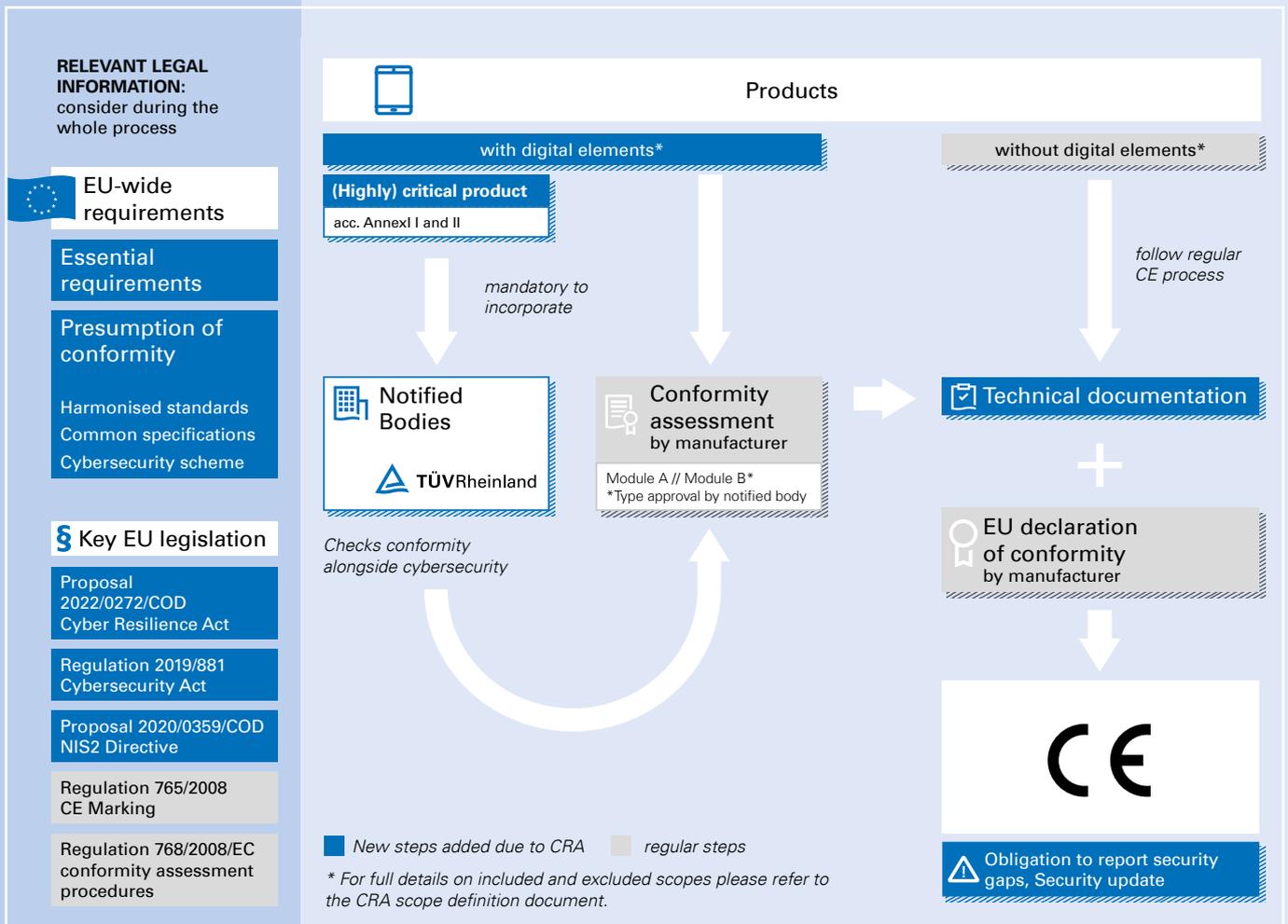


How the Cyber Resilience Act impacts CE Marking

With the **Cyber Resilience Act (CRA)** officially released, the European Union is introducing binding cybersecurity requirements for **products with digital elements**. The aim of the cybersecurity requirements for companies is to increase resilience against cyberattacks and to provide reliable digital services.

As part of this regulation, cybersecurity has become a **mandatory requirement for CE marking**. Manufacturers must demonstrate that their products comply with the new regulatory security standards and the company has adequate **vulnerability management** in place.

The CRA builds upon the established CE marking process but introduces additional cybersecurity-specific requirements. Manufacturers must now ensure that their products meet not only traditional **safety and environmental standards** but also the **cybersecurity provisions** outlined in the CRA, including secure software updates and risk management measures.



TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
service@i-sec.tuv.com
www.tuv.com/cra

[ONLINE CONTACT](#)

TÜVRheinland®
Precisely Right.