EU Cyber Resilience Act Factsheet

The EU Cyber Resilience Act

The EU Cyber Resilience Act introduces mandatory cyber security requirements on placing products into the EU market where the product has a digital element.

Scope

Any product “with digital elements” where there’s a likelihood that the product will be connected to a device or network falls under the scope of the CRA.

A remote data processing solution, such as a custom cloud-based system sending instructions to or ingesting data from the product, is in scope and treated as part of the product that relies on it.

Importers and distributors become subject to the requirements if they place a product on the market under their own name.

There are exclusions for some categories of device including medical, automotive, and aero. Services without a product element also do not fall into scope.

Important Dates

11 September 2026

Reporting obligations under the act come into force, including for products already on the EU market.

11 December 2027

Full application of the requirements, including necessary assessments, CE marking, and technical documentation.

Reporting Obligations

As of September 2026, products newly placed on the market and existing products already on the market will be required to comply with the incident reporting and vulnerability disclosure obligations.

Reporting obligations apply to actively exploited vulnerabilities and severe incidents.

Obligation	Summary
Timely reporting	Initial early warning within 24 hours. Full notification within 72 hours. Final report within 14 days of a fixed vulnerability, or one month of an incident occurring.
Authority notification	Report required to be made via ENISA Single Reporting Platform.
User notification	Affected users must be notified.

Obligation	Summary
Upstream notification	If the vulnerability is within a 3rd party component, the component maker must be notified.

> Being pre-registered on the ENISA SRP is recommended to reduce operational friction during the 24-hour window.

Core Obligations

In-scope products placed on the EU market after December 2027 will be required to meet the standard set of obligations from the act.

- Secure by design (appropriately risk assessed)
- Secure by default
- No known exploits at release
- Defined support period of at least five years, or at least matching the product's anticipated lifetime
- Vulnerability handling capability throughout the support period
- Plain language documentation for clients
- Internal documentation maintained for at least 10 years

> Note: the act makes provisions for special categories of products that come with additional obligations.

Planning for Compliance

Example Compliance Activities

See below an example of how implementing the requirements of EU CRA might impact business functions across an organisation.

This table serves as an example of the types of activities that an organisation with in-scope products is likely to undertake to reach compliance and how they might be categorised into business functions in larger organisations.

Business Function	Example Activities
Engineering	Risk assessments, secure design and SDLC, updates
Vulnerability mgmt.	Vulnerability disclosure, monitoring and report triage
Supply chain	Component supplier vulnerability reporting, due diligence
Product mgmt.	Product version and behaviour cataloguing
Legal	Conformity assessments and markings
Customer support	Security update delivery, user contact details, notifications
Technical writing	Required user documentation to ship with products
Leadership	Sustainable support period roadmaps

What To Do Next

A pathway toward compliance is outlined below.

The European Commission is developing a set of recognised harmonised standards, which will make it easier for organisations to comply with EU CRA by following a standard recognised framework. Until a set of harmonised standards is published, organisations can prepare by following industry best practice steps that align with the requirements of the act.

While these steps are intended to help an organisation take a structured approach toward complying with the act it's important to note that complying with EU CRA is not a one-size-fits-all exercise.

While the compliance standard doesn't materially change by organisation size, the practical implementation can. Every organisation has its own operating models and internal structures, and these impact the most efficient and effect way of implementing the act.

Pathway Activities

1	Ensure an up-to-date listing of products and versions placed on or planned for the EU market.
2	Run a scoping assessment for each against the act's scope wording.
3	Verify an operationally effective and tested vulnerability and incident reporting chain is in place for the September deadline and register for the EU Single Reporting Platform.
4	Run a gap analysis exercise for documentation already held, against the Annex VII requirements.
5	Where gaps exist, determine which are merely documentation gaps, and which are operational gaps and triage accordingly. It is common for teams to be performing more security activities than they can point to evidence for.
6	Where required, put in place a process to ensure current client facing technical documentation exists for each distinct product version.

Bedrock Cyber Can Help

Bedrock Cyber

Bedrock Cyber helps UK software and SaaS businesses build product security operations that fit their needs.

If your business might benefit from advice on complying with EU CRA, Bedrock Cyber can help with tailored support to help you achieve your obligations under the act.

Learn more at **bedrockcyber.co.uk**