SmartSuite

Framework / Cybersecurity / Other

EU Cyber Resilience Act (CRA)

The EU Cyber Resilience Act sets cybersecurity requirements for products with digital elements, a five-year minimum support period and 24-hour exploited vulnerability reports.



What it is

The EU Cyber Resilience Act (Regulation (EU) 2024/2847) requires manufacturers, importers and distributors of products with digital elements, meaning hardware and software with a data connection, to build them to essential cybersecurity requirements, handle vulnerabilities for a support period of at least five years, and report actively exploited vulnerabilities and severe incidents. The Regulation entered into force on December 10, 2024, its reporting duties apply from September 11, 2026 and the full Regulation applies from December 11, 2027.

The European Parliament and the Council adopted it on October 23, 2024. Market surveillance authorities in each Member State enforce it, and ENISA and the national CSIRTs receive vulnerability and incident reports through a single reporting platform (Article 14 and Article 16). Medical devices, in vitro diagnostic devices, motor vehicles and certified aviation products are excluded (Article 2).

At a glance

PUBLISHER European Parliament and Council of the European Union	TYPE Regulation	VERSION Regulation (EU) 2024/2847
EFFECTIVE December 10, 2024 (entry into force); reporting duties from September 11, 2026; full application from December 11, 2027	DOMAIN Cybersecurity	FAMILY Other
REGION European Union	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Why it matters

- **A legal baseline for products** Annex I Part I requires products to be made available without known exploitable vulnerabilities, secure by default, protected against unauthorized access and with security updates (Annex I, Part I (2)).
- **Vulnerability handling as a duty** Annex I Part II requires manufacturers to document vulnerabilities and components, including a software bill of materials, test regularly, and run a coordinated vulnerability disclosure policy.
- **A support period** Manufacturers set a support period reflecting the expected use time, and it must be at least five years unless the product will be used for less time (Article 13(8)).
- **Reporting to authorities** Actively exploited vulnerabilities and severe incidents are reported on a 24-hour, 72-hour and final-report timetable (Article 14).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports EU CRA

Product and Class Register

Record each product with digital elements, its Annex III class, the conformity route chosen and the manufacturer, importer or distributor role.

Annex I Requirement Library

Map the Part I and Part II requirements to design controls and test evidence, with justification where a requirement does not apply (Article 13(4)).

Component and SBOM Tracking

Keep the software bill of materials, open-source and third-party component owners and the vulnerabilities reported upstream (Article 13(5) and (6)).

Support Period and Update Plan

Record the support period end date, security update releases and public disclosure of fixed vulnerabilities (Article 13(8) and Annex I, Part II).

Article 14 Reporting Workflow

Time each exploited vulnerability or severe incident against the 24-hour, 72-hour and final-report deadlines, with the report platform record (Article 14).

Technical File and Declaration

Keep technical documentation, the EU declaration of conformity and CE marking evidence for at least 10 years or the support period (Article 13(13)).

Common framework mappings

EU DORA | GDPR | ISO 27001:2022 | NIS2 (EU 2022/2555) | NIST 800-218 SSDF

Official resources

EU Cyber Resilience Act Text

Provides the official regulation text outlining cybersecurity requirements for digital products in the EU.

eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1001

Cyber Resilience Act Overview

Describes the objectives and scope of the CRA, highlighting its impact on market stakeholders.

digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Cyber Resilience Act Q&A

Offers detailed answers to common questions regarding the CRA's implementation and compliance.

digital-strategy.ec.europa.eu/en/faqs/cyber-resilience-act-questions-answers

Cyber Resilience Act Implementation Guide

Outlines steps for organizations to comply with the CRA, focusing on secure development and risk management.

digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Frequently asked questions

Who must comply with the EU Cyber Resilience Act?

Manufacturers, importers and distributors of products with digital elements made available on the EU market, whether made inside or outside the Union (Article 2). Medical devices, in vitro diagnostic devices, motor vehicles, certified aviation products and spare parts are among the exclusions.

When do the CRA's obligations apply?

The Regulation entered into force on December 10, 2024. Article 14 reporting obligations apply from September 11, 2026 and the rest of the Regulation from December 11, 2027 (Article 71).

What must a manufacturer report and when?

Actively exploited vulnerabilities and severe incidents are reported through the single reporting platform to the CSIRT coordinator and ENISA: an early warning within 24 hours, a notification within 72 hours, and a final report within 14 days after a fix is available for vulnerabilities, or within one month of the notification for incidents (Article 14).

How long must a manufacturer support a product?

The manufacturer sets the support period to reflect how long the product is expected to be in use. It must be at least five years unless the product is expected to be used for less time, and its end date is stated at the time of purchase (Article 13(8) and (19)).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the fines under the CRA?

Up to EUR 15 million or 2.5 percent of worldwide annual turnover for breaches of the essential requirements or Articles 13 and 14, whichever is higher. Other listed obligations carry up to EUR 10 million or 2 percent, and misleading information up to EUR 5 million or 1 percent (Article 64).

License included / downloadable: Yes The Regulation is EU law published in the Official Journal and is included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/eu-cyber-resilience-act-cra

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.