Cobalt

DATA SHEET

European Cyber Resilience Act (CRA): overview and compliance best practices



The European Cyber Resilience Act (CRA) is a new legal framework adopted by the European Council in late 2024. It introduces mandatory cybersecurity requirements for products with digital elements (PDEs)—both hardware and software—sold in the European Union market.

The regulation aims to ensure that manufacturers, importers, and distributors prioritize security throughout a product's entire lifecycle. By establishing universal standards, the CRA seeks to close supply chain vulnerabilities and empower consumers to identify and select secure products.

Who is impacted?

The CRA applies to the entire supply chain of connected devices sold in the EU, regardless of where the company is headquartered.

- **Manufacturers:** Must ensure products are designed, developed, and produced with security in mind. They are responsible for risk assessments, vulnerability handling, and documentation (including software bill of materials—SBOMs).
- **Importers and distributors:** Must verify that products bear the CE conformity marking and that the manufacturer has met all technical documentation and conformity assessment requirements.

What's covered: Products with Digital Elements (PDEs)

The regulation covers almost all connected hardware and software, including:

- **Consumer tech:** Smartphones, laptops, smart speakers, and connected home appliances.
- **Software:** Operating systems, word processors, and games.
- **Infrastructure:** Firewalls, VPNs, and intrusion detection systems. (Note: Medical devices, aviation equipment, and connected cars are excluded as they are covered by existing specific legislation.)

Penalties

Non-compliance with the CRA can result in significant fines (up to €15 million or 2.5% of global turnover) and product withdrawals.

Key compliance requirements

To obtain the CE mark required to sell in the EU, organizations must demonstrate the following:

1. **Security by design:** Integrate cybersecurity into the design, development, and production phases.
2. **Vulnerability management:** Detect and mitigate vulnerabilities for a support period of five years (or the product's expected lifetime).
3. **Transparency:** Provide a Software Bill of Materials (SBOM) and technical documentation.
4. **Reporting:** Actively report exploited vulnerabilities and incidents to relevant authorities.

Implementation timeline

- **Reporting obligations began September 11, 2026:** Manufacturers will be required to report actively exploited vulnerabilities and severe incidents to authorities (ENISA and national CSIRTs) starting on this date.
- **Full implementation and enforcement begins December 11, 2027:** By this date, all products sold in the EU market must be fully compliant with all CRA requirements, including CE marking, technical documentation, and security support lifecycles.

How penetration testing supports CRA compliance

The CRA explicitly requires manufacturers to conduct ongoing risk assessments and ensure products are released without exploitable vulnerabilities. Penetration testing is a critical tool for meeting these obligations.

- **Map the attack surface:** Offensive security testing helps manufacturers identify all digital elements and entry points, a prerequisite for the required risk assessments.
- **Identify and mitigate vulnerabilities:** Regular pentesting validates that products are free of known exploitable vulnerabilities before they hit the market—a core CRA mandate.
- **Continuous support:** The CRA requires vulnerability management for five years after release. Continuous pentesting ensures emerging threats are identified and mitigated throughout this support lifecycle.
- **Audit-ready documentation:** Professional pentest reports serve as audit-quality evidence of due diligence, supporting the technical documentation required for conformity assessments.

Establishing a robust offensive security program now allows organizations to map their risks, secure their supply chain, and prepare for the reporting deadlines ahead.

Book a demo to see how Cobalt can help you achieve compliance and build your offensive security program. *cobalt.io/get-started*

Disclaimer: This content provides general information, not legal advice. Cobalt is not responsible for any errors or omissions, and this content does not create an attorney-client relationship. You should always consult a legal professional for advice specific to your situation.

© 2026 Cobalt Labs, Inc. All Rights Reseved.