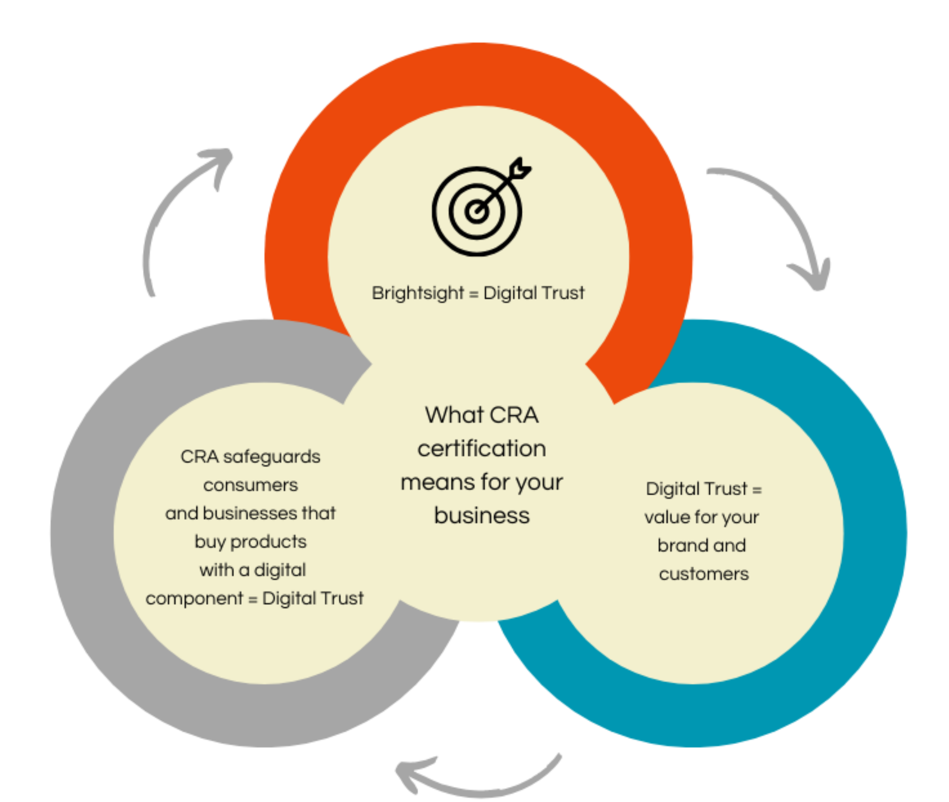
Brightsight - **Cyber Resilience Act**
Piecing together the puzzle to achieve CRA compliance

brightsight

By SGS


Brightsight = Digital Trust
What CRA certification means for your business
CRA safeguards consumers and businesses that buy products with a digital component = Digital Trust
Digital Trust = value for your brand and customers

CRA IN SHORT

The Cyber Resilience Act (CRA), also known as Regulation (EU) 2022/2847, is legislation that governs the cybersecurity of all connectable software and hardware products including its remote data processing solutions made available on the EU market. It ties in with the mission of working on digital trust. And therefore, creating value for the end-user, your customer. The CRA enhances the level of cybersecurity in many products, and enforces timely security updates for products and software.

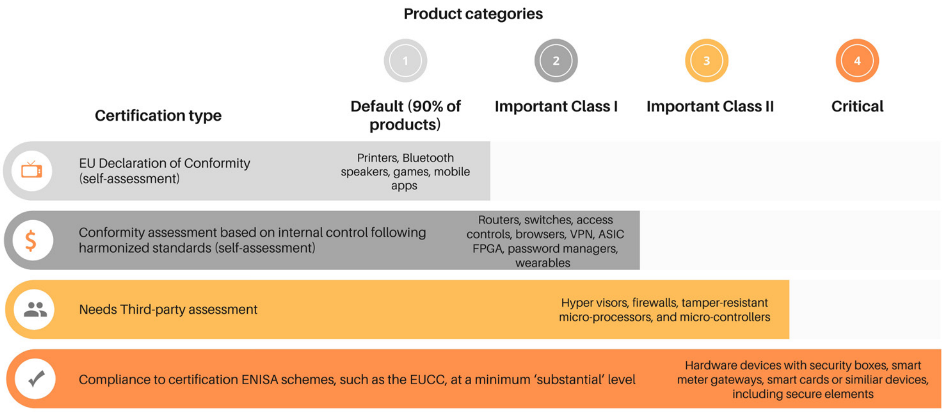
The three critical components of cyber resilience are risk mitigation, incident recovery and response, and business continuity.

FOR WHOM

The Cyber Resilience Act applies to economic operators such as manufacturers, software developers, distributors and importers who supply new or updated digital products to the European market. It is important to understand that, unlike NIS2 or DORA, the CRA regulates products, not entities.

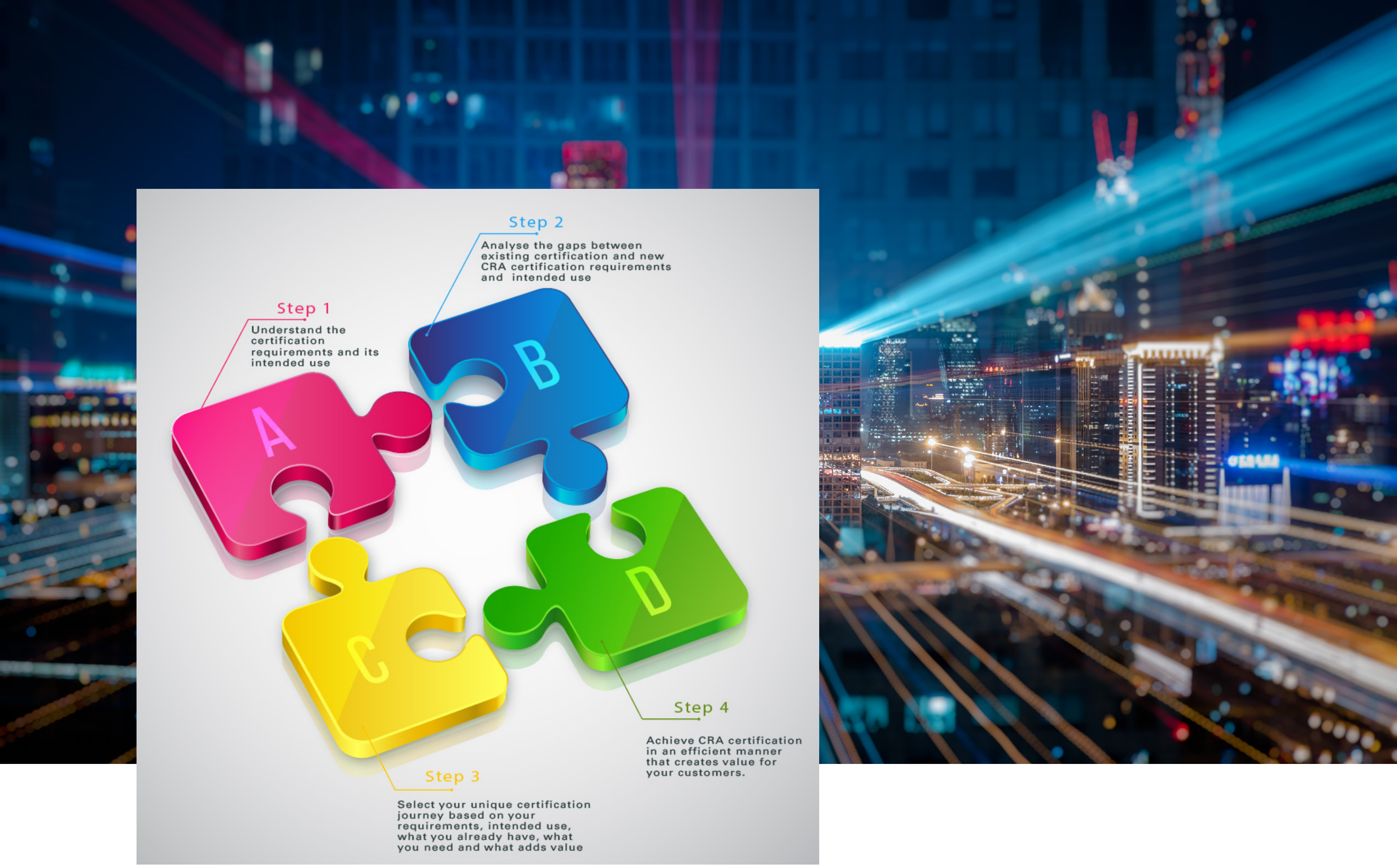
In a traditional sense, we can expect that an organization that stores sensitive or highly desirable items, such as a bank, is regulated. However, the same is not to be expected of a smartwatch or a baby monitor. At least, up until now. We soon will be expecting that an IoT product cannot be subject to hacking for instance to endanger its users.

Together, we need to reduce the risk that hackers can compromise the security of a connected device. Compliance to the CRA essential requirements creates an added value for your product since its users will be assured of its security, with regards to the risks associated with the intended use of the product levels.



Product categories

Certification type	1 Default (90% of products)	2 Important Class I	3 Important Class II	4 Critical
EU Declaration of Conformity (self-assessment)	Printers, Bluetooth speakers, games, mobile apps			
Conformity assessment based on internal control following harmonized standards (self-assessment)		Routers, switches, access controls, browsers, VPN, ASIC FPGA, password managers, wearables		
Needs Third-party assessment			Hyper visors, firewalls, tamper-resistant micro-processors, and micro-controllers	
Compliance to certification ENISA schemes, such as the EUCC, at a minimum 'substantial' level				Hardware devices with security boxes, smart meter gateways, smart cards or similiar devices, including secure elements


Step 1
Understand the certification requirements and its intended use
Step 2
Analyse the gaps between existing certification and new CRA certification requirements and intended use
Step 3
Select your unique certification journey based on your requirements, intended use, what you already have, what you need and what adds value
Step 4
Achieve CRA certification in an efficient manner that creates value for your customers.
A
B
C
D

The fact that you are contributing to a create digital trust is an important value proposition.

By improving the security of products with digital elements, the CRA contributes to strengthening the digital resilience of all users, and thus of the entire European ecosystem.

The Cyber Resilience Act differentiates four categories among the products it regulates:
1. The Default category
2. Important products of Class I
3. Important products of Class II
4. Critical products

It's important to understand this classification, as it determines the conformity assessment procedure required for each product.

The more critical the product, the more rigorous the assessment will be — meaning the involvement of a third-party that is required for:

Important Products Class II
1. Hypervisors
2. Firewalls, intrusion detection and prevention systems;
3. Tamper-resistant microprocessors;
4. Tamper-resistant microcontrollers.

Critical Products
1.. Hardware Devices with Security Boxes
2. Smart meter gateways
3. Smartcards or similar devices, including secure elements

More resources
For a complete explanation we refer you to the following resources:
• CRA Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)
https://eur-lex.europa.eu/eli/reg/2024/2847/oj
• New legislative framework that clarifies the use of CE marking and creates a toolbox of measures for use in product legislation.
https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en
• ENISA (European Union Agency for Cybersecurity)
The ENISA website focuses on enhancing cybersecurity across the EU. It provides in-depth resources regarding the Cybersecurity Resilience Act.
https://www.enisa.europa.eu/topics/cs-resilience
• Council of the European Union – CRA Documents
Offers documents related to the CRA, including drafts, working group discussions, and position papers from various EU member states.
https://www.consilium.europa.eu/en/documents-publications/publications/
• The Blue Guide on the implementation of the product rules 2022:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC

PIECING TOGETHER THE CERTIFICATION PUZZLE

With our solid proof in security evaluation experience, Brightsight can solve your certification puzzle and show you what is missing. The missing pieces of the puzzle we try to identify with a gap analysis and to determine how to obtain certification in an efficient manner.

The Cyber Resilience Act does not exist in a vacuum. This act will complement the existing EU NIS2 Directive, however, as mentioned before, this directive is aimed at organizations, whereas CRA is aimed at products, Additionally, the CRA also closely resembles existing cybersecurity standards, including SESIP, EN 303 645, PSA EN 18031.

If you have already achieved compliance with the above-mentioned standards, you might be close to achieving compliance with the Cyber Resilience Act in the future.

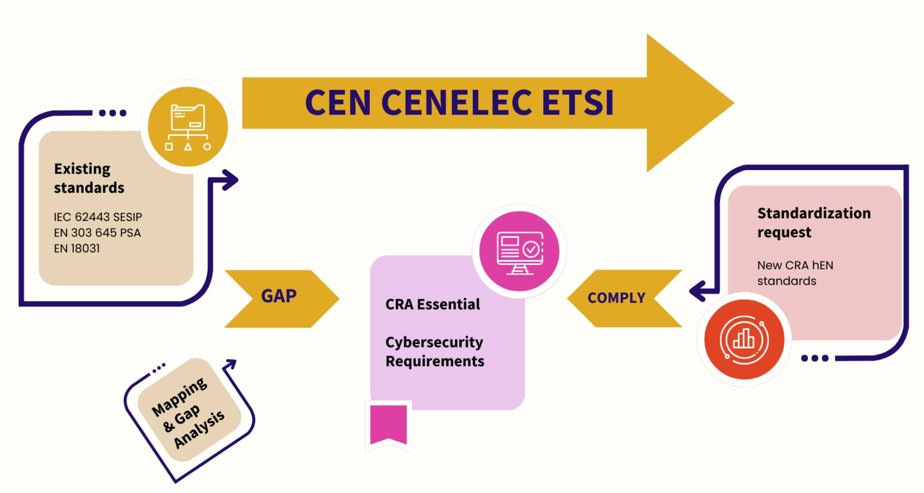
What does this specifically mean for your business? How do you identify the gaps? That is exactly where Brightsight comes in. Solving the pieces of the puzzle through a gap analysis. In a way that is valuable to your business and beneficial to your customers. The CRA spans a wide range of products, and Brightsight can offer value added services in the whole value chain. However, the important class 2 products and the critical products require mandatory third-party certification.

Need to know more? We would be happy to assess your puzzle and try to solve it together during an in-depth tailored presentation how to achieve CRA certification for your business.

Send an e-mail to brs.sales@sgs.com to start the conversation!

Timelines
Get ready now! You have until 2027 to get ready for this mandatory certification.

- 2024 CRA enters into force
- Sept 11, 2026 Incident reporting becomes mandatory, also for non-certified products
- Dec 11, 2027 CRA in full effect


CEN CENELEC ETSI
Existing standards
IEC 62443 SESIP
EN 303 645 PSA
EN 18031
GAP
Mapping & Gap Analysis
CRA Essential
Cybersecurity Requirements
COMPLY
Standardization request
New CRA hEN standards