



EU Cyber Resilience Act – Readiness-Check

Are you ready for the future of Cyber Security?
Check how well prepared your company is for the emerging EU regulation.

AIM OF THE CYBER RESILIENCE ACT

With the Cyber Resilience Act, the EU aims to increase the security of products with digital elements. This regulation aims to strengthen cyber security of several levels and create uniform rules for the entire European internal market.

This protects both consumers and companies from digital threats and promotes transparent competition. At the same time, the complexity between the different regulatory approaches of the member states and the legislation of various product groups will be reduced.

BENEFIT FROM EARLY PREPARATION

As the regulation has not yet fully entered into force, you can save internal resources and avoid future compliance risks by preparing early. This includes for example, bans on the sale of certain products in the European internal market, exclusion from tenders and the associated loss of customers. Early preparation offers your company the opportunity to position itself strongly against the competition and stay one step ahead of the requirements.

Contact us now to optimally prepare your company for the requirements of the Cyber Resilience Act and strengthen your Cyber Security.

CHECK AT A FIXED PRICE - WITH FOCUS ON:

- 1. Briefing:** We explain the basic aspects of the regulation, including the obligations that companies must comply with and the consequences of non-compliance.
 - 2. Scoping:** We then jointly determine the role of your company within the Cyber Resilience Act. We clarify the extent to which the emerging requirements are applicable to your company and which compliance obligations will be relevant for you.
 - 3. Classification of your Products:** We check whether your products fall within the scope of the regulation and which specific requirements must be met.
 - 4. Report and „next steps“:** Finally, we draw up an individual action plan for your company. We offer ongoing support from initial planning to full implementation so that you can operate safely efficiently and in compliance with the regulation.
- Optional:** We also highlight the points of demarcation and overlap with the RED (Radio Equipment Directive) that are relevant to Cyber Security.

TÜV Rheinland i-sec GmbH
Am Grauen Stein · 51105 Köln
Tel. 0800 806 9000 3000
service@i-sec.tuv.com

www.tuv.com

 **TÜVRheinland**[®]
Precisely Right.