Will the European Union certify my Bluetooth toothbrush?

Miguel Bañón
ISO/IEC JTC 1/SC 27/WG 3, “Security evaluation, testing and specification”
CEN/CLC/JTC 13/WG 3, “Security evaluation and assessment”
CEN/CLC JTC 13/WG 10, “Cryptography”

SHORT ANSWER:
IT DEPENDS ON THE TOOTHBRUSH FUNCTIONALITY.

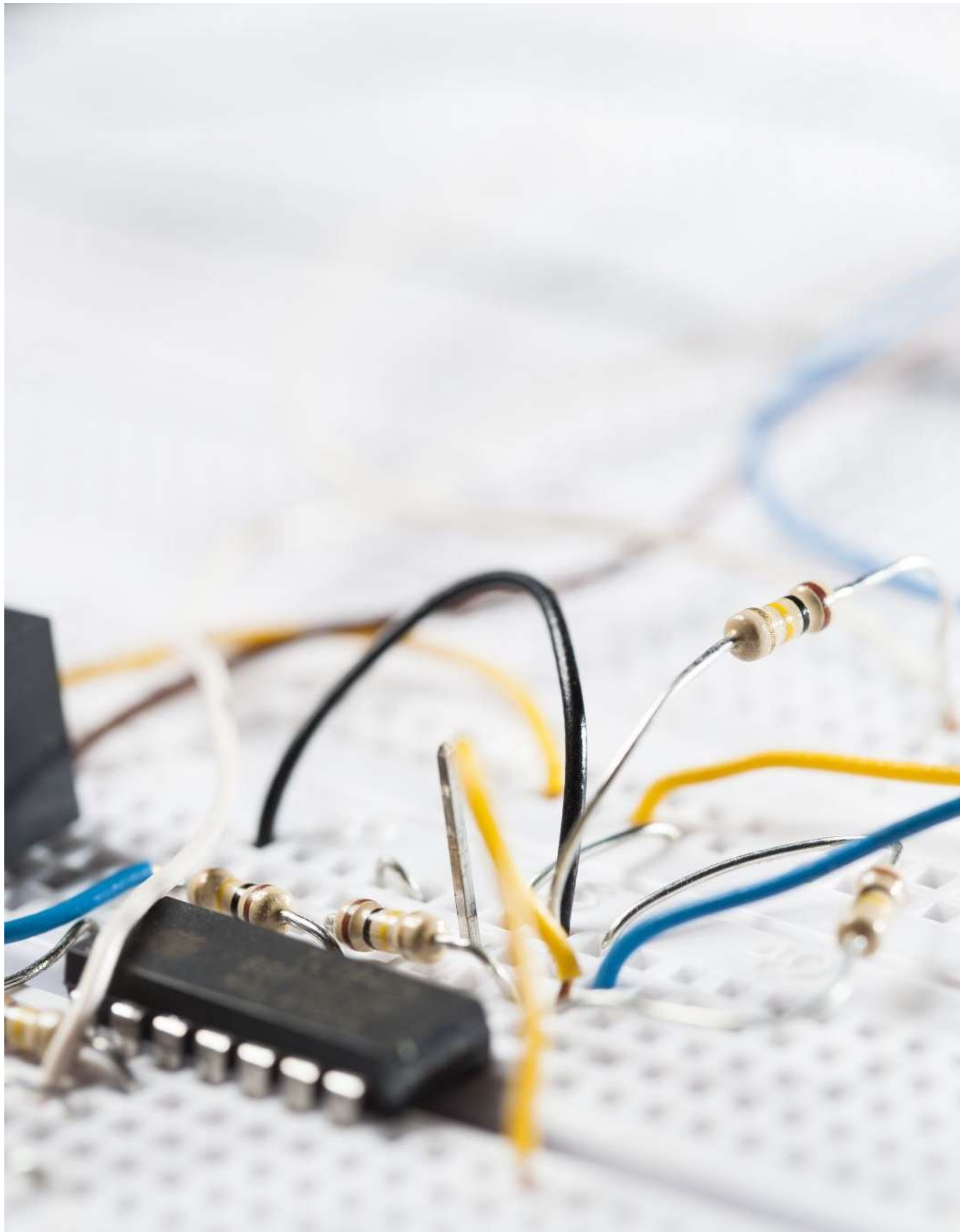
The EU New Legislative Framework (NLF) provides a modernized system for ensuring that products placed on the European market are safe and compliant with EU requirements.

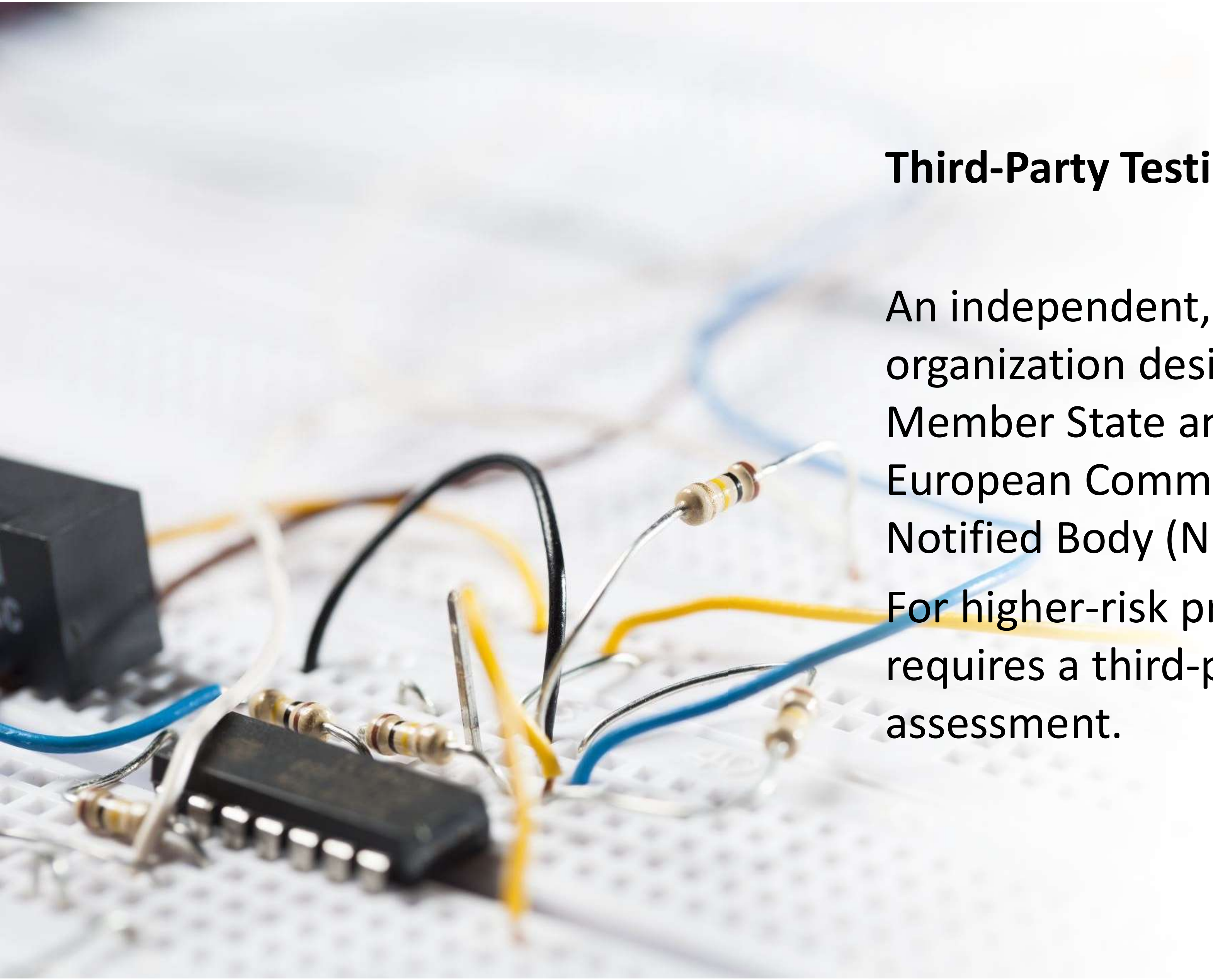
One important aspect of the NLF is the **conformity assessment**, which can involve **first-party**, **second-party**, or **third-party** testing — depending on the product risk and the applicable EU legislation (e.g., CE marking directives or regulations).

First party

The manufacturer tests their own product for conformity to EU requirements (such as safety, performance, and labeling).

This is allowed for low-risk products where legislation permits self-declaration of conformity (e.g., simple electrical devices under the Low Voltage Directive).





Third-Party Testing (Notified Bodies)

An independent, accredited organization designated by an EU Member State and notified to the European Commission — called a Notified Body (NB).

For higher-risk products, EU legislation requires a third-party conformity assessment.

Type	Performed By	Independence	Common For	EU NLF Role
First-party	Manufacturer	No	Low-risk products	Self-declaration, CE marking
Second-party	Customer or client	Partial	B2B supply chains	Extra assurance (not mandatory)
Third-party	Notified Body	Yes	High-risk products	Required by law for many sectors

Testing Party	Who Performs It	Residual Risk (Product)	Confidence Level (for Manufacturer & Public)	Typical Use Case
First-Party	Manufacturer (self-assessed)	**Low**	**Low to Medium** (reliant on internal control)	Simple, low-risk products (e.g., desk lamp)
Second-Party	Customer/importer	**Medium**	**Medium** (external but interested party)	Buyer wants assurance (e.g., OEM sourcing)
Third-Party	Independent Notified Body	**High**	**High** (objective and independent)	High-risk products (e.g., medical devices, pressure vessels)

Harmonized standard

A technical specification (like a European standard – EN) that is:

- Developed by a recognized European Standardization Organization (ESO):
    - CEN (European Committee for Standardization)
    - CENELEC (European Committee for Electrotechnical Standardization)
    - ETSI (European Telecommunications Standards Institute)

- Requested by the European Commission via a standardization mandate to support a specific EU legal act, such as a directive or regulation.
- Published in the Official Journal of the European Union (OJEU), which gives it legal status.

When a product complies with a harmonized standard:

It is presumed to conform to the essential requirements of the relevant EU legislation (e.g., safety, health, cybersecurity). This is known as the “presumption of conformity”.

Manufacturers can avoid having to prove compliance from scratch — unless the product is challenged.

THE RADIO EQUIPMENT DIRECTIVE

Under the Radio Equipment Directive (RED) 2014/53/EU, cybersecurity has become a key legal requirement, after the 2021 delegated act that added specific cybersecurity provisions (enforcement date, August 1, 2025).

Article 3(3)(d) – Protection of Personal Data & Privacy

Devices must not harm users’ personal data or privacy.

Article 3(3)(e) – Protection from Fraud

Devices must include features to prevent fraud (e.g., identity spoofing, phishing).

Article 3(3)(f) – Protection of Networks

Devices must not adversely affect the functioning of networks or misuse network resources.

Is a Bluetooth Toothbrush Subject to RED Cybersecurity Requirements?

RED Applies to All Radio Equipment

A Bluetooth toothbrush is radio equipment under RED 2014/53/EU because it uses Bluetooth (a radio communication protocol).

Article	What It Requires	Does It Apply to a Bluetooth Toothbrush?
3(3)(d)	Protection of **personal data and privacy**	**Yes, if** the toothbrush collects/transfers **user data** (e.g., brushing habits, geolocation, usage linked to identity)
3(3)(e)	Protection from **fraud**	**Yes, if** there is **payment, account, or cloud access** involved (e.g., app with account login)
3(3)(f)	Protection of **network and misuse of resources**	**Yes, if** the device could be **exploited** (e.g., becomes part of a botnet, sends malformed data)

Functionality	RED Art. 3(3) Applies?
Only uses Bluetooth for **simple control (no app)**	Likely not
Connects to a **smartphone app**	Yes
Sends **brushing data** to the cloud or app	Yes (Art. 3(3)(d))
App requires **user login or syncs with health records**	Yes (d), possibly (e)
Device can be **remotely updated** (firmware)	Yes (all three)
No cybersecurity controls (e.g., default passwords)	Non-compliant post-2025

The CEN/CENELEC Joint Technical Committee 13 (JTC 13), specifically Working Group 8 (WG 8), has developed the EN 18031 series of standards to address the cybersecurity requirements outlined in Articles 3(3)(d), (e), and (f) of the Radio Equipment Directive (RED) 2014/53/EU.

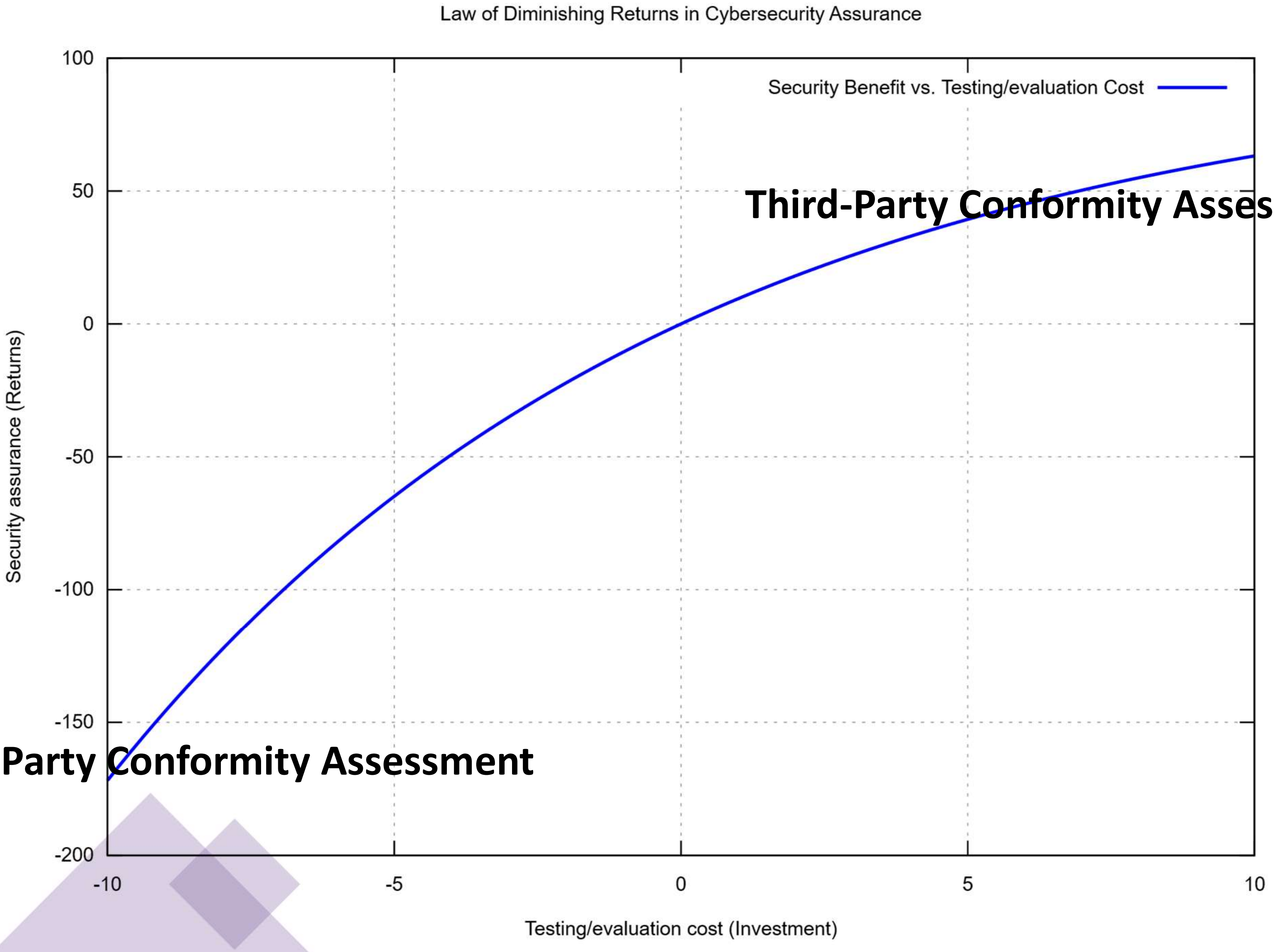
EN 18031-1: Protection against harm to networks or misuse of network resources (Article 3(3)(d)).

EN 18031-2: Protection of personal data and privacy (Article 3(3)(e)).

EN 18031-3: Protection against fraud, particularly for devices processing virtual money or monetary value (Article 3(3)(f))

These standards were finalized and approved by CEN members in June 2024.

As of February 2025, they have been officially cited in the Official Journal of the European Union, granting them the status of harmonized standards.



Third-Party Conformity Assessment

First-Party Conformity Assessment

NEW KID IN THE BLOCK: THE CYBER RESILIENCE ACT

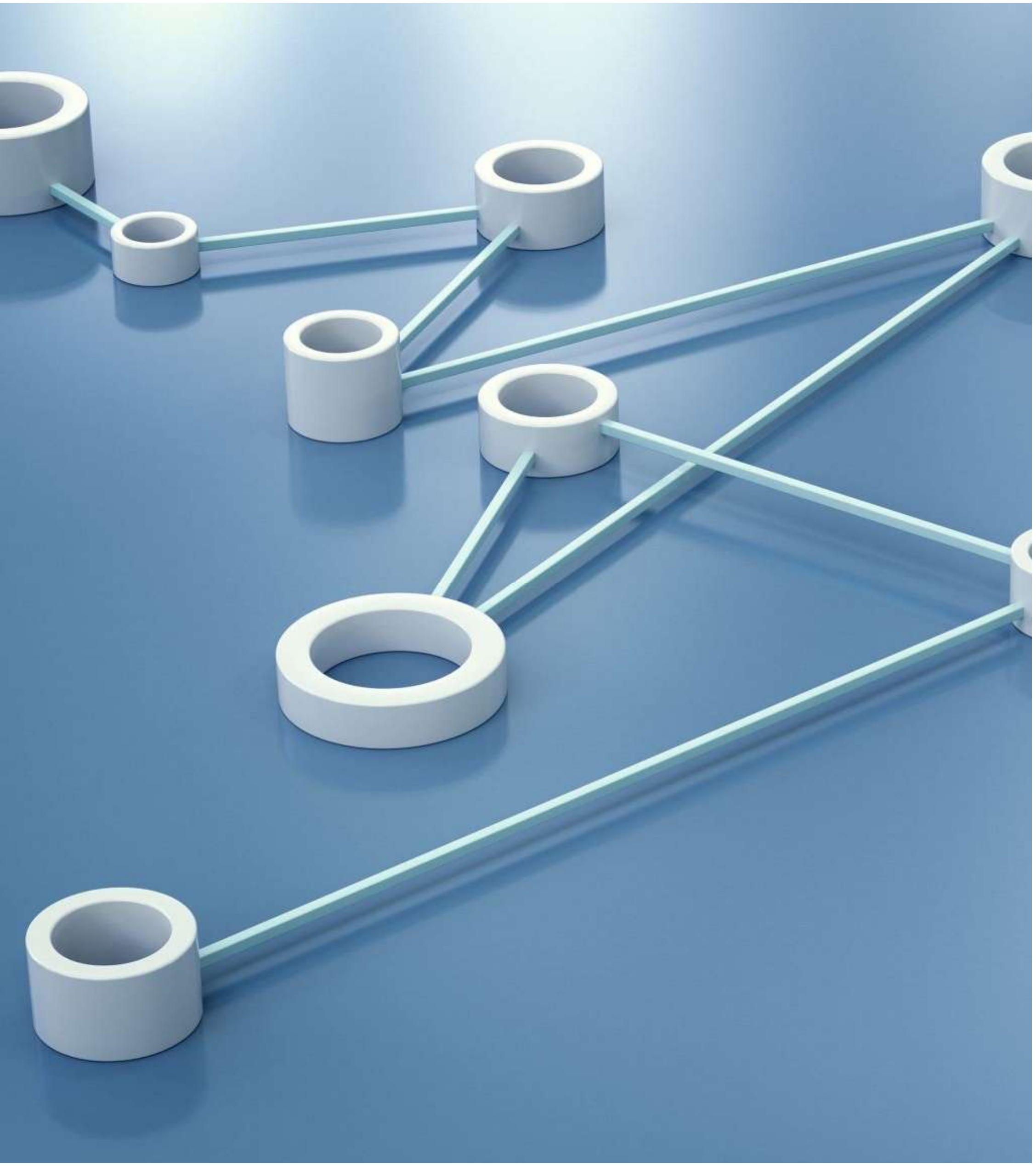
The European Union’s Cyber Resilience Act (CRA) was officially published in the EU’s Official Journal on 20 November 2024 and entered into force on 10 December 2024.

However, the CRA’s main obligations will apply in full starting from 11 December 2027.

This includes requirements for manufacturers, importers, and distributors of products with digital elements (PDEs) to ensure cybersecurity throughout the product lifecycle.

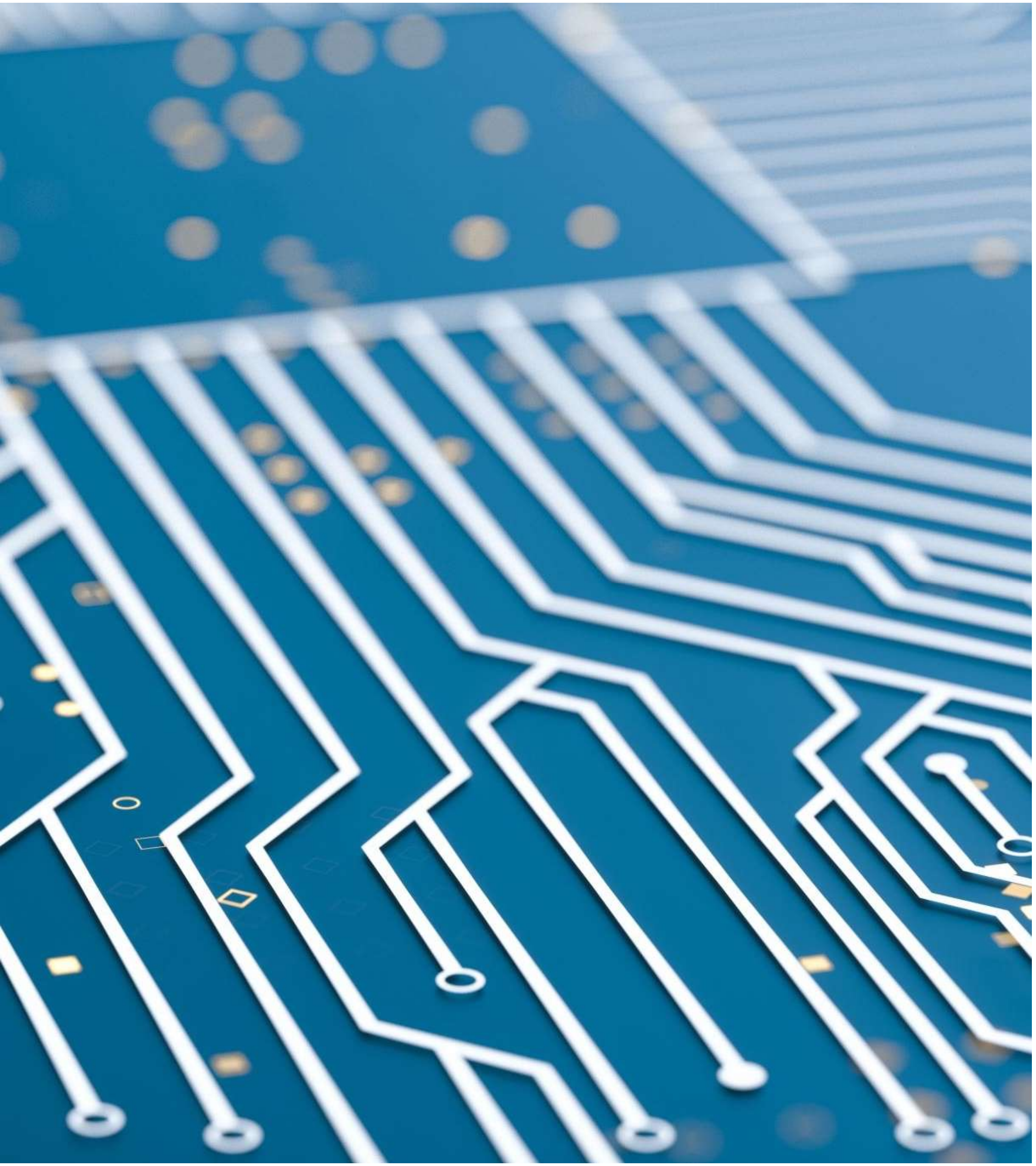
To facilitate its implementation, the European Commission issued a standardization request to European Standardization Organizations (ESOs) on February 3, 2025, under Commission Implementing Decision C(2025)618

The standardization request aims to develop harmonized European standards that provide technical specifications for manufacturers to demonstrate compliance with the CRA’s essential cybersecurity requirements. These standards will cover the entire lifecycle of PDEs, including design, development, production, and maintenance phases.



Horizontal Standards: These are overarching standards applicable across various sectors, focusing on general principles such as:

- Security by design and by default
- Risk management
- Vulnerability handling processes
- Transparency and accountability measures

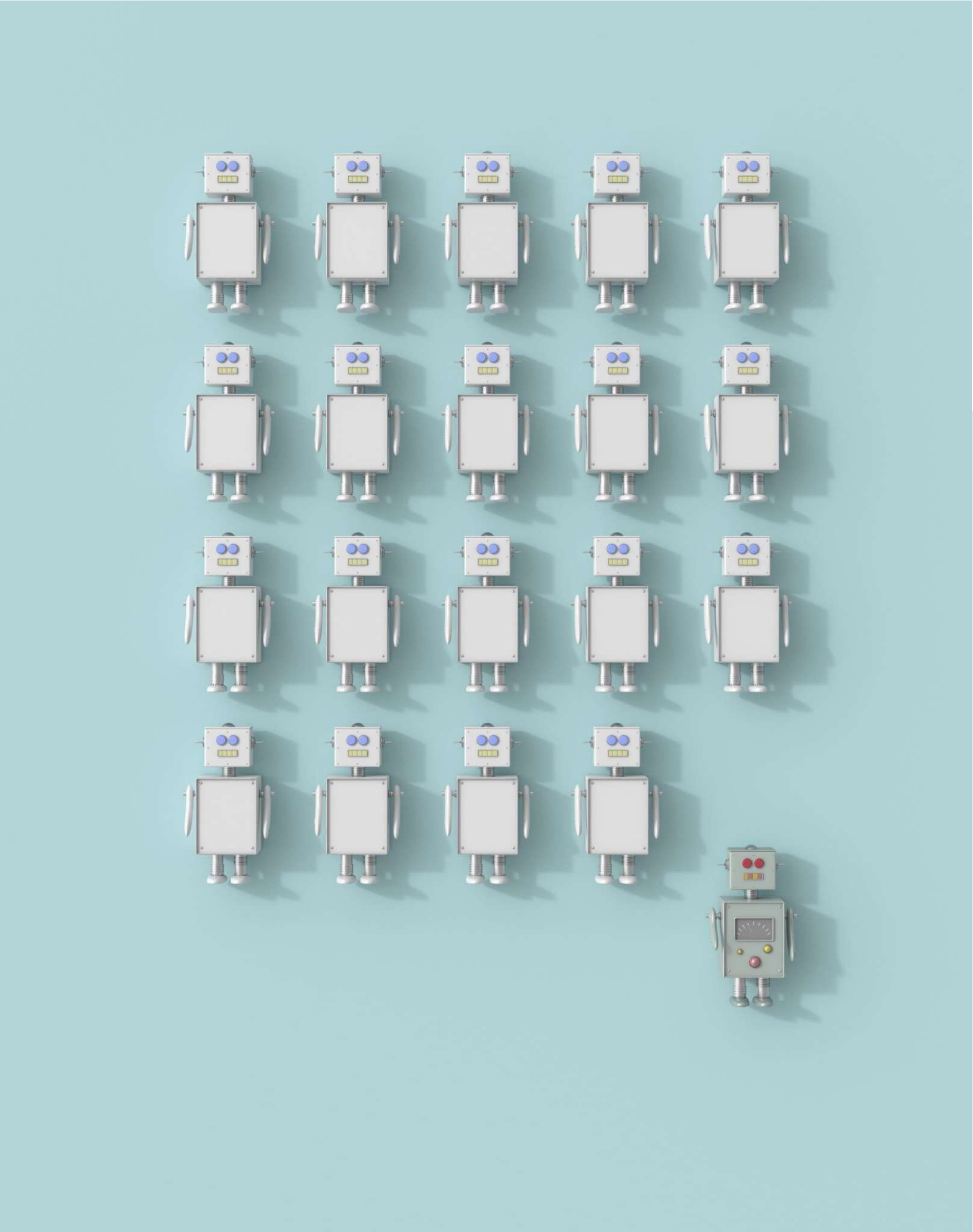


Vertical Standards:

These are sector-specific standards addressing particular needs of different industries or product categories.

Examples include standards for:

- Identity management systems
- Hypervisors and container runtime systems
- Semiconductors and trusted chips



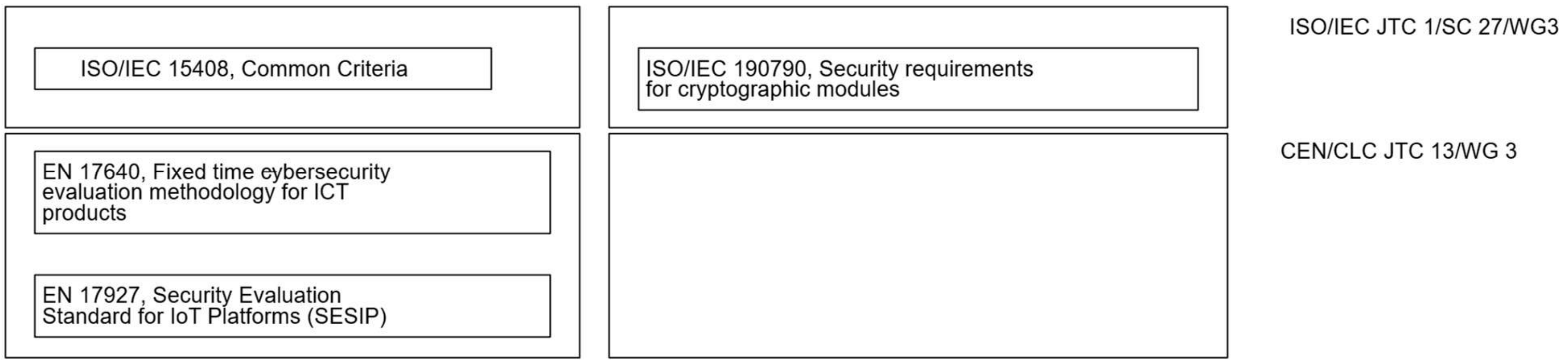
Under the CRA, products with digital elements are categorized based on their cybersecurity risk levels.

The Critical Products category encompasses items that pose the highest risk and, therefore, are subject to the most stringent compliance requirements (Annex IV of the CRA).

Manufacturers of critical products must demonstrate compliance with the CRA’s essential cybersecurity requirements through one of the following methods:

- **European Cybersecurity Certification Scheme**: Obtain a certificate under a scheme adopted pursuant to the EU Cybersecurity Act (Regulation (EU) 2019/881), achieving at least a “substantial” assurance level.
- **Third-Party Conformity Assessment**: Undergo an evaluation by a notified body to verify compliance with the CRA’s requirements.
- Self-assessment is not permitted for critical products due to their potential impact on essential services and infrastructure.

STANDARDS FOR THIRD-PARTY CYBERSECURITY ASSESSMENT?



ISO/IEC 15408, Common Criteria	ISO/IEC 190790, Security requirements for cryptographic modules	ISO/IEC JTC 1/SC 27/WG3
EN 17640, Fixed time eybersecurity evaluation methodology for ICT products EN 17927, Security Evaluation Standard for IoT Platforms (SESIP)		CEN/CLC JTC 13/WG 3

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14578-The-EU-Cybersecurity-Act_en

CSA, Have your saying

The initiative will revise the Cybersecurity Act, clarify the mandate of the EU Agency for Cybersecurity (ENISA) and improve the European Cybersecurity Certification Framework to achieve better resilience.

No change – Maintaining the current CSA as is.

Non-legislative improvements – Making clarifications or updates to ECCF implementation and reporting obligations without revising the law itself.

Targeted regulatory intervention – Updating ENISA's mandate to reflect additional tasks assigned in other legislation and streamlining ECCF governance and reporting structures.

Repeal and replacement – Introducing a comprehensive new regulation that extends ENISA’s scope, improves ECCF efficiency, addresses ICT supply chain challenges (including non-technical threats), and simplifies reporting.

LET’S MEET AGAIN ON 11 DECEMBER 2027…

MANY THANKS!