CYBERSTAND.eu

Supporting EU experts
in Cybersecurity
standardisation activities

How can Cyberstand help?

Cyberstand.eu is an initiative funded by the European Commission to help prepare companies for the Cyber Resilience Act. We will develop trainings, produce guidelines and run workshops for companies so that they know what to expect and will be able to comply with the CRA.

You can join our Cyber Resilience Act Standardisation Communities to keep up to date with all the latest developments on the CRA and be the first to know about the trainings and workshops.

Take the Cyber Resilience Act Public Survey

CRA Timeline

10 October 2024	The European Council adopted the CRA
30 October 2025	The CRA officially enters into force, marking the beginning of the adaption period for businesses.
July 2026	Manufacturers must report severe incidents and actively exploited vulnerabilities to public authorities.
October 2027	36 months after entry into force

Full compliance with all CRA requirements is expected. Businesses, including SMEs, must align their products and services with the new cybersecurity standards.

Co-funded by the European Union
ECCC European Cybersecurity Competence Centre

CYBERSTAND.eu

CYBERSTAND.eu

Supporting EU experts in Cybersecurity standardisation activities

The European Union is introducing the Cyber Resilience Act (CRA): by 2027 all producers of digital products and services will need to verify the cybersecurity of their products.

What does the CRA mean for SMEs?

In simple terms, it is a set of rules aimed at ensuring that products with digital elements – from software to connected devices – are built to resist cyber threats from the ground up. The CRA brings some new expectations, but remember that it is here to help, not hinder: it is about making resilience part of your business foundation, so you can focus on growth without the fear of not being able to trust your digital infrastructure.

What does the CRA affect?

The CRA is focused on products with digital elements – which means any hardware or software that connects to the internet or handles data could be affected. If your business designs, manufactures or sells products with digital components, you are likely within its scope. However, even if you do not create digital products yourself, the CRA still affects you if you use or integrate these kinds of products into your business.

Take the Cyber Resilience Act Public Survey

Co-funded by the European Union
ECCC European Cybersecurity Competence Centre

CYBERSTAND.eu

A quick checklist to see if the CRA may apply to your business

Do you sell or supply digital products?	If you create, manufacture, or distribute digital products (like software, apps, or connected devices), you will need to comply with CRA requirements.
Are you an SME using digital tools or connected devices?	Even if your business does not create digital products, you likely rely on digital tools or devices to run your daily operations - whether it is software for managing finances or devices like smart security systems.
Do you modify or integrate digital components?	If you customise or integrate digital components into products that you provide to customers, you will need to follow CRA guidelines. For example, if you are adding a software component to a physical device or creating an IoT setup, these integrated products need to be CRA compliant.

How the will work
in practice

90% of products

Default category

- Smart home devices
- Printers
- Bluetooth speakers
- Media player software applications

10% of products

Critical "Class I"

Products with virtual private network function

- Network management systems
- Boot managers
- Operating systems

Critical "Class II"

- Firewalls, intrusion detection & prevention systems
- Tamper-resistant microprocessors & microcontrollers

Critical Class

- Hardware devices with security boxes
- Smart meter gateways
- Smart cards or similar devices including secure elements

What will be required of companies?

Determine if your products fall under the CRA scope

Do you manufacture any of the products identified in the scope of the legislation?

Assess security risks

You must identify potential weaknesses in your products and the risks these vulnerabilities could pose to users or connected systems. This process involves analysing:

- Vulnerabilities
- Impacts
- Connectivity

Ensure conformity with cra requirements

Identify the requirements of the CRA and ensure that your product meets them. Cyberstand can help with this!

Maintain up-to-date documentation

The CRA requires manufacturers to keep comprehensive technical documentation of each product's cybersecurity measures.

Stay compliant

Commit to providing security updates for a defined period and clearly disclose the end-of-support date (the period for which security updates will be provided) to users.