience Act text, Annex 1 \(15.9.2022\) \(european-cyber-resilience-act.com\)](#)



Importers²⁹:

- ▶ **Market Compliance:** Importers must ensure that they only place on the market digital products that are compliant with the essential cybersecurity requirements of the CRA detailed in Annex I²⁸ and carry the necessary CE marking. This is applicable even for organizations based outside of the EU that intend to sell their products in the EU's market.
- ▶ **Verification of Obligations:** They are tasked with confirming that manufacturers have complied with their obligations, including the completion of conformity assessments and that products are accompanied by the necessary documentation and markings.
- ▶ **Notification and Corrective Actions:** If an importer suspects non-compliance or identifies a cybersecurity risk, they must refrain from placing the product on the market and take appropriate corrective measures, as well as inform the

manufacturer and market surveillance authorities.

Distributors³⁰:

- ▶ **Verification of Compliance Markings:** Distributors have the duty to verify that digital products bear the CE marking and other compliance indicators before offering them on the market.
- ▶ **Duty of Care:** Distributors must act with due care to ensure that the products they provide have met the CRA obligations by both the manufacturer and importer.
- ▶ **Notification of Non-Conformity:** Similar to importers, distributors must not distribute products that they believe do not comply with essential requirements, and they must report any significant cybersecurity risks to the manufacturer and market surveillance authorities.

²⁹ [Cyber Resilience Act text, Article 13 \(15.9.2022\) \(european-cyber-resilience-act.com\)](#) (Article 19 in updated version)

³⁰ [Cyber Resilience Act text, Article 14 \(15.9.2022\) \(european-cyber-resilience-act.com\)](#) (Article 20 in updated version)



3 Compliance and oversight of the implementation of the CRA by organizations

Conformity assessment process

The conformity assessment model for the CRA operates on a set of procedures that align with the level of risk associated with the product. This model ensures a simple and cost-effective self-assessment for the majority of products, and a more rigorous third-party evaluation for those posing greater risks⁵.

For products that **do not belong to the important or critical categories**, manufacturers can opt for conducting a cybersecurity **self-assessment** and declare, under their own responsibility, that their products comply with the cybersecurity requirements of the CRA, affixing the CE marking and writing the EU declaration of conformity for each product. This self-declaration process is typically less stringent and is applicable to the majority of products on the market¹⁷.

For **important products of class I (lower risk)**, manufacturers can still opt for self-assessment if they adhere to harmonized cybersecurity standards developed by European

standardization organizations, or applicable cybersecurity certification schemes under the EU Cybersecurity Act. If such standards or schemes do not exist, or if the manufacturer does not fully apply them, a **third-party conformity assessment** by a Conformity Assessment Body is required.

For **critical or important products of class II (higher risk)**, manufacturers must undergo a **third-party conformity assessment**. This ensures a higher level of scrutiny, given the potential impact that these products may have on cybersecurity and user safety.

Nonetheless, this model has elicited discussion from various stakeholders during the preparation of the current version. Some examples include the European Consumer Organisation (BEUC) advocating in 2022 for *“independent third-party assessment of certain products that*



pose higher risks to consumers, such as smart home systems”³¹, which may significantly impact consumer safety and protection. BEUC argued that self-assessment by manufacturers, while suitable for less critical products, may not provide sufficient assurance of cybersecurity for products that have a greater potential to harm consumers if compromised.

Similarly, in 2022, the ICT Council³² supported the call for conformity assessments conducted by bodies independent of the product developers, expressing apprehension that allowing manufacturers to self-evaluate most products may lead to a scenario where products that could compromise consumer safety and protection remain on the market due to potential biases or gaps in self-assessment processes.

This discussion contributed to ensure a more rigorous compliance landscape, increasing consumer trust and mitigating potential risks associated with greater reliance on manufacturer-led self-assessments.

Notification and application of sanctions

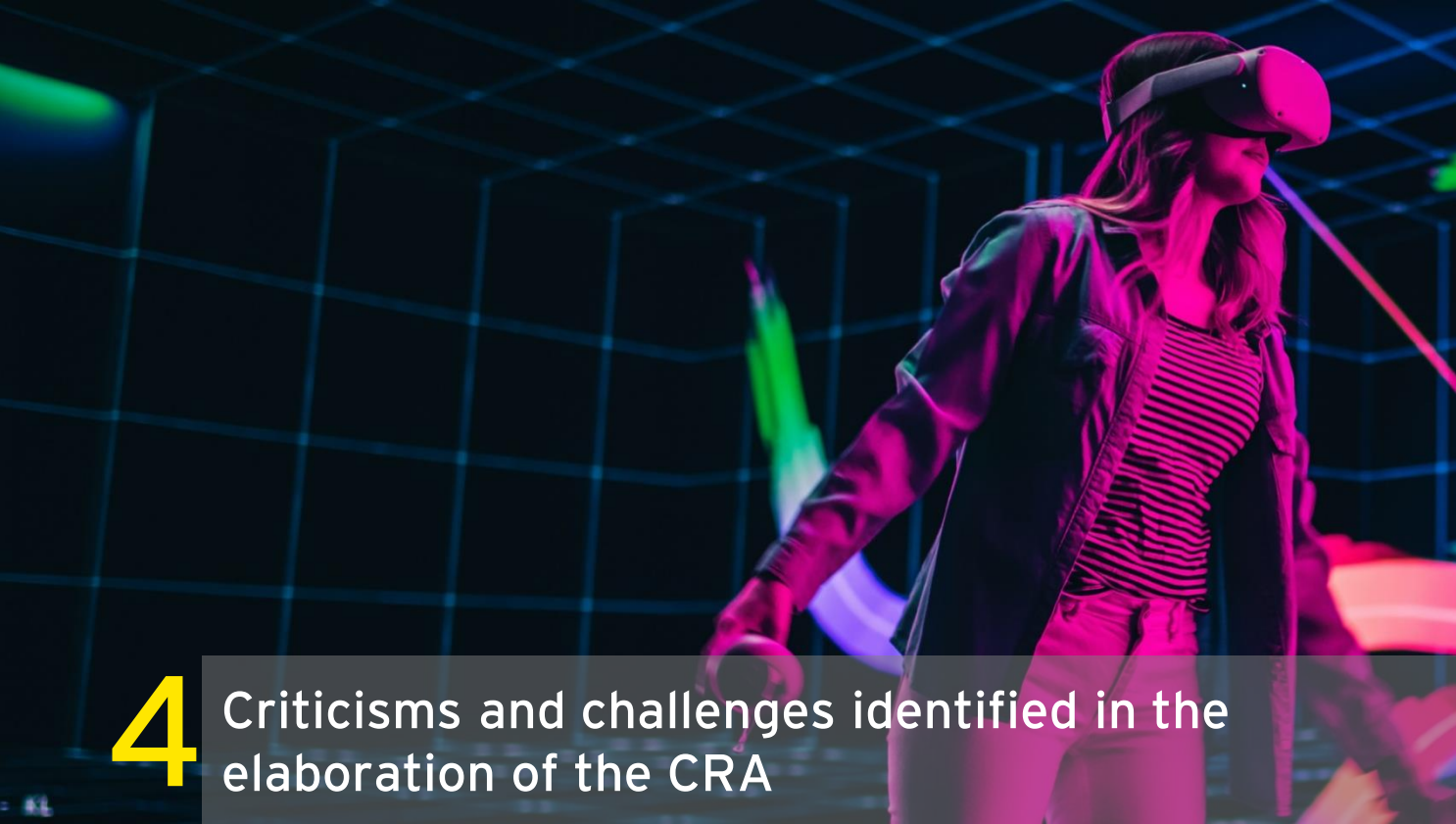
Manufacturers, importers, and distributors are required to actively monitor products with digital elements for cybersecurity risks and to take corrective actions when necessary. They must report significant cybersecurity incidents and vulnerabilities to the designated authorities, following the protocol set out in the regulation^{25,26}.

These authorities will be appointed by the Member States and oversee the enforcement of CRA’s obligations. They are granted authority to take actions against non-compliance, including demanding corrective measures, restricting product availability, or imposing fines.

The CRA prescribes stringent penalties to deter non-compliance, which vary depending on the severity of the infringement and the economic operator involved.

31 [Cybersecurity of connected products could improve significantly following Commission proposal \(beuc.eu\)](https://www.beuc.eu)

32 [PRESS RELEASE: TIC Council Welcomes the European Commission’s Proposal for a Cyber Resilience Act :: TIC \(tic-council.org\)](https://www.tic-council.org)



4 Criticisms and challenges identified in the elaboration of the CRA

During the public consultation on the proposed CRA, several key issues were raised by industry experts, companies, and other stakeholders, highlighting the potential challenges that the regulation might introduce. Among these concerns are the unwanted exposure of vulnerabilities caused by the vulnerability disclosure requirements³³.

The CRA's requirement for companies to disclose vulnerabilities within 24 hours of being discovered, before a patch or mitigation is available or widely deployed, could inadvertently lead to increased exposure to cyber threats, as *"government agencies would have access to a real-time software database with unpatched vulnerabilities"*³⁴, making them susceptible to be exploited by malicious actors.

These disclosure requirements prove to be a challenge particularly with vulnerabilities in the supply chain, due to its extensive scope and a shortage of capacity for conformity assessments, which could result in delays or

barriers to placing secure products on the EU market, that cause a disruption in the single market and negatively impact Europe's competitiveness³⁵.

Another issue that was raised is the limitation on agility in product development and availability. There was a concern that the CRA, with its stringent conformity assessments and regulatory requirements, might slow down the pace of innovation as tech companies and startups often operate with a fast-paced development cycle to stay competitive and respond to market needs. The conformity assessments, especially for critical products that require third-party validation, and the administrative burden of the regulatory paperwork and compliance processes may lead to longer product development cycles, impacting the time it takes for new products to reach the market and potentially discouraging their introduction³⁵.

³³ [Cyber Resilience Act text, Article 11 \(15.9.2022\) \(european-cyber-resilience-act.com\)](#)

³⁴ [Cyber Resilience Act: Disclosure requirement concerns raised by experts - Euractiv](#)


³⁵ [Cyber Resilience Act: da cooperação europeia ao risco de exposição \(itsecurity.pt\)](#)



In general, stakeholders emphasized the need for a nuanced approach that ensures cybersecurity without hindering innovation or inadvertently increasing cyber risks. These concerns from the public consultation have since contributed to the shaping and refinement of the final text of the CRA³⁶.

The updated regulation now requires manufacturers to report cybersecurity incidents and vulnerabilities simultaneously to the national Computer Security Incident Response Teams (CSIRTs) and to the EU's cybersecurity agency, ENISA. Member states are also encouraged to create a "*single reporting platform*" as an entry point to facilitate these reporting obligations, and CSIRTs must share incident reports through a centralized platform, with the discretion to delay sharing sensitive information for cybersecurity reasons³⁶.

³⁶ [EU ambassadors set to endorse new cybersecurity law for connected devices - Euractiv](#)



5 Potential impacts for organizations

The CRA is expected to bring significant impacts in both the public and private sectors, with a set of positive and negative consequences³⁷.

Positive impacts

In the **public sector**, the implementation of the CRA is expected to lead to **improved cybersecurity defenses** across digital products and services used by citizens. This security reinforcement is important as it underpins governmental operations and public services. Consequently, a more secure digital environment is anticipated, fostering **public trust** in digital services provided by governments.

Additionally, the **private sector** stands to benefit from the CRA through enhanced **reputational gain**. Companies that ensure adherence to the CRA's stringent cybersecurity requirements can market this compliance as a testament to their dedication to security, thus potentially boosting their reputation among

consumers and within the industry and leading to a higher demand for their products. Moreover, the standardization of cybersecurity across the EU presents businesses, especially small and medium-sized enterprises (SMEs), with the opportunity to expand their market share through a *“seamless access to the internal market and a reduction of market fragmentation”*³⁷.

The Cyber Resilience Act may also serve as a benchmark for cybersecurity standards beyond the European Union. The Act's EU-based standards will aid in its adoption and could provide a competitive advantage for EU manufacturers in international markets.

³⁷ [Cyber Resilience Act - Impact assessment | Shaping Europe's digital future \(europa.eu\)](#)



Negative impacts

However, these advancements come at a cost.

For **public entities**, the **economic burden of establishing, updating, and maintaining the mechanisms for regulation enforcement and oversight** could be substantial. The operational workload of consistently guiding and monitoring the compliance efforts of the private sector can also negatively influence costs.

The **private sector**, particularly SMEs, might feel the economic efforts more significantly, since there is a **substantial financial investment** in aligning products with the new cybersecurity requirements, a challenge which could strain resources and impact their economic sustainability³⁵. A **delayed introduction of products to the market** due to compliance

hurdles could also lead to a loss of competitiveness in the global digital landscape. Furthermore, the operational costs - from conducting conformity assessments to maintaining detailed documentation and managing reporting procedures - are likely to increase operational costs for businesses.

There is also the possibility that the EU standards based on the Act could end up not being sufficiently valued in the global markets to reflect a significant competitive advantage for EU manufacturers, in which case the investments made would result in substantial financial losses for businesses.

Overall, as the CRA takes effect, it will be instrumental in reducing the frequency of cybersecurity incidents and lowering the costs associated with managing such events⁵. Nevertheless, both sectors will have to navigate the trade-offs between the immediate financial and operational strains against the longer-term prospects of enhanced digital security and trust. While the private sector may bear the brunt of the short-term challenges, the public sector's role in providing oversight and the communal benefits of a more secure digital marketplace signify a shared journey towards a more cyber-resilient future.



6 Potential impacts for consumers

The implementation of the CRA is also likely to have both beneficial and disadvantageous impacts for consumers, derived from its focus on improving the cybersecurity of products with digital elements.

Positive impacts

On the benefit side, consumers stand to gain considerably from the CRA's emphasis on a higher general level of security³⁵. Products reaching the market will have been subjected to rigorous cybersecurity assessments, ensuring that consumer data and privacy are better protected. The reduction in vulnerabilities at the point of purchase translates into a lower risk of cyber incidents, which can compromise personal information and lead to financial or other forms of loss.

Moreover, strict reporting requirements for vulnerabilities and incidents mean that consumers can expect transparency from manufacturers and remain more well informed about the digital products they use³⁷. This could also result in better and more timely support should any security issues arise.

Negative impacts

One of the main impacts on consumers is the increase in the prices of digital products³⁷. As described in the previous section, in order to comply with the CRA's requirements, manufacturers may incur additional costs associated with the design, testing, and certification of these products to meet new cybersecurity standards. These increased costs could be passed on to the end users and consumers, raising the retail price of products ranging from smart devices to software applications. The requirement for ongoing security updates and support throughout a product's lifecycle could further contribute to higher initial costs for such products.



In essence, the CRA provides a framework that is expected to raise the overall security of digital products, although it may also introduce higher costs for consumers due to the investments required from organizations to achieve compliance. Ultimately, while consumers might notice an increase in prices, this is weighed against the enhanced security and peace of mind from using products that adhere to stringent European cybersecurity standards.



7 Procedures for CRA compliance

This new legislative framework introduces stringent requirements, to ensure the security of products with digital elements, that organizations must now take critical steps to adhere to.

To achieve compliance with the CRA, an organization must follow the following procedures:

Scope Definition: Determine which products in the organization's portfolio, including those already on the market, fall under the CRA's purview by assessing their digital elements.

Documentation: Create relevant documentation and evidence to prove a product's exemption from the CRA in a clear manner, for communication to authorities if needed.

Cross-Industry Consideration: Evaluate whether products are used across different industries or for purposes that may not be exempt, ensuring compliance in those cases where the CRA applies.

Risk Assessment: Conduct cybersecurity risk assessments for planned products to identify and address vulnerabilities from the outset (security by design).

Consumer Information: Ensure that end-users are well-informed about cybersecurity matters related to the products they are using.

Incident Reporting: Set up a process for immediate reporting of security incidents to users and relevant authorities.



Product Categorization: Meticulously categorize the company's product portfolio according to the CRA classifications, such as products that fall under the important or critical products of class I or II and document this categorization thoroughly.

Product Lifecycle Monitoring: Continuously monitor all products throughout their lifecycle for cybersecurity issues and maintain a proactive stance on product security management.

Security Updates: Establish a system for providing security updates to users promptly and without additional charge, as stipulated by the CRA.

These procedures will help an organization align its products and processes with the CRA's requirements, enhancing the overall cybersecurity posture and contributing to a proactive approach to cybersecurity governance that mitigates risks and aligns with the EU's vision for a resilient digital economy.

8 Conclusions

The CRA is a pivotal EU legislation aimed at setting comprehensive cybersecurity standards for products with digital elements and the processes involved in their production. It outlines specific compliance obligations for organizations and conformity assessments manufacturers must undertake to ensure their products meet essential requirements, with different levels of scrutiny based on the product's significance and potential impact.

In the event of non-compliance, authorities have the power to enforce corrective actions, restrict or ban products from the market, demand recalls or withdrawals, and issue fines, within the maximum fine thresholds established.

The CRA will be fully applied 36 months from the date of its entry into force, by then organizations should be compliant with the new requirements it introduces, excluding the reporting of vulnerabilities that should already be applied 21 months from its entry into force.

As for its reach, the CRA could set a global cybersecurity benchmark, facilitating

implementation and supporting EU manufacturers in competing on the global scale.

From the authors' perspective, the CRA could have a profound impact. The authors see the Act as an essential step towards harmonizing cybersecurity regulations, which will benefit businesses by providing clear, unified standards. The authors anticipate that the CRA will foster greater trust in digital products among consumers, improve overall product safety, and present new competitive opportunities for businesses adhering to high cybersecurity standards. Furthermore, The authors expect the CRA to drive innovation in cybersecurity measures as companies strive to meet these new requirements, ultimately reinforcing the global standing of EU digital products.



Disclaimer

Our analysis was based solely on publicly accessible information. We assume that the information provided to us (or the assumptions made by us) are complete and accurate. We have not conducted an independent review of the same and have not otherwise verified facts, nor the assumptions taken for the purposes of this analysis. A misinterpretation or omission of any circumstances and the alteration or modification of any facts or assumptions on which we based our analysis may require the alteration of part or all of the report.

Our report was prepared in June 2024. We are not obliged to update our comments in connection with circumstances or changes in law or facts or assumptions that occur after that date. The comments contained herein do not bind public authorities and courts, and we cannot guarantee that said authorities will not adopt a position different from the approach expressed above.

Authors



Paulo Moniz

Director
EuroDefense Portugal
moniz.paulo@gmail.com



Jorge Libório

Partner, Cybersecurity
and Technology
Ernst & Young S.A.
jorge.liborio@pt.ey.com



Luís Avilez

Manager, Cybersecurity
Ernst & Young S.A.
luis.avilez@pt.ey.com

