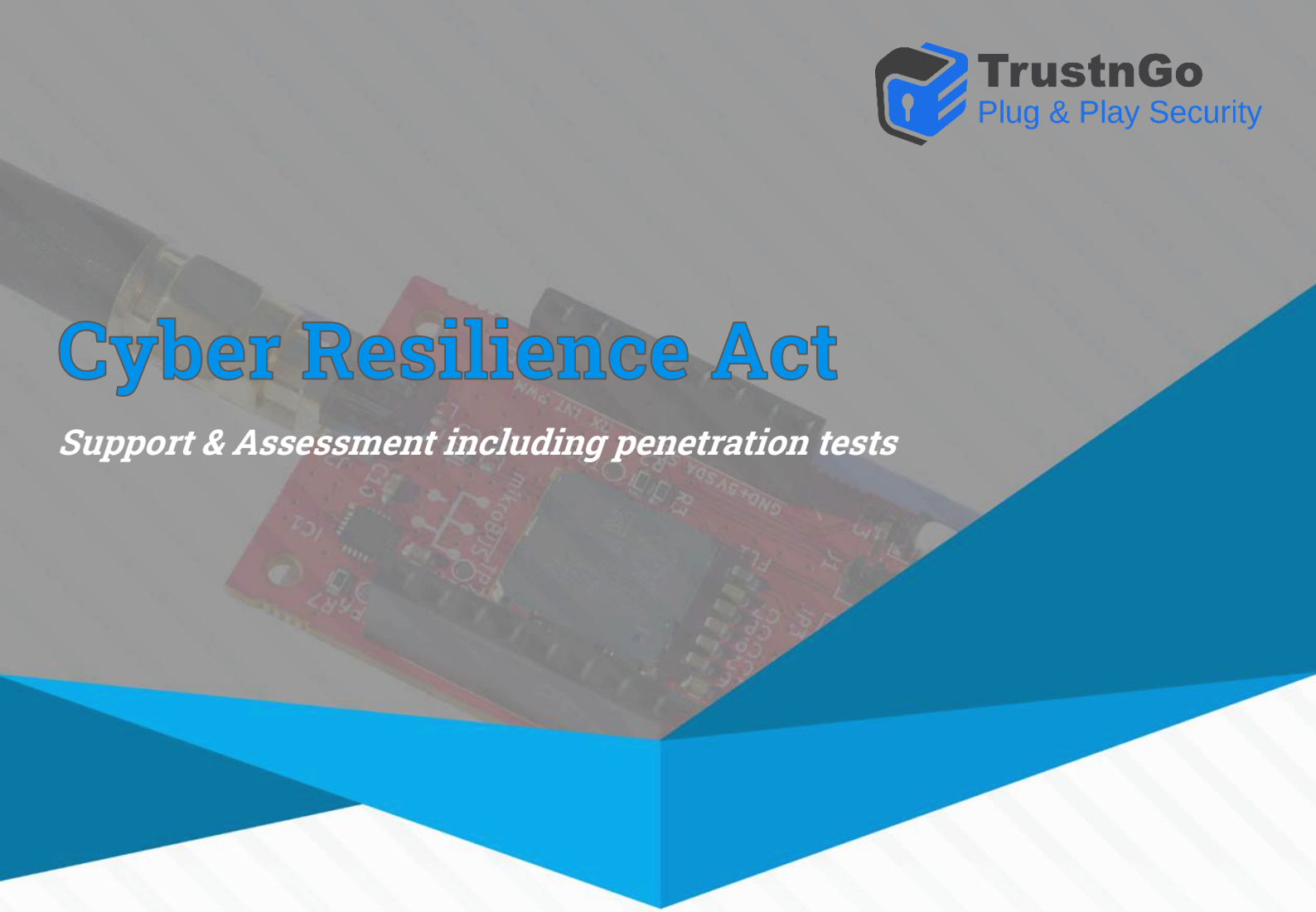
TrustnGo
Plug & Play Security



Cyber Resilience Act

Support & Assessment including penetration tests

In Brief

The **Cyber Resilience Act (CRA)** is a new EU regulation ensuring that all connected products — hardware or software — are secure by design and throughout their lifecycle. It requires manufacturers to manage cyber risks, provide timely security updates, and report incidents. From **December 2027**, products sold in the EU must comply and carry a **CE mark** proving cybersecurity conformity. The CRA builds consumer trust, strengthens digital safety, and harmonizes cybersecurity standards across Europe — making digital products safer and more reliable for everyone.

TrustnGo provides consulting, assessment & testing services to tackle these challenges and allow you to meet the requirements of the CRA the D-day.

One stop shop

From initial audit to full CRA compliance, TrustnGo manages the entire process including gap analysis, technical advice, documentation writing & pentests.

Integrated Technical & Regulatory expertise

TrustnGo combines deep knowledge of EU cybersecurity regulations with hands-on experience in securing digital products.

Time Savings and Risk Reduction

By anticipating CRA obligations, you secure your products early, minimize compliance risks and costs, and strengthen customer and partner confidence in your brand.

Why choose TrustnGo ?

Securing an embedded device can be a challenge and demonstrating this security is another one.

During the past years, the EU has severely tightened cybersecurity requirements for IoT & embedded devices. NIS2, RED Directive, CRA, Regulation of machinery, ... TrustnGo follows all these topics and has developed a comprehensive and cost-effective methodology based on our expertise in EN 303 645, EN 18031, IEC 62443-4-1/2, etc.

As a one-stop-shop, we also deliver technical advice on how to implement security functions, and we perform penetration testing to assess the robustness of your implementation.

We can act not only at the product level but also at the company level to achieve sustainable and reproducible compliance.

Consulting services

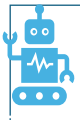
- **Self-Assessment according to**
  - EN18031, EN 303 645, IEC 62443-4
- **Integration of security features**
  - Secure bootloader
  - TrustZone & Secure Enclaves
  - Secure coms & Crypto. libraries
- **Secure Development Life-Cycle**
  - Code review & hardening
  - Secure supply chain & provisioning
  - Monitoring of vulnerabilities
- **Cryptography**
  - PKI management
  - Crypto. protocols analysis

Our approach to CRA


Mapping of products and processes


Gap analysis at organizational level


Define a compliance roadmap


Risk & Gap analysis at product level


Fix the gaps with our advice


Demonstrate compliance

Example case

A company selling solutions embedding a custom internet gateway, with wireless interfaces and already compliant to EN 18031-1/2, wants to comply with CRA requirements.

The solution is considered as a whole, including the backend and the related mobile application. A risk & gap analysis is conducted and the EN 18031's evidence are completed to demonstrate the conformity of the solution.

In addition, a secure development life cycle is deployed at company level and vulnerability management is fully integrated to the company's processes.

Third party penetration testing & certification

TrustnGo has partnership with ISO 17025 laboratories and ISO 17065 notified bodies. We help you bring your company and products into compliance and have this validated by recognized partners.

Version 1.0

TrustnGo
Plug & Play Security

https://trustngo.tech
+33 781 765 448
sales@trustngo.tech

TrustnGo S.A.S
20 rue Paule Marrot
33300 Bordeaux