EU Cyber Resilience Act

Are You Ready?

A self-assessment for product security, GRC, and engineering teams

Regulation (EU) 2024/2847 — the Cyber Resilience Act — establishes binding cybersecurity requirements for almost every connected hardware and software product placed on the EU market. Two dates matter most. On **11 September 2026**, manufacturers must begin reporting actively exploited vulnerabilities and severe incidents within a 24-hour window. On **11 December 2027**, the full regulation applies — secure-by-design properties, vulnerability handling, SBOMs, conformity assessment, and CE marking. Non-compliance can reach **€15 million or 2.5% of worldwide turnover**, and market surveillance authorities can pull non-conforming products from the market.

Use this guide as a self-check. Tick what is true today, not what is planned. The gaps that remain are your roadmap.

KEY DATES

11 Sep 2026
Article 14 reporting obligations take effect

11 Dec 2027
Full CRA application – Annex I and conformity

CHECKLIST FRAMEWORK

1.1 VULNERABILITY VISIBILITY	1.2 EXPLOIT TRIAGE	1.3 REPORTING WORKFLOW	2.1 SOFTWARE BILL OF MATERIALS	2.2 COORDINATED VULNERABILITY DISCLOSURE AT SCALE	2.3 SECURE-BY-DESIGN PRODUCT PROPERTIES	2.4 CONFORMITY ASSESSMENT AND CE MARKING

CRA at a Glance

SCOPE	**Products with digital elements (hardware + software) made available on the EU market, including their remote data processing solutions**
WHO	**Manufacturers, importers, distributors, authorized representives, and open-source software stewards.**
KEY DATES	**11 Jun 2026 — notified bodies. 11 Sep 2026 — vulnerability and incident reporting (Art 14). 11 Dec 2027 — full application.**
PENALTIES	**Up to €15M or 2.5% of worldide annual turnover for breaches of essential requirements or reporting duties (Art. 64).**
CLASSIFICATION	**Default / Important Class I & II (Annex III) / Critical (Annex IV) — drives the conformity assessment path.**

PART I

Article 14 readiness

Effective 11 September 2026

Reporting obligations for actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements. Applies to all in-scope products on the market, including those placed before the full application date.

1.1 Vulnerability visibility

☐ Maintain a current inventory of every product with digital elements placed on the EU market, including software components and remote data processing solutions.

☐ Identify and document vulnerabilities in every product and its components, including third-party and free / open-source components.

☐ Enrich vulnerability detection with multiple authoritative sources — NVD, GHSA, OSV, the European vulnerability database, and CISA ADP — not a single feed.

☐ Maintain an SBOM covering at least top-level dependencies in a commonly used machine-readable format.

PART I

Article 14 readiness *(continued)*

Effective 11 September 2026

Reporting obligations for actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements. Applies to all in-scope products on the market, including those placed before the full application date.

1.2 Exploit triage

☐ Article 14 is triggered by actively exploited vulnerabilities — those with reliable evidence of exploitation in a system without permission. This is a narrower bar than CISA KEV; document the internal definition and who can confirm it.

☐ Subscribe to exploit-signal sources — CISA KEV, vendor advisories, public exploit databases — and route them into a single triage queue.

☐ Establish a severe-incident definition aligned with Art. 14(5): incidents that affect availability, authenticity, integrity, confidentiality, or that lead to malicious code execution.

☐ Map products to the Member States where they have been made available, and identify the corresponding CSIRT coordinator endpoint before September 2026 — this drives where notifications route.

1.3 Reporting workflow

☐ Submit an early-warning notification within 24 hours of becoming aware of an actively exploited vulnerability or severe incident, via ENISA's single reporting platform through the CSIRT coordinator.

☐ Submit a detailed notification within 72 hours, including corrective and mitigating measures available and sensitivity classification.

☐ Submit a final report — 14 days after a corrective measure is available for vulnerabilities; one month after the 72-hour notification for incidents.

☐ Notify impacted users of the product without delay, with corrective or mitigating measures — in a machine-readable format where appropriate.

PART II

Article 14 readiness

Effective 11 December 2027

Essential cybersecurity requirements covering product properties (Annex I Part I) and vulnerability handling processes (Annex I Part II), plus conformity assessment, CE marking, technical documentation, and the EU declaration of conformity.

2.1 Software bill of materials at scale

☐ Generate an SBOM for every product release in a commonly used machine-readable format (SPDX or CycloneDX), covering at least top-level dependencies.

☐ Retain SBOMs for at least the support period and be prepared to provide them to market surveillance authorities on reasoned request, including for ADCO Union-wide dependency assessments.

2.2 Coordinated vulnerability disclosure

☐ Publish a coordinated vulnerability disclosure policy and a single point of contact — easily findable on the product and in user instructions.

☐ Once a security update is available, publicly disclose information about the fixed vulnerability — description, affected versions, impact, severity, and remediation.

☐ Provide security updates separately from functionality updates where technically feasible, and at no cost to users.

☐ Apply due diligence on third-party and open-source components: verify supplier compliance, update history, known vulnerabilities; report upstream when found.

2.3 Secure-by-design product properties

☐ Conduct and document a cybersecurity risk assessment covering intended purpose, foreseeable use, and operational environment. Include in technical documentation.

☐ Ship without known exploitable vulnerabilities; provide secure-by-default configuration; ensure vulnerabilities can be addressed through security updates.

PART I

Article 14 readiness *(continued)*

Effective 11 December 2027

2.4 Secure-by-design product properties

☐ Classify each product: default, Annex III Class I, Annex III Class II, or Annex IV critical. Document the basis — classification drives the assessment path.

☐ Select the appropriate conformity assessment procedure (module A, B+C, H, or a European cybersecurity certification scheme).

☐ Draw up the technical documentation (Annex VII) and the EU declaration of conformity (Annex V). Retain both for at least 10 years or the support period, whichever is longer.

☐ Affix the CE marking on the product, packaging, or EU declaration. For high-risk AI systems under (EU) 2024/1689, align conformity per Art. 12.

☐ Draw up the technical documentation (Annex VII) and the EU declaration of conformity (Annex V). Retain both for at least 10 years or the support period, whichever is longer.

☐ Affix the CE marking on the product, packaging, or EU declaration. For high-risk AI systems under (EU) 2024/1689, align conformity per Art. 12.

Where to focus first

The 24-hour reporting clock arrives before most other CRA obligations. If your team has limited cycles between now and September 2026, concentrate on three things: **a complete inventory of products on the EU market, continuous multi-source vulnerability visibility**, and **a tested 24 / 72 / 14 notification workflow with named owners**. Every other obligation in Part 2 can be sequenced behind those — but none of them can substitute for the September readiness gate.

The 2027 milestone is broader but more predictable. SBOM generation, coordinated vulnerability disclosure, technical documentation, and conformity assessment all reward early movers and punish teams that treat December 2027 as a single point-in-time cutover.

How Code Insight helps

Revenera's Code Insight gives product teams the inventory and vulnerability intelligence the CRA expects: machine-readable SBOMs (SPDX / CycloneDX), multi-source vulnerability enrichment across NVD, GHSA, OSV, and CISA ADP with KEV signals, exploit-aware alerting tuned for the Article 14 reporting window, and the long-term inventory needed for ADCO dependency assessments and Annex VII technical documentation.

Unsure where to start? Revenera Code Insight helps close the most common gaps in CRA readiness. Please contact Revenera today.

References

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). OJ L, 20.11.2024. ELI: http://data.europa.eu/eli/reg/2024/2847/oj