Cyber Resilience Certificate of Conformity

Get ready for the new EU Cyber Resilience Act (CRA). Assess your level of adherence to the CRA Essential Cybersecurity Requirements and improve the cyber resilience maturity of your product and company processes. The Applus+ Cyber Resilience Mark assesses the products' adherence to the CRA (Cyber Resilience Act) essential requirements, for ‘Default’ or ‘Unclassified’ categories.

The CRA regulation is expected to enter into force in the second half of 2024, and manufacturers will have 36 months to apply its requirements, excepting a more limited 21-month period for the reporting obligation of manufacturers for incidents and vulnerabilities. CRA will impact a wide range of businesses selling their digital products in Europe, but with different degrees of stringency. Read our publication to get a deeper understanding of the CRA essential requirements and affected products.

All vendors affected by the new regulation should start preparing, as compliance will affect the product development at its core, to assess the company’s cyber resilience maturity. Applus+ Laboratories has developed a new Certificate of Conformity aimed at vendors of non-critical products that will qualify as ‘Default’ or ‘Unclassified, as defined by the CRA. Around 90% of the impacted products are expected to be in this category. Although those vendors can opt for a self-assessment, compliance with CRA requirements would be a legal obligation, including the provision of all the evidence needed (with potential fines for non-compliant companies).

Cyber Resilience Evaluation Methodology

Applus+ Laboratories has developed an internal methodology, settled in the European Fixed-time cybersecurity evaluation methodology for ICT products (FITCEM) EN 17640: 2022.

FITCEM EN 17640:2022 is a generic framework to develop evaluation methodologies based on a set of pre-defined tasks. It was developed by CEN CENELEC to standardize existing national methodologies like LINCE (Spain), CSPN (France) or BSZ (Germany) with the participation of Applus+ Laboratories experts as co-editors. Our internal methodology is an instantiation of FITCEM, tailored to the future requirements of the CRA. Our experts in different technologies can analyze the specific needs depending on the type of product.

Evaluation tasks included in the service, as defined by FITCEM

- **Completeness check:** a completeness check to review that all the requested evidence is received by Applus+ Laboratories.
- **Review of security functionalities**: the mandatory risk analysis assessment conducted by the manufacturer is reviewed to ensure that the security functionalities are well-defined and cover the risks identified by the manufacturer.
- **Development documentation**: the processes and documents provided by the manufacturer are analyzed and the compliance with the requirements of the CRA regarding product and vulnerability handling are verified.
- **Vulnerability review**: a vulnerability analysis review based on public or known vulnerabilities for the product and its components is performed.

Evidence Needed for the Cyber Resilience Certificate of Conformity

The manufacturer shall provide the following evidence included in the Technical File /Technical Documentation (see CRA Annex II and Annex V):

- **Product description** including the identification of the product and the security functionalities, manuals, user guidelines, etc.
- A **description of the design** (functional specifications, cryptographic algorithms, modules, components…), development and production processes and vulnerability handling and patch management processes.
- An **assessment of the cybersecurity risks** against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of CRA. Risk assessment procedures and latest risk analysis.
- If applied, a list of the **harmonized standards, common specifications and cybersecurity schemes applied** in full or in part. If these harmonized standards, common specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements.

- **Reports of the tests** carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of CRA-Annex I.
- A copy of the **EU declaration of conformity** (optional, not needed for the current assessment).
- Where applicable, the **software bill of materials**, as defined in CRA-Article 3 point 36.

What do you get?

The outcome of the evaluation is a CoC (Certificate of Conformity) that lists how many requirements are accomplished from product and vulnerability handling requirements. The CoC will be accompanied with the right to use the Applus+ Cyber Resilience mark.

Why Choose Applus+'s Cyber Resilience CoC?

Applus+ Laboratories is your partner in building a cyber resilient digital future. We are one of the top 3 cybersecurity labs for Common Criteria certification. We are top-notch experts in security evaluation, offering more than 20 cybersecurity schemes for different verticals, from Payment to IoT, to Automotive or Cryptography for Defense applications.

Stay ahead of the upcoming cybersecurity regulations

Whether your products will classify as Default, Class I or Class II, the Applus+ Cyber Resilience Conformity mark:

- Showcases your organization's commitment to cyber resilience
- Reassures your clients and partners you are ahead of new requirements
- Positions you at the forefront of regulatory compliance

Contact us to learn more about how Applus+ Cyber Resilience Mark can elevate your cybersecurity posture and provide a competitive edge in today's digital world.