



EU CYBER RESILIENCE ACT · REG. (EU) 2024/2847

# Cyber Resilience Act

## What manufacturers need to know

The first EU regulation imposing binding cybersecurity requirements on all products with digital elements placed on the EU market. Full application: 11 December 2027.

**11 Dec 2027**

Full application

**€15 M / 2.5%**

Max administrative fine

**24h · 72h · 14d**

Reporting cadence to ENISA

**Annex I**

Product essential requirements

PREPARED BY

**BlackIoT Sagl** — Swiss engineering partner for CRA-compliant electronic products

## 01 · CONTEXT

# What the CRA is

The first horizontal EU regulation imposing binding cybersecurity requirements on products with digital elements.

## KEY FACTS

- Regulation (EU) 2024/2847 — adopted 23 October 2024.
- Entered into force 10 December 2024; full application 11 December 2027.
- Applies to hardware and software products sold, distributed or otherwise placed on the EU market.
- Extraterritorial — applies to non-EU manufacturers who place products on the EU market.
- Horizontal regulation — does not replace sector-specific rules where equivalent.

## IN SCOPE

- All Products with Digital Elements (PDEs) placed on the EU market.
- Connected consumer IoT (smart meters, smart home, wearables).
- Industrial IoT, controllers, networked machinery.
- Firmware, operating systems, libraries and embedded software.
- Remote data-processing solutions necessary for the product function.

## OUT OF SCOPE

Products covered by equivalent Union law:  
medical devices (MDR/IVDR), civil aviation,  
motor vehicles, spare parts, custom-built for defense.

## 02 · ECONOMIC OPERATORS

# Who must comply

Every operator along the supply chain carries obligations — from silicon to retail.

01

## Manufacturer

Designs or makes a PDE, or has one designed, and places it on the market under its own name. Primary obligations: Annex I compliance, technical file, SBOM, vulnerability handling, conformity assessment, CE marking.

02

## Authorized rep.

Appointed in writing by a manufacturer based outside the EU to carry out specific tasks on its behalf. Keeps the technical file and Declaration at the disposal of market-surveillance authorities.

03

## Importer

Places a PDE from a third country on the EU market. Verifies that the manufacturer has carried out conformity assessment, CE marking is affixed, and the product is accompanied by the required documentation.

04

## Distributor

Makes the product available on the market. Must verify the product bears CE marking and is accompanied by the required documentation; takes corrective action if necessary.

## 03 · TIMELINE

# Compliance milestones

Four phased dates between 2024 and 2027. Plan your redesign now.

10 DEC 2024



## Entry into force

The Regulation is published in the Official Journal and enters into force. Preparation clock starts.

11 JUN 2026



## Conformity assessment bodies

Chapter IV applies — notification of conformity assessment bodies begins. Notified Bodies become available.

11 SEP 2026



## Reporting obligations to ENISA

Manufacturers must report actively exploited vulnerabilities and severe incidents on the 24 h / 72 h / 14 d cadence.

11 DEC 2027



## Full application

All CRA obligations apply. Products placed on the EU market must meet Annex I essentials, ship with SBOM, pass conformity assessment.

# Essential cybersecurity requirements

Product properties — must be designed, developed and produced to meet all of the following.

- Secure-by-design and by-default configuration; minimum attack surface.
- Protection from unauthorized access with appropriate control mechanisms (authentication, identity / access management).
- Protection of confidentiality and integrity of stored, transmitted or processed data — including encryption at rest and in transit.
- Processing of only the minimum personal data necessary for intended use.
- Protection of availability of essential functions, including resilience against denial-of-service.
- Minimization of negative impact on other devices or networks connected to the product.
- Limitation of attack surfaces including external interfaces (exposed ports, debug probes).
- Reduction of the impact of an incident using appropriate mitigation mechanisms.
- Provision of security-related information by recording and monitoring relevant internal activity (logging).
- Secure default configuration; user ability to reset to factory settings; secure removal of user data.
- Delivery of security updates without delay, free of charge, with clear advisory messages for the duration of the declared support period.

# Vulnerability handling requirements

Ongoing obligations throughout the product support period.

- Identify and document vulnerabilities and components in the product, including a machine-readable SBOM covering at least top-level dependencies.
- Address and remediate vulnerabilities without delay — including through security updates delivered free of charge.
- Apply effective and regular security testing and reviews (SAST, DAST, fuzzing, pen-testing where applicable).
- Once a security update is available, publicly disclose information about fixed vulnerabilities; provide advisory information in a common machine-readable format (CSAF).
- Operate a coordinated vulnerability disclosure policy aligned with ISO/IEC 29147.
- Facilitate sharing of information about potential vulnerabilities via a contact address.
- Provide for mechanisms to securely distribute updates — secure boot, signed firmware, rollback protection.
- Ensure support period is clearly declared to the user — aligned with product expected use, minimum five years where proportional.

# Software Bill of Materials

The machine-readable inventory that makes vulnerability handling operationally possible.

## WHAT IT IS

A machine-readable inventory of all software components shipped in the product, including firmware, third-party libraries, and their versions. SPDX and CycloneDX are the two widely adopted formats.

## WHY IT MATTERS

When a CVE is published against a library, an SBOM lets you instantly answer the question 'do any of my products ship this version?'. Without an SBOM the 24 h / 72 h / 14 d reporting cadence is not realistically achievable.

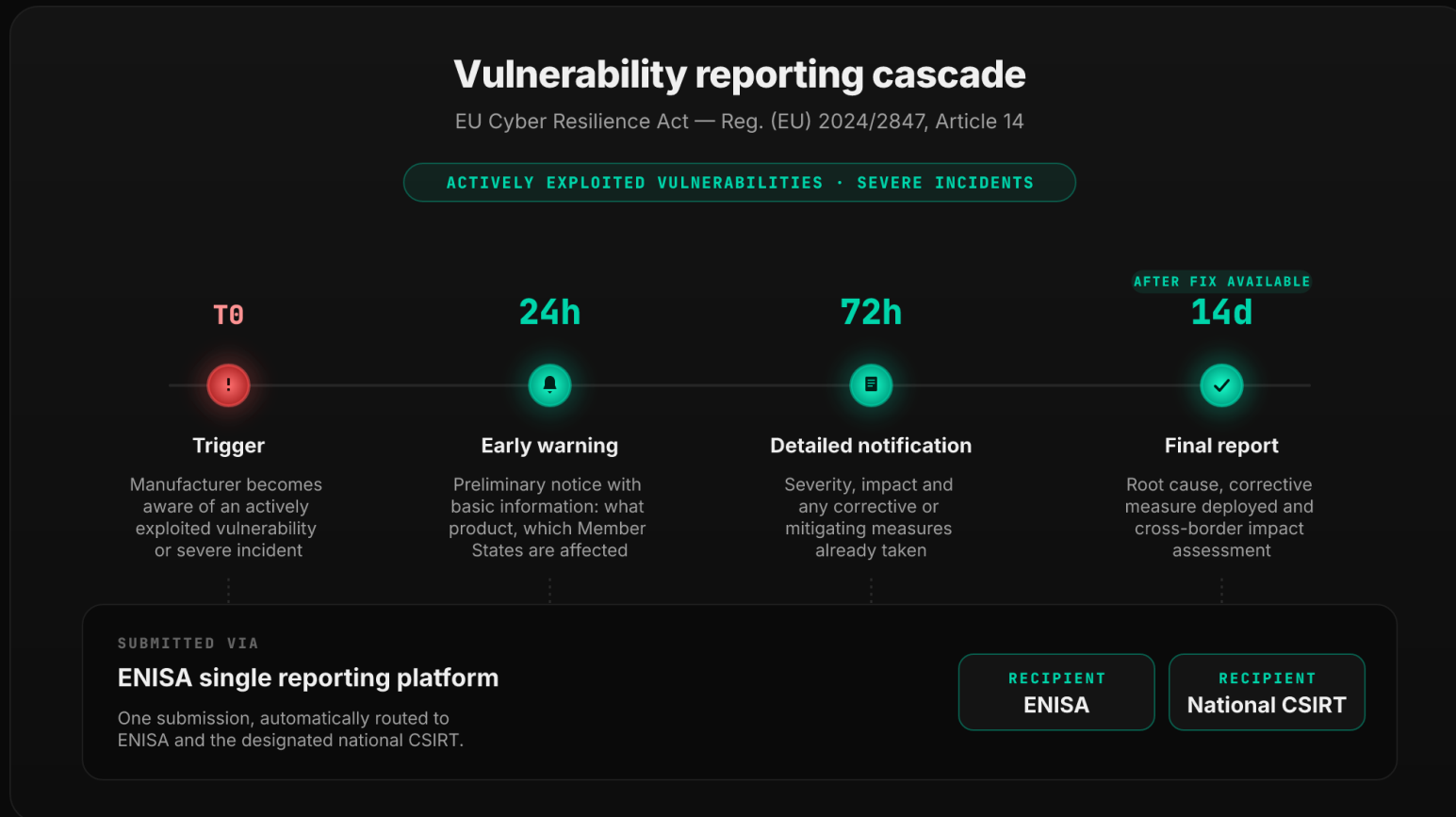
## HOW IT GETS USED

Included in the technical file presented at conformity assessment, kept up to date over the support period, made available to market-surveillance authorities on request, and increasingly required in public-sector procurement.

## 07 · INCIDENT REPORTING

# The 24 h / 72 h / 14 d cascade

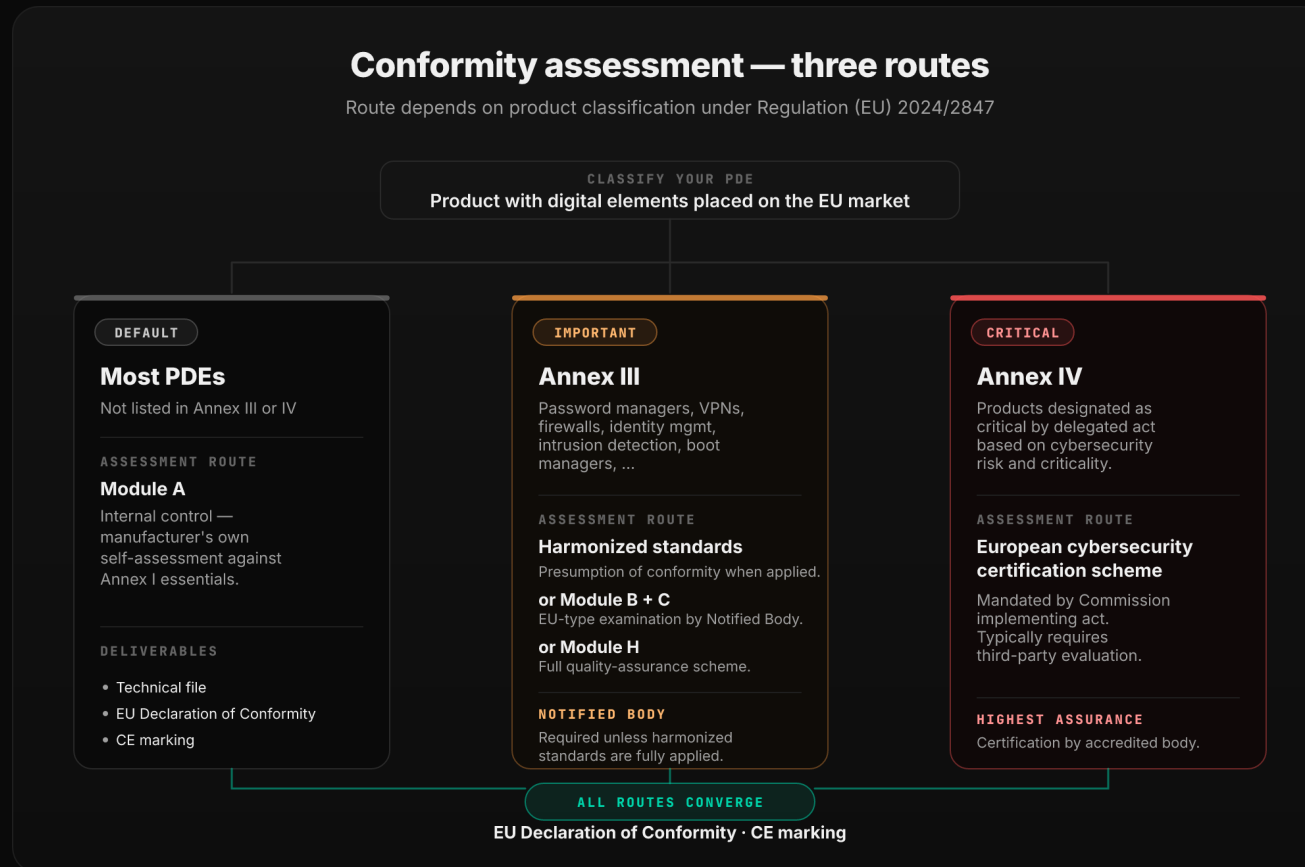
One submission via the ENISA single reporting platform, three escalating deadlines, two recipients.



## 08 · CONFORMITY ASSESSMENT

# Three routes, one CE marking

Route depends on product classification under the Regulation.



## 09 · PENALTIES

# Administrative fines

Non-compliance is a commercial risk — not a technical inconvenience.

**TIER 1**

## €15 M

or 2.5% of turnover

Non-compliance with Annex I essential requirements or vulnerability handling obligations (Annex I § 2).

**TIER 2**

## €10 M

or 2% of turnover

Non-compliance with other obligations under the Regulation — including those of importers, distributors, authorized representatives.

**TIER 3**

## €5 M

or 1% of turnover

Supply of incorrect, incomplete, or misleading information to notified bodies or market-surveillance authorities.

Whichever is higher — of the total worldwide annual turnover for the preceding financial year. Article 64 CRA.

# End-to-end CRA redesign services

Swiss engineering partner backed by IPC-certified PCB design practice.

**01**

## CRA Gap Assessment

Audit against Annex I § 1 (product cybersecurity) and § 2 (vulnerability handling). Deliverable: classification, risk assessment, remediation backlog.

**02**

## Secure-by-Design Redesign

Hardware and firmware rework. Root of trust, secure boot, signed firmware, cryptographic services, TRNG, attack-surface reduction, secure update path.

**03**

## SBOM & PSIRT

Machine-readable SBOM (SPDX / CycloneDX), vulnerability handling workflow, ENISA reporting plumbing on 24 h / 72 h / 14 d cadence, CSAF advisories.

**04**

## Conformity Assessment

Technical file, EU Declaration of Conformity, CE marking. Notified Body liaison for Annex III Important and Annex IV Critical products.

**05**

## Aerospace & Defense PCB

IPC Class 3 high-reliability PCB design — IPC-A-610, IPC-6012, J-STD-001, IPC-2221. IPC-trained for military and aerospace applications.

**06**

## Industrialization

Design for manufacturing and test (DFM / DFT), test fixtures, supply-chain due diligence for CRA Article 13 component traceability.



# Let's make your product **CRA-compliant.**

Book a CRA Gap Assessment — typical deliverable in 4–6 weeks.

EMAIL

[info@blackiot.swiss](mailto:info@blackiot.swiss)

WEB

[www.blackiot.swiss](http://www.blackiot.swiss)

ADDRESS

Via Stefano Franscini 2A,  
6833 Vacallo, Switzerland