IT-BERATER / WORKING COLLECTION

Cyber Resilience Act Organisational Pack

Organisational CRA readiness guidance and evidence collection.

Working pack · Editable edition

Figure 1 · Cover illustration; supplementary illustration. Use the guide and completed cards for the full detail.

Open the files

Extract the complete ZIP into its own folder first. In the top-level folder, open `produktsicherheit-guide-en.pdf` for the guide and `produktsicherheit-workbook-en.pdf` for the separate workbook. The matching DOCX files are editable. `produktsicherheit-full-en.pdf` also combines all cases, exercises, sources and licence information in one document. Further editable templates are in `editable/en/`; Markdown and CSV working files are in `package/en/`. The German edition is included too.

Germany/EU · 19 September 2026 · EUR 79

Outcome: a traceable case file with evidenced answers, named unknowns and a clear handover.

• Read GUIDE_EN.md and assign roles and evidence storage.

• Import WORKBOOK_EN.csv as UTF-8 or copy the Markdown form. Use a separate file per matter.

• Practise with completed cases A/B; their evidence is entirely fictional.

• Record real answers with evidence, owner, date, next action and review. Unknowns stay open; inapplicability needs a reason.

• Before closure, verify execution and accessible evidence.

INVENTORY_EN.md lists every included file; LICENSE_EN.md sets out internal usage. SOURCES.md records legal sources. The guidance does not replace a specific professional decision or legal advice. This English edition does not extend the geographical scope.

Guide: CRA readiness as an organisational routine

Purpose and boundaries

This guide treats the Cyber Resilience Act (CRA) as an operating flow: inventory the product, review role and scope, document cyber risk, collect secure-by-design evidence, run a vulnerability channel, set the support period and escalate incidents. It is not a conformity assessment, audit or legal advice.

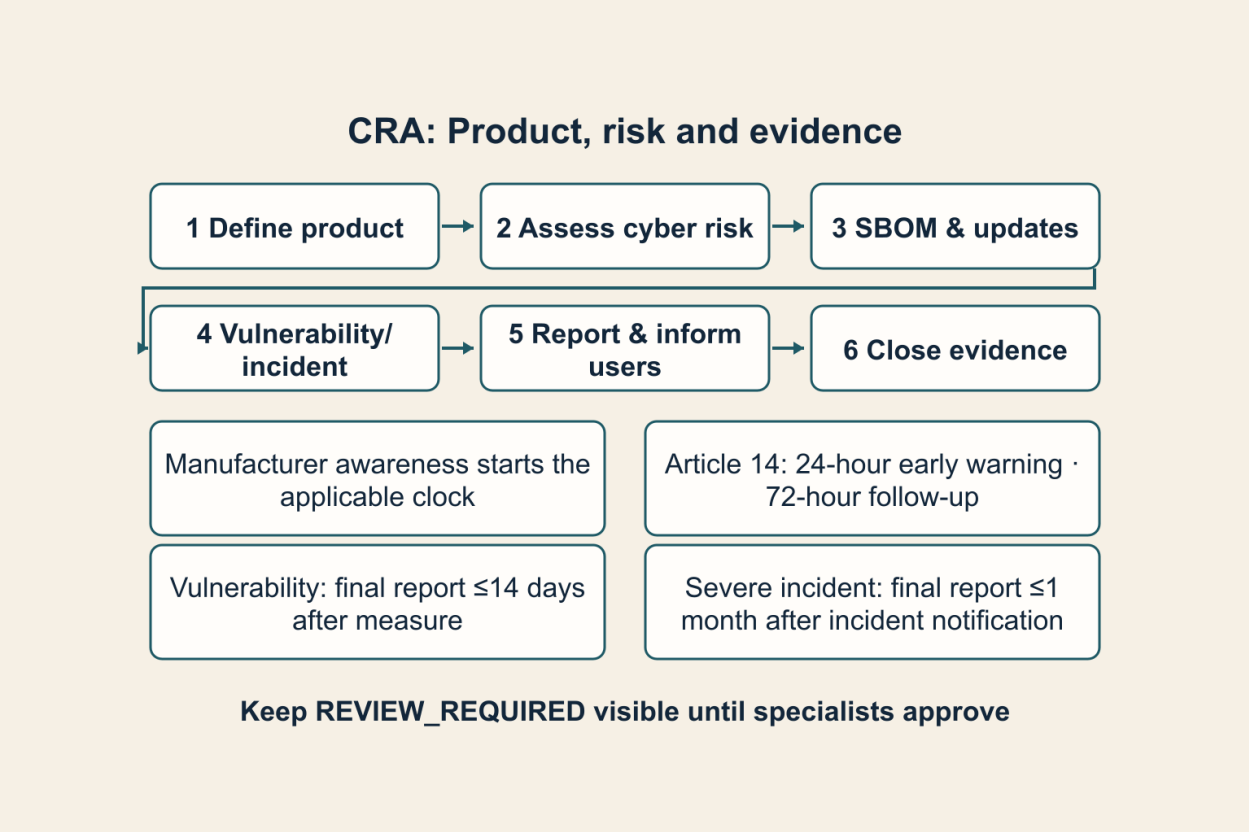

Figure 2 · Working sequence; supplementary illustration. Use the guide and completed cards for the full detail.

1. Define product and role

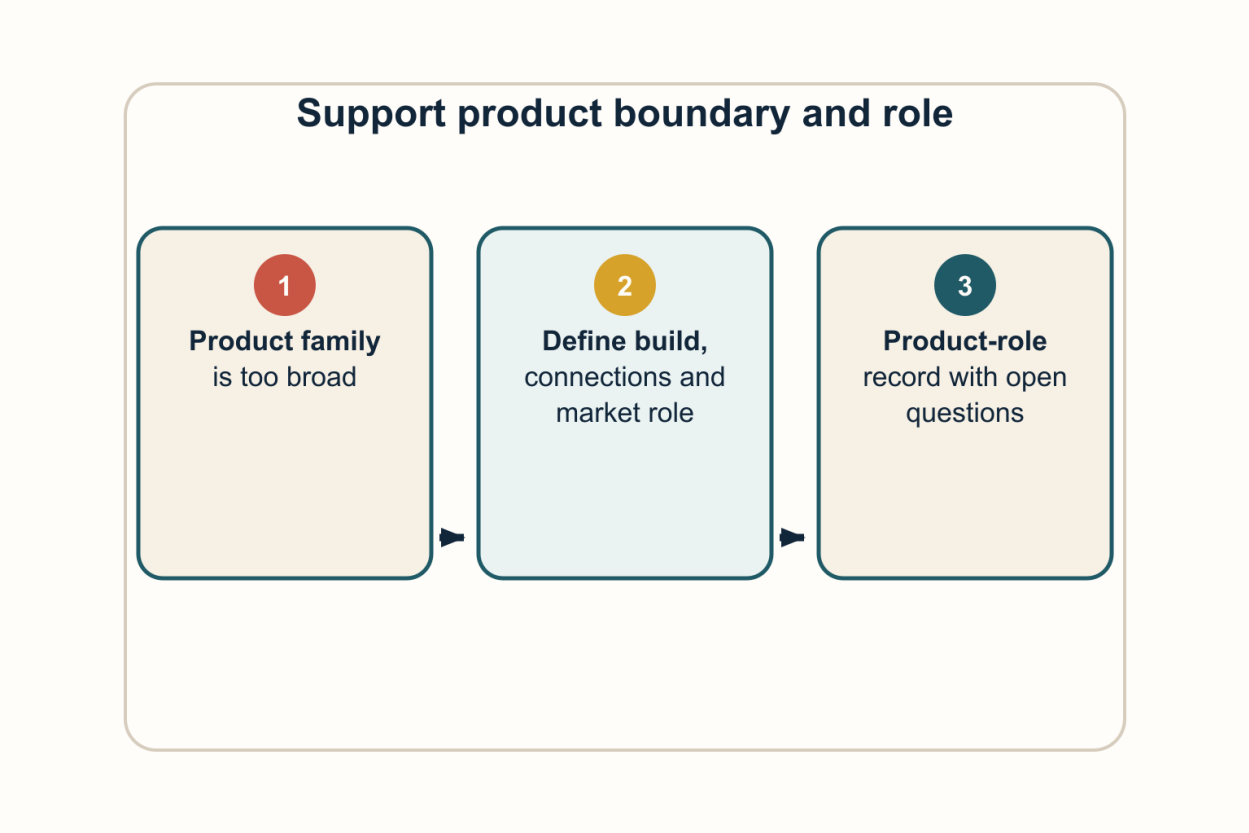

Figure 3 · Support product boundary and role. Situation, action and bounded result.

Record product name, version, variants, manufacturer, importer, distributor, open-source steward, EU markets and data/network connection. CRA Article 2 covers products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect connection. Review exclusions and overlaps, including sectoral Union acts, in `M7-CRA-01`; “scope likely” is not a legal conclusion.

2. Risk and secure development

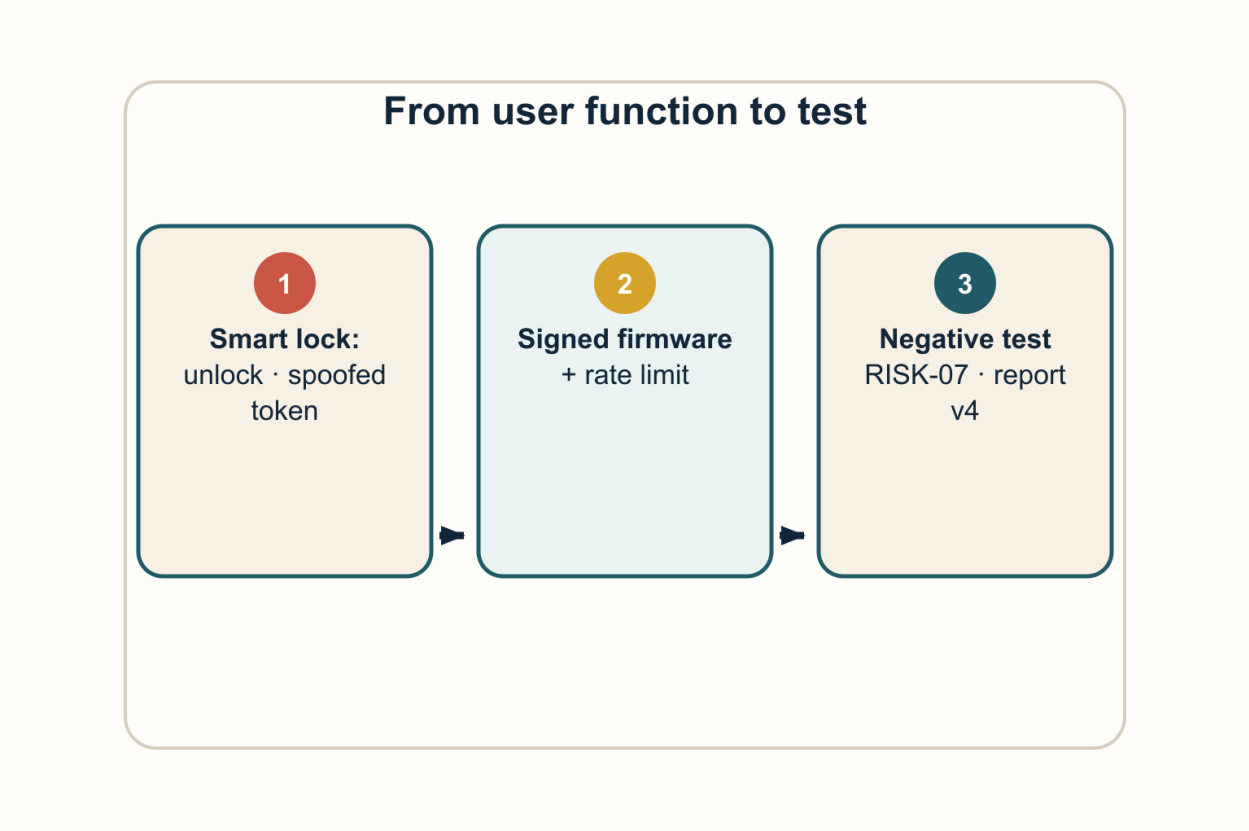

Figure 4 · From user function to test. Situation, action and bounded result.

Under Article 13 the manufacturer documents a cybersecurity risk assessment and accounts for it during planning, development, production, delivery and maintenance. Record assets, attack surface, assumptions, operating environment, expected use period, residual risk, controls and open decisions. Annex I Part I includes, among other things, no known exploitable vulnerabilities, secure defaults, updates, access control, confidentiality, integrity, availability and data minimisation.

3. Components and SBOM

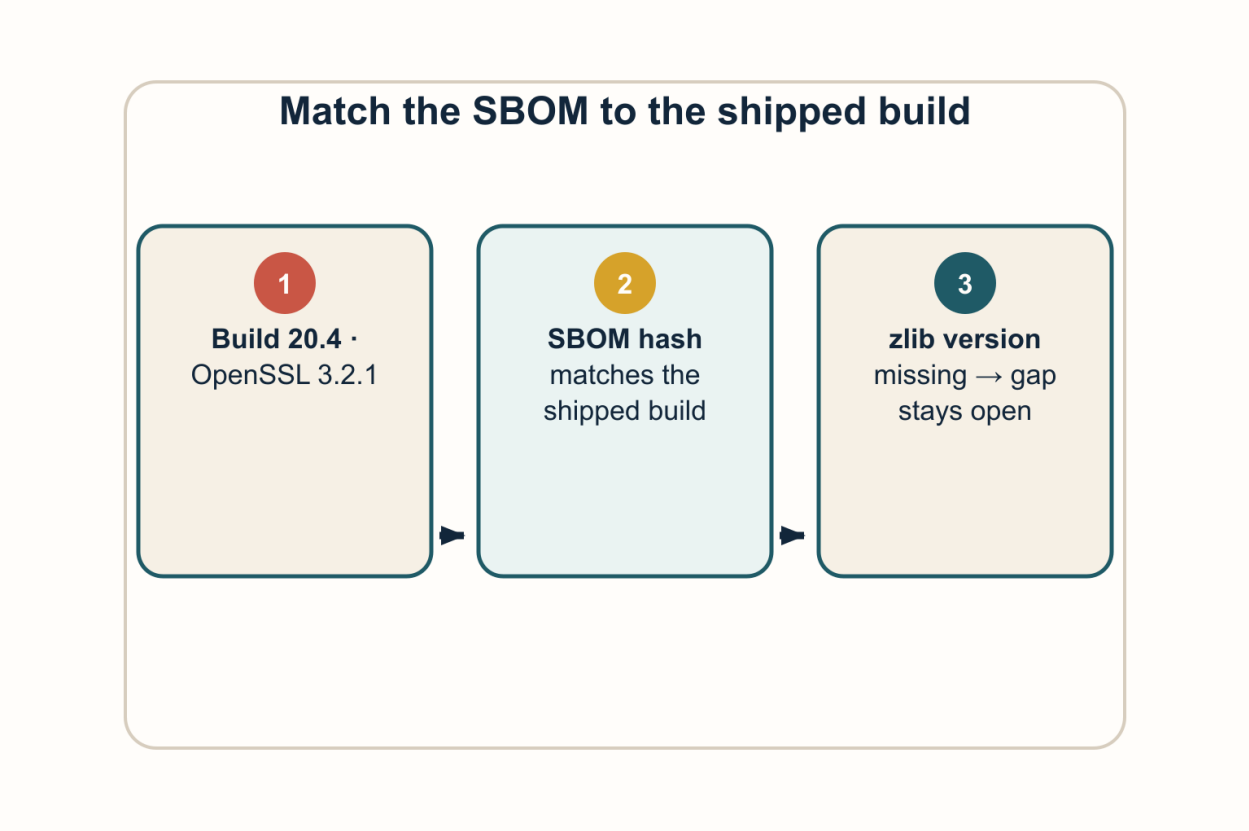

Figure 5 · Match the SBOM to the shipped build. Situation, action and bounded result.

Create a verifiable component list/SBOM with version, origin, licence, owner and review evidence. Annex I Part II requires at least top-level dependencies in a commonly used machine-readable format. The workbook records status; it does not prove SBOM technical accuracy.

4. Vulnerability handling

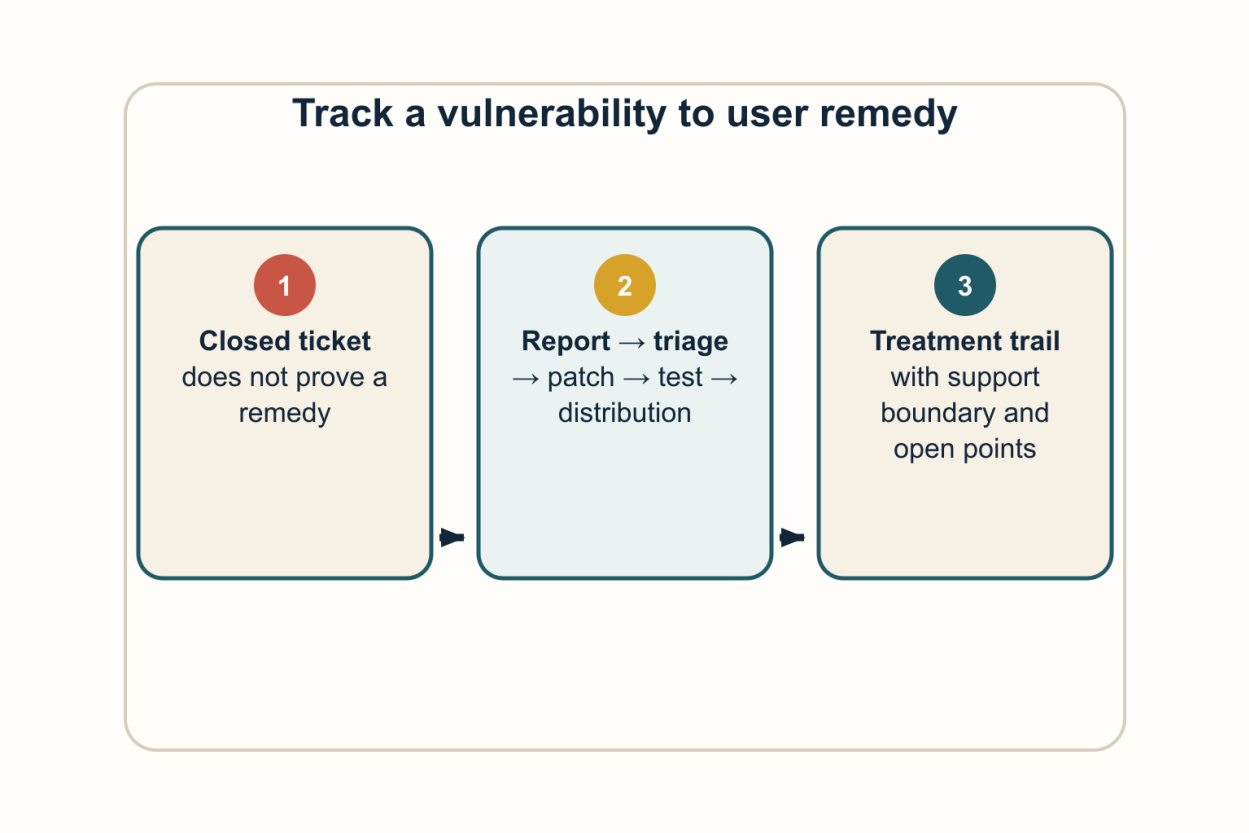

Figure 6 · Track a vulnerability to user remedy. Situation, action and bounded result.

Provide a public reporting contact, triage, severity, owner, patch/mitigation decision, testing, secure distribution and disclosure evidence. Record whether security updates can be separated from feature updates. Set a reasoned support period and end date; Article 13 generally names at least five years where expected use is not shorter. Do not mark a field “secure” based only on an unverified assertion.