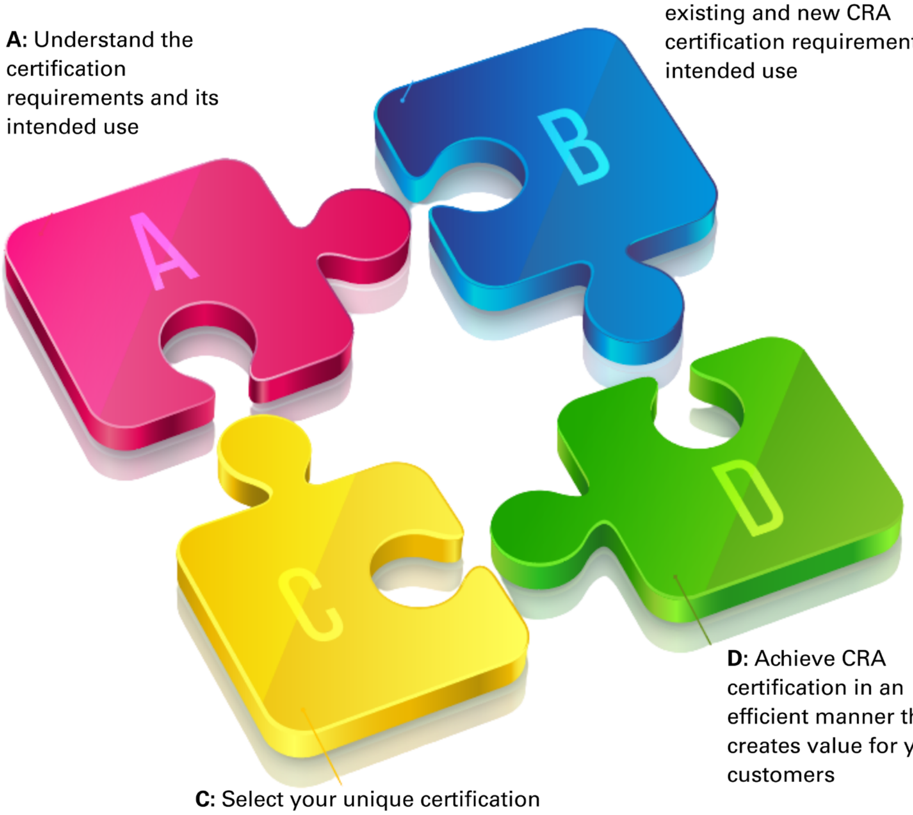


A: Understand the certification requirements and its intended use

B: Analyse the gaps between existing and new CRA certification requirements and intended use

C: Select your unique certification journey based on your requirements, intended use, what you already have, what you need and what adds value

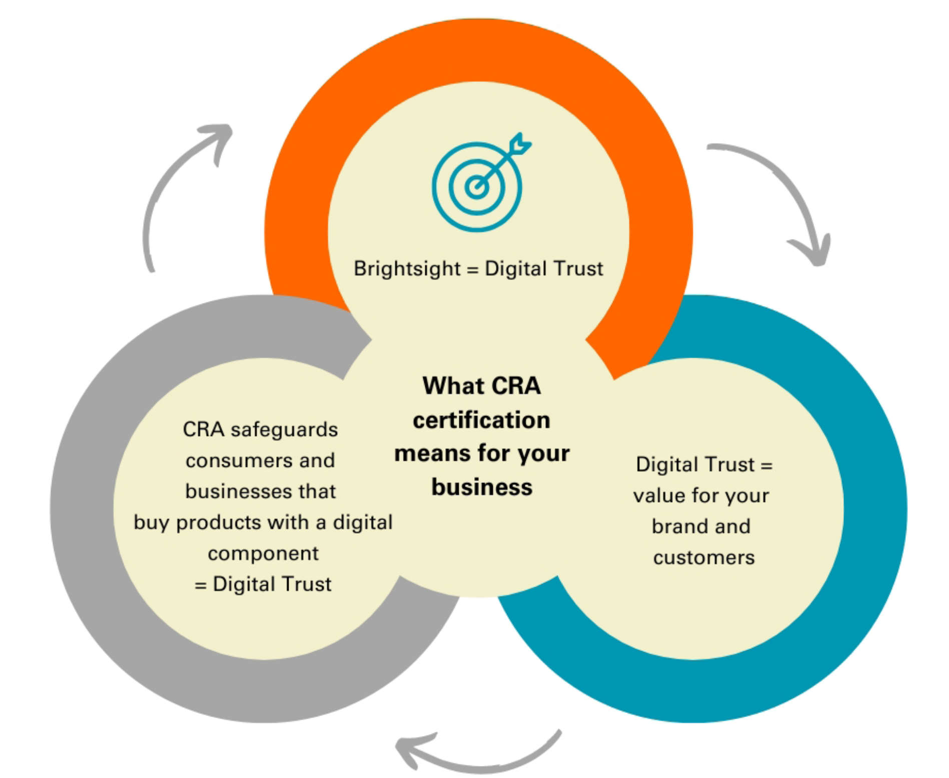
D: Achieve CRA certification in an efficient manner that creates value for your customers

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

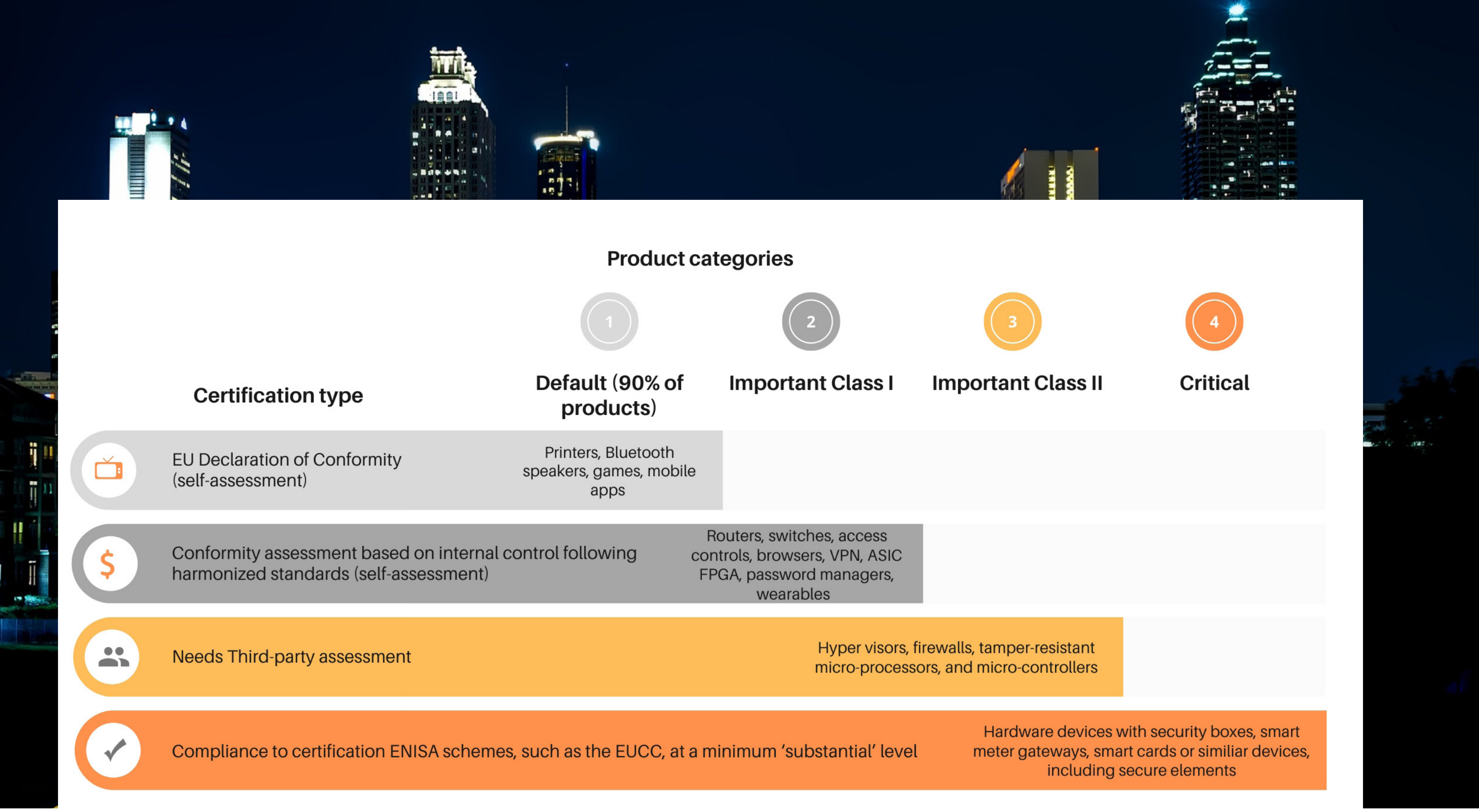
The Cyber Resilience Act applies to economic operators such as manufacturers, software developers, distributors and importers who supply new or updated digital products to the European market. It is important to understand that, unlike NIS2 or DORA, the CRA regulates products, not entities.

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.

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



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

It is 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 conformity assessment, 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

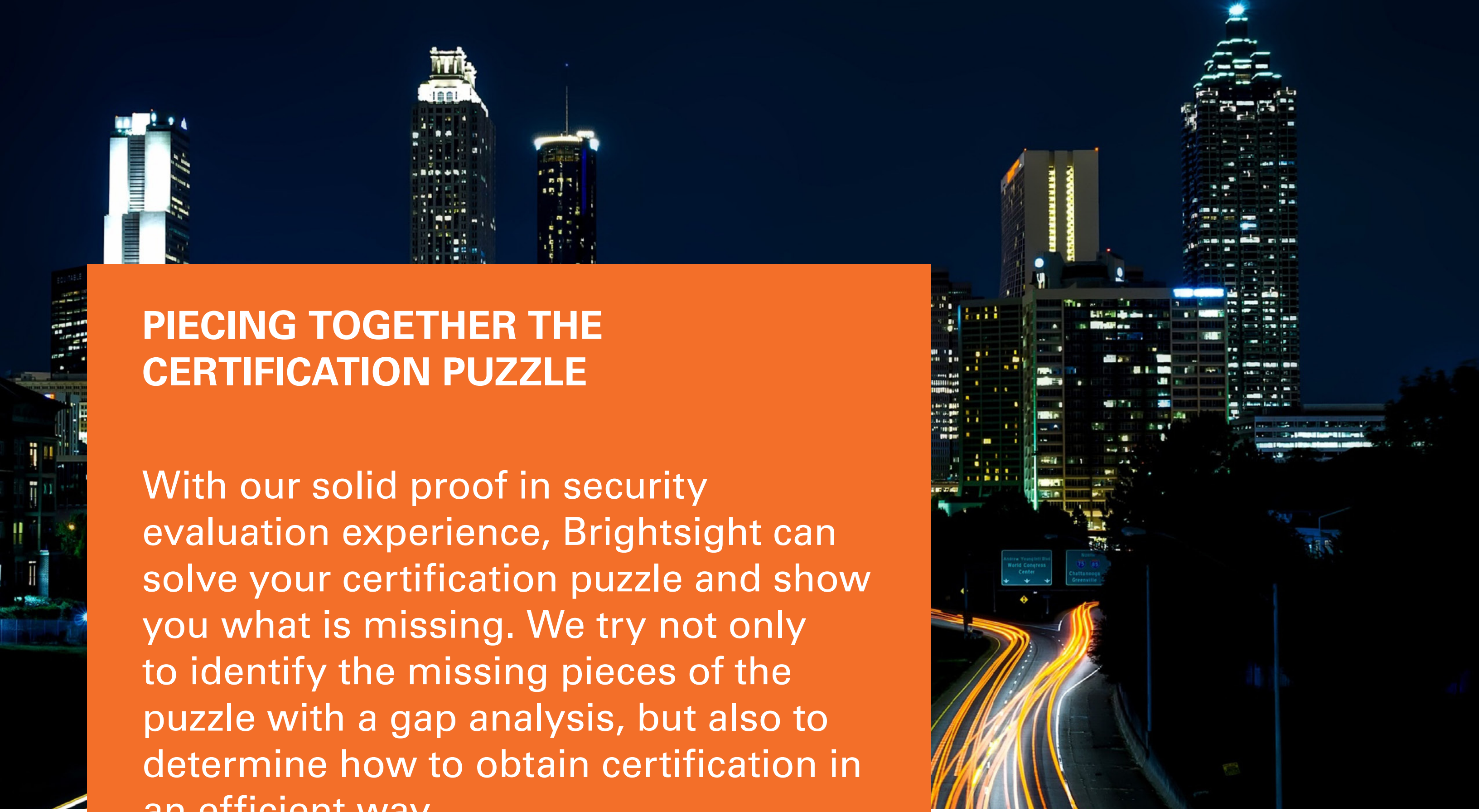
Further reading

- 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).

- New legislative framework that clarifies the use of CE marking and creates a toolbox of measures for use in product legislation.

- The website of the European Commission provides background information on the EU cybersecurity strategy, legislation and certification and the Cyber Resilience Act

- The Blue Guide on the implementation of the product rules 2022.



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. We try not only to identify the missing pieces of the puzzle with a gap analysis, but also to determine how to obtain certification in an efficient way.

The Cyber Resilience Act does not exist in a vacuum. This act will complement the existing EU NIS2 Directive, which is aimed at organizations, whereas the 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.

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

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, when it comes to the important class 2 products and the critical products, both require mandatory third-party certification.

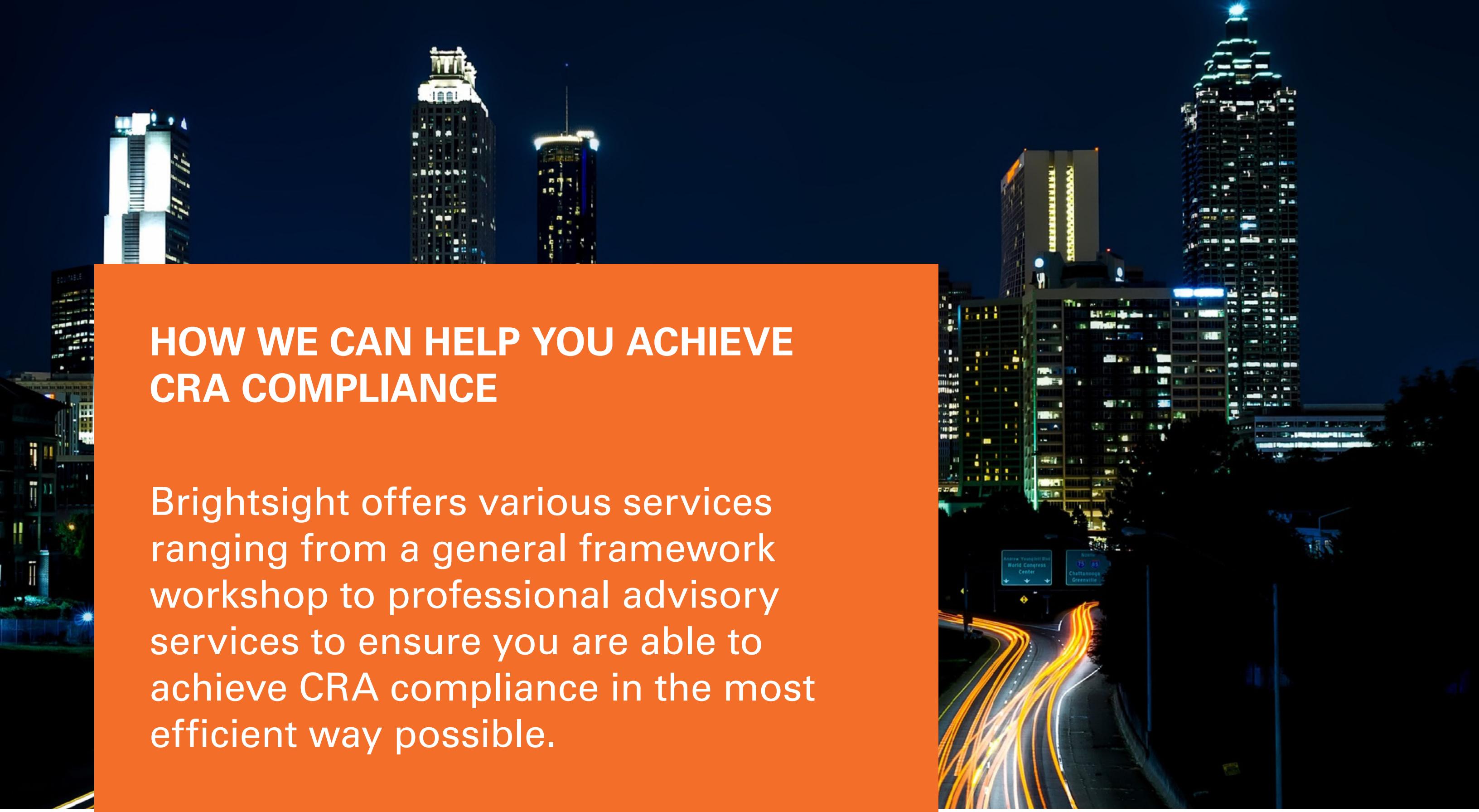
Need to know more? We would be happy to assess your puzzle and try to solve it together during an in-depth tailored presentation how to achieve CRA certification for your business.

Our CRA services include:

General CRA framework workshop (2 hours)
Gain a foundational understanding of the European Union's Cyber Resilience Act (CRA) through our comprehensive introductory workshop.
This session provides a clear overview of the regulation's timelines, scope and key content.
Participants will gain insights into the essential requirements and the strategic implications for their organization.

Product-specific CRA workshop with regulatory focus (4-6 hours)
Building upon the general CRA framework, this in-depth workshop delves into the specific implications of the CRA for your organization's product(s).

Gain a full understanding of the CRA requirements that are already covered by the product-related standards and the CRA requirements that require further product-specific assessment.



HOW WE CAN HELP YOU ACHIEVE CRA COMPLIANCE

Brightsight offers various services ranging from a general framework workshop to professional advisory services to ensure you are able to achieve CRA compliance in the most efficient way possible.

This session includes the core content of the general workshop, augmented by 2-4 hours dedicated to:

- Your product focus: A detailed analysis of how the CRA applies to your specific product(s).
- Standard mapping: Mapping relevant for European and international product standards (for example: PCI, Common Criteria, GBIC, RED) against the specific requirements of the CRA.
- GAP analysis: Identifying potential gaps between the existing product standards and the mandatory requirements of the CRA.

Product-specific CRA gap assessment

Utilize our expertise to thoroughly assess your product(s) gaps against the CRA requirements.

This service contains a review of your existing documentation and processes against the CRA requirements in order to identify any discrepancies or gaps. It also includes a risk analysis review.

As output, our gap assessment offers actionable insights for remediation, helping you determine which CRA requirements your product conforms to and which ones it fails, and so needs improvement.

CRA support

Following the gap assessment, we can provide additional guidance to help you close the identified gaps and achieve CRA compliance.

CRA-ready certification

Upon a successful completion of the product-specific GAP assessment and after a closure of identified gaps, we offer a "CRA-ready" certificate. This certification reflects the current status of your product's alignment with the CRA essential requirements. The findings from our gap assessment may also be leveraged during future conformity assessments with Notified Conformity Assessment Bodies (CABs), streamlining your product's certification process.

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

Stay up-to-date with Brightsight's news, updates and latest CRA developments by following us on LinkedIn.

Brightsight - **Building digital trust**

brightsight

By SGS