GUIDE 2025/2026

CRA guide for manufacturers

The Cyber Resilience Act, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is the CRA? 3

1.1 The regulation in plain words 3

1.2 How the CRA is structured 3

1.3 The deadlines — what applies from when? 3

1.4 How it relates to other rules 4

2 Does it apply to you? 5

3 The path to conformity — 7 phases 7

4 What does the CRA cost? 8

5 The 10 most common mistakes 9

6 Readiness check: are you ready? 11

7 Glossary 13

8 Your next step 15

1 What is the CRA?

1.1 The regulation in plain words

CRA stands for **Cyber Resilience Act** — the EU regulation on horizontal cybersecurity requirements for products with digital elements (Regulation (EU) 2024/2847). It entered into force on **10 December 2024** and applies directly in every member state — with no national transposition.

The aim: products placed on the EU market should be secure across their whole lifecycle. The CRA therefore shifts responsibility: it is no longer the user who has to make an insecure product safe, but the manufacturer who has to ship it secure and keep it secure.

> **The core idea:** the CRA does not ask "is your IT secure?", it asks "is your *product* secure — and does it stay secure for the whole support period?"

The penalties are substantial: up to **€15 million or 2.5 % of worldwide annual turnover**, whichever is higher. Market surveillance authorities can also prohibit distribution and order recalls.

1.2 How the CRA is structured

The regulation groups its requirements into a few very concrete areas:

1. **Product properties** (Annex I Part I) — how the product itself has to be built: secure default configuration, access protection, encryption, data minimisation, a limited attack surface.
2. **Vulnerability handling** (Annex I Part II) — which processes have to sit behind it: SBOM, vulnerability monitoring, updates, coordinated disclosure.
3. **Manufacturer duties** (Art. 13) — risk assessment, support period, conformity assessment, technical documentation.
4. **Reporting obligations** (Art. 14) — actively exploited vulnerabilities and severe security incidents to ENISA and the national CSIRT.
5. **Duties of the other actors** (Art. 19–22) — importers and distributors have to check, document and act when they see a risk.

> **A way to remember it:** Part I describes *the product*, Part II describes *your processes*. Together they make up CE conformity.

1.3 The deadlines — what applies from when?

The CRA arrives in stages. Anyone who only looks at the final date misses the first duty by more than a year:

11 Sep 2026	11 Dec 2027	5 years
reporting to ENISA begins	full application, CE required	minimum support period

From **11 September 2026**, manufacturers have to report actively exploited vulnerabilities and severe security incidents — whether or not the product has already been through a conformity assessment. From **11 December**

2027 the regulation applies in full: without a conformity assessment and CE marking, an affected product may no longer be made available on the EU market.

1.4 How it relates to other rules

Rule	Focus	Scope
CRA	cybersecurity of products	EU-wide, mandatory
NIS-2	cybersecurity of organisations	EU, critical sectors
ISO 27001	information security in general	voluntary (certification)
Machinery Regulation	safety of machinery	complements the CRA for machines
RED (radio equipment)	radio products	partly superseded by the CRA

> **Worth knowing:** an existing ISO 27001 ISMS already covers about half of the CRA process requirements — risk management, supplier control, the vulnerability process and incident response are the same building blocks in both worlds. What stays product-specific is classification, security by design, the SBOM and the conformity assessment.

2 Does it apply to you?

The CRA covers **products with digital elements** — every product that contains software or firmware and is placed on the EU market. The definition is deliberately broad: it also catches devices you would rarely call an "IT product".

A. Who counts as a manufacturer?

A manufacturer is anyone who develops a product, or has it made, and markets it **under their own name or trademark**. That holds even when major parts are bought in or a contract manufacturer builds it.

- software vendors (on-premise and in part SaaS)
- makers of connected devices (IoT, building technology, medical technology)
- machine and plant builders with control software
- suppliers of components carrying firmware
- white-label resellers of other companies' products

B. The three product classes

The classification decides the assessment route — and with it effort, cost and lead time:

Class	Examples	Assessment
Standard	the large majority of all products	internal control (self-assessment)
Important, class I	password managers, VPN, network management, browsers	self-assessment against a harmonised standard, or a notified body
Important, class II	firewalls, operating systems, hypervisors, microprocessors	notified body required
Critical	hardware security modules, smart cards, smart meter gateways	European certification scheme

C. Importers and distributors

Anyone importing products from outside the EU has to check, before placing them on the market, that the conformity assessment, the CE marking and the technical documentation exist. Distributors have to check the marking and inform the manufacturer and the authorities about risks they know of.

> **A special case:** if you substantially modify a bought-in product, or sell it under your own name, you become the manufacturer yourself — with every duty that carries, including for code you did not write.

D. Exemptions

Products already covered by sector-specific EU law are out of scope — medical devices, motor vehicles and civil aviation among them. Pure open-source software is also exempt, as long as it is not supplied in the course of a **commercial activity**.

> **A real example:** a machine builder with 60 staff ships plant with PLC control and remote maintenance access. The plant is a product with digital elements, falls under the CRA as a standard product and may be self-assessed — but it needs an SBOM, a vulnerability process, technical documentation and a five-year update commitment.

3 The path to conformity — 7 phases

CRA conformity is not made in the development department alone. It touches product management, purchasing, sales, legal and service. This order has proved itself:

Phase 1 — Product inventory and classification

Record every product, identify the digital elements, classify against Annexes III and IV. Result: you know which products are affected and which assessment route applies. *Two to four weeks.*

Phase 2 — Gap analysis

Compare your existing development and security processes against Annex I Parts I and II. Result: a solid list of gaps with an effort estimate. *Three to five weeks.*

Phase 3 — Risk assessment per product

The cybersecurity risk assessment under Art. 13(2), from which the concrete measures follow. Without it you cannot later explain why one thing was done — and another was not. *Two to four weeks per product family.*

Phase 4 — SBOM and vulnerability process

Generate the software bill of materials automatically in the build, link it to a CVE source, define reporting routes and deadlines, set up a contact point. *Six to ten weeks.*

Phase 5 — Product changes

Secure default configuration, update mechanism, signature verification, a smaller attack surface. The most demanding part — especially for products already in the field. *Three to nine months.*

Phase 6 — Technical documentation

Annex VI in full: product description, risk assessment, SBOM, test reports, support period. To be kept for ten years. *Four to eight weeks, alongside phase 5.*

Phase 7 — Conformity assessment and CE

Depending on the class, internal control or a notified body, then the EU declaration of conformity and the CE marking. *Four weeks to six months.*

> **Tip:** start phases 1 and 4 in parallel. The SBOM is the single most time-consuming technical task and later blocks everything else — the earlier it stands, the calmer the final stretch becomes.

4 What does the CRA cost?

Cost depends more on the product architecture than on the size of the company. What matters is whether an update mechanism exists and how many third-party components are built in:

Starting point	Total cost*	Timeframe	Internal effort
One product, modern architecture	**€14,000–22,000**	5–8 months	20–35 person-days
One product, existing device	**€22,000–38,000**	8–14 months	35–60 person-days
Product family (3–5 variants)	**€30,000–55,000**	9–15 months	50–80 person-days
Portfolio (10+ products)	**from €60,000**	12–24 months	½–1 FTE
Class II product	**plus €15,000–40,000**	+4–8 months	notified body

* Covers classification, gap analysis, risk assessment, building the SBOM, process definition and technical documentation. Excluding product development and the fees of the notified body.

What drives the cost?

- **No update mechanism:** retrofitting an update path into existing devices is by far the largest single item — often a replacement product is the cheaper route.
- **Number of third-party components:** the more libraries and bought-in parts, the more work the SBOM and vulnerability tracking take.
- **An existing ISMS (ISO 27001):** cuts the process effort by 30–50 %.
- **Product class:** class II calls for a notified body, with considerable lead time and fees of its own.

Running cost after conformity

Plan for **20–30 % of the set-up cost per year** to keep things running. On top of that:

- maintaining the SBOM with every release
- vulnerability monitoring and assessment
- security updates across the whole support period (at least 5 years)
- round-the-clock readiness for the reporting process
- keeping the technical documentation current

> **On transparency:** the ranges in the market are wide, because “CRA consulting” can mean very different things. A quote made without first classifying the products is not worth much — always ask which products and which class it assumes.

5 The 10 most common mistakes

From guiding a good many manufacturer projects, we know the usual stumbling blocks:

1. **Planning only for December 2027**
   The reporting duties start on 11 September 2026. Plan for the final date only, and the first actively exploited vulnerability finds you unprepared.

2. **Reading the scope too narrowly**
   “We are not a software house.” The CRA covers every product with firmware — from a sensor to a machine tool. Classification is the first step, not the last.

3. **Not costing the support period**
   Five years of updates is a commitment with a direct effect on pricing, spare-part stocks and staffing. It belongs in product management, not in development.

4. **The SBOM as a spreadsheet**
   Hand-kept parts lists are out of date after the second release. If the SBOM is not produced in the build, it is worthless when it matters.

5. **Not holding suppliers to account**
   You are liable for third-party components. Without a contractual duty to supply an SBOM and to report, you cannot meet your own obligations — and renegotiating takes months.

6. **A reporting process that exists only on paper**
   The 24-hour early warning runs at night and at weekends too. Without an on-call rota that can decide, the first real case is guaranteed to go wrong.

7. **Settling the conformity assessment too late**
   Notified bodies for the CRA are scarce. Ask in 2027 and you will not get a slot before the deadline.

8. **Reconstructing the technical documentation at the end**
   Annex VI calls for evidence from the whole development process. Gathered afterwards it costs several times as much — and stays incomplete.

9. **Treating the CRA as a development project**
   Product management, purchasing, sales, legal and service are all affected. A development team on its own runs aground on the support commitment and the supply chain.

10. **Misreading the open-source exemption**

The exemption only applies outside commercial activity. Build open-source components into a product you sell and you carry full responsibility for them.

6 Readiness check: are you ready?

Answer the following ten questions honestly with yes or no. The result shows your CRA maturity.

1. **Do you know which of your products fall under the CRA?**
   A product inventory marking the digital elements.
2. **Is every affected product classified against Annexes III and IV?**
   Standard, important class I/II or critical — with reasons.
3. **Have you set and published a support period for each product?**
   At least 5 years, visible before purchase (Art. 13(8)).
4. **Is there a documented cybersecurity risk assessment?**
   The basis for every measure under Art. 13(2).
5. **Do your products ship free of known vulnerabilities?**
   Secure baseline configuration, no default passwords, no open debug access.
6. **Do you keep a machine-readable SBOM per product?**
   CycloneDX or SPDX, generated automatically in the build.
7. **Do you watch for vulnerabilities in your components systematically?**
   SBOM linked to a CVE source, mapped to the affected products.
8. **Can you ship security updates promptly?**
   An update mechanism in place, separate from feature updates.
9. **Is a 24 h / 72 h / 14 day reporting process set up and rehearsed?**
   On-call rota, access to the ENISA platform, a documented procedure.
10. **Does technical documentation under Annex VI exist?**
    Description, risk assessment, SBOM, test reports — to be kept for ten years.

Your yes answers	Where you stand	What to do
0–3 × yes	**At acute risk**	Start on the product inventory and classification now. Expect 12–18 months to conformity — and the reporting duty from September 2026 comes before that.
4–6 × yes	**Partly prepared**	Focus on the gaps — usually the SBOM, the reporting process and technical documentation. 6–10 months.
7–10 × yes	**A good base**	Prepare the conformity assessment and complete the documentation. 3–6 months.

CRA conformity is within reach — but only with structured planning and an early answer on the product class. If you have questions, or the classification is unclear, a free first conversation helps.

7 Glossary

The key terms around the CRA, explained plainly:

CRA

Cyber Resilience Act — Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements.

Product with digital elements (PDE)

Any software or hardware product, including its remote data processing solutions, whose intended use involves a data connection.

SBOM

Software bill of materials — a machine-readable list of every software component in a product. Common formats: CycloneDX, SPDX.

Security by design

Security is built in from the start of development instead of added afterwards. The CRA makes it binding through Annex I Part I.

Support period

The period in which the manufacturer has to provide security updates — at least five years, or the expected lifetime if that is shorter.

ENISA

The European Union Agency for Cybersecurity — the central reporting point for CRA incidents, together with the national CSIRT.

CSIRT

Computer Security Incident Response Team — the national contact point for security incidents; in Germany it sits at the BSI.

Actively exploited vulnerability

A vulnerability with reliable evidence that attackers are in fact exploiting it. Triggers the 24-hour early warning.

Coordinated vulnerability disclosure (CVD)

A defined route for security researchers to report vulnerabilities — a contact point and a handling process are mandatory.

Notified body

A conformity assessment body notified by a member state, which carries out the assessment for important class II products and critical products.

EU declaration of conformity

The manufacturer's declaration under Annex V that the product meets the requirements. A precondition for the CE marking.

Technical documentation

The evidence package under Annex VI — product description, risk assessment, SBOM, test reports. To be kept for ten years after placing on the market.

Market surveillance authority

The national authority that inspects products, demands evidence and can prohibit distribution. In Germany this will most likely be the BNetzA and the BSI.

Substantial modification

A change that affects the conformity of the product — it triggers a new conformity assessment.

8 Your next step

You have read this guide — that is the first step already. Implementing the CRA in a structured way secures your market access, reduces liability risk and keeps your products sellable beyond December 2027.

A free first conversation

In a 30-minute call, with no obligation, we work out together:

- ✓ Which of your products fall under the CRA?
- ✓ Which product class applies — and which assessment route?
- ✓ Where do you stand on SBOM, updates and reporting?
- ✓ What timeframe and what budget are realistic?

No sales pitch, no pressure — just an honest assessment.

The CRA quick check

On **iso-easy.de** you can test in 3 minutes whether the CRA applies to you and get a first read on your maturity — without leaving any contact details.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

iso-easy.de

iso-easy is part of notivia GmbH.

With more than 30 years in IT consulting and information security we support manufacturers in implementing the CRA, ISO 27001, NIS-2 and neighbouring standards — practical, transparent and as equals.

© 2025/2026 notivia GmbH — **iso-easy.de** | All rights reserved.