

Is Your Business Ready?

The EU Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for products with digital elements.

If your organisation develops, manufactures, imports or distributes connected hardware or software into the EU, the CRA could create significant new obligations for your business, even if you are based outside the EU.

The CRA entered into force on 10 December 2024, with its requirements being introduced in phases.

Mandatory vulnerability and incident reporting obligations apply from 11 September 2026, while most of the remaining requirements become applicable from 11 December 2027.



Could the CRA Apply to Your Organisation?

The CRA covers a wide range of products with digital elements, including:

- > Connected and Internet of Things devices
- > Operating systems and software applications
- > Network equipment such as routers and switches
- > Security products, including firewalls and anti-malware software
- > Software and hardware components sold separately
- > Certain remote data-processing solutions that are integral to a product

It can also apply to organisations outside the EU if an in-scope product is made available on the EU market.

Responsibilities vary depending on whether your organisation is considered a manufacturer, importer or distributor. Importantly, a business that commissions a product and sells it under its own name or trademark may be treated as the manufacturer, even if another organisation carried out the technical development.

What Will Businesses Need to Have in Place?

For manufacturers in particular, the CRA introduces requirements across the product lifecycle.

Organisations may need to demonstrate:

- > A documented cybersecurity risk assessment
- > Secure-by-design and secure-by-default controls
- > Effective vulnerability identification and remediation processes
- > Security testing and management of third-party components
- > Processes for delivering security updates
- > Defined product support periods
- > Technical documentation and evidence of compliance
- > Appropriate conformity assessment and CE marking
- > Processes capable of meeting mandatory vulnerability and incident reporting timescales

The challenge is not simply having policies in place. Organisations need to be able to demonstrate that appropriate cybersecurity controls, governance and evidence are embedded within the way products are developed, supplied and supported.

Reporting Obligations From September 2026

From **11 September 2026**, manufacturers must be ready to report actively exploited vulnerabilities and severe security incidents affecting in-scope products.

The reporting timescales are demanding, including an initial warning within 24 hours and a more detailed notification normally within 72 hours.

Meeting these deadlines requires effective monitoring, escalation, decision-making and evidence collection. Organisations therefore need more than a written reporting policy. They need processes that can operate quickly and effectively when a potentially reportable event occurs.



How We Can Help

Working together, Capital Compass and AJC can help you understand how the Cyber Resilience Act affects your organisation and prepare a practical route towards compliance.

Combining Capital Compass's local EU presence with AJC's specialist cybersecurity and compliance expertise, we work together to provide practical support for organisations preparing for the Cyber Resilience Act.

CRA Readiness Assessment

We can identify which products and organisational roles may fall within scope, determine the relevant product classification and conformity-assessment route, and assess your existing controls against CRA requirements.

Cybersecurity and Vulnerability Management Review

We can review your cybersecurity risk assessments, secure development processes, vulnerability management, third-party component governance, security testing and update mechanisms to identify areas requiring improvement.

Incident Reporting Readiness

We can assess whether your organisation has the monitoring, escalation and decision-making processes needed to identify potentially reportable events and meet the CRA's 24-hour, 72-hour and final reporting requirements.

Compliance and Conformity Readiness

We can review technical documentation and supporting evidence, identify gaps and help you prepare for conformity assessment, including engagement with a notified body where third-party assessment is required.



Practical Remediation Roadmap

Where gaps are identified, we can provide a prioritised roadmap to help you address them in a proportionate and manageable way ahead of the relevant deadlines.

Why Start Preparing Now?

Although most CRA requirements do not become applicable until December 2027, achieving compliance may require changes across product development, cybersecurity, vulnerability management, governance and documentation.

Starting early gives organisations time to identify gaps and integrate CRA requirements into existing product and security processes, rather than treating compliance as a separate exercise immediately before the deadline.

Not Sure How the Cyber Resilience Act Affects Your Organisation?

We can help you understand where you stand, identify any gaps and develop a practical roadmap towards compliance.

Talk to our team about a
CRA readiness assessment
and what your organisation
needs to do next.