SmartSuite

Framework / Cybersecurity / Other

EU Cyber Resilience Act (CRA)

The EU Cyber Resilience Act mandates cybersecurity requirements for products with digital elements sold in the EU to reduce vulnerabilities.

What it is

The EU Cyber Resilience Act (CRA) is a regulatory framework that establishes mandatory cybersecurity requirements for products with digital elements placed on the European Union market. Its primary objective is to enhance the security of hardware and software products to ensure better protection of consumers and organizations against cyber threats.

Published by the European Union, the CRA applies to manufacturers, importers, and distributors of connected devices and software across a wide range of sectors. The regulation sets out obligations for risk assessment, secure development, vulnerability management, and incident reporting, complementing existing EU directives such as the NIS2 Directive and GDPR in supporting cybersecurity, risk management, and regulatory compliance.

At a glance

PUBLISHER European Commission	TYPE Regulation	VERSION Regulation (EU) 2024/2847
EFFECTIVE January 16, 2024	DOMAIN Cybersecurity	FAMILY Other
REGION European Union	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

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

Why it matters

- **Strengthen product security governance** Support consistent, organization-wide cybersecurity policies throughout the product lifecycle and supply chain.
- **Enhance regulatory alignment** Enable alignment with EU-wide cybersecurity regulations, simplifying compliance with related frameworks such as NIS2 and GDPR.
- **Improve vulnerability management** Mandate proactive vulnerability identification, mitigation, and reporting to reduce risk exposure and speed incident response.
- **Increase accountability and oversight** Require clear documentation and traceability for security controls, improving internal oversight and external audit readiness.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports EU CRA

Product Scope and Inventory

Catalog covered products, versions, components, and accountable owners.

Secure-by-Design Requirements Tracking

Manage security requirements, design reviews, and implementation evidence.

Vulnerability Intake and Disclosure Management

Track vulnerability intake, triage, remediation, disclosure, and patch status.

Release and Update Governance

Document approvals, security testing evidence, and update/patch release records.

Supplier and Component Oversight

Manage dependency risk, supplier assurances, and third-party component tracking.

Compliance and Audit Reporting

Report product readiness, open issues, and evidence coverage by product line.

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

What is the EU Cyber Resilience Act used for?

The EU Cyber Resilience Act (CRA) is designed to enhance the cybersecurity of products with digital elements on the EU market. It ensures that hardware and software are developed, maintained, and supported with strong security controls to protect users and organizations from cyber threats. The regulation drives improvements in secure design, vulnerability management, and incident handling across the product lifecycle.

Is compliance with the EU Cyber Resilience Act mandatory?

Yes, compliance with the CRA is mandatory for manufacturers, importers, and distributors of relevant products sold or made available within the European Union. Organizations must adhere to the regulatory requirements, and non-compliance can result in enforcement actions and penalties.

What products and organizations fall within the scope of the CRA?

The CRA applies to all products with digital elements—including connected devices, software, and certain standalone software—placed on the EU market. This includes global manufacturers, importers, and distributors targeting EU customers, regardless of where the company is legally based.

What are the key security requirements of the EU CRA?

The CRA sets out core requirements such as secure-by-design and by-default principles, conducting risk assessments, implementing technical and organizational security controls, managing vulnerabilities, maintaining technical documentation, and incident reporting. Organizations must also establish conformity assessments to demonstrate compliance with these obligations.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How is CRA compliance implemented during product development?

Organizations incorporate CRA compliance by mapping requirements into product lifecycle activities, including secure coding, security testing, vulnerability monitoring, and maintaining traceable technical documentation. Risk management and compliance checkpoints are embedded into development and post-market processes to ensure ongoing adherence.

How does the EU Cyber Resilience Act relate to NIS2 and GDPR?

The CRA complements existing EU legislation such as the NIS2 Directive and the General Data Protection Regulation (GDPR) by focusing on product-level cybersecurity and resilience. While NIS2 covers organizational security for essential services, and GDPR addresses personal data protection, the CRA targets security practices specifically in digital product development and supply chains.

What are the ongoing compliance requirements under the CRA?

Ongoing compliance includes continuous risk assessment, regular vulnerability scanning and patch management, timely incident notification, and periodic review and update of technical documentation. Organizations must also prepare for regulatory audits and maintain readiness for reporting security incidents to national authorities.

How would SmartSuite support the EU Cyber Resilience Act?

SmartSuite streamlines CRA compliance by enabling centralized risk tracking, mapping CRA requirements to existing control libraries, and attaching evidence directly to policy items. It supports end-to-end compliance through remediation workflows, technical documentation management, conformity assessment tracking, audit readiness tools, and robust reporting and incident logging for regulator submissions.

License included / downloadable: Yes The Cyber Resilience Act is European Union legislation and is publicly available through official EU regulatory publications.

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