CRA Article 14 Reporting Readiness Checklist

For manufacturers of products with digital elements on the EU market · Reporting obligations apply from 11 September 2026 (Art. 71(2)) · July 2026 edition

This product is a compliance-support tool, not legal advice. It does not determine, submit, or guarantee compliance with CRA (Regulation (EU) 2024/2847) reporting obligations. You (the manufacturer) remain responsible for all reporting decisions, submissions, and deadlines. Verify all outputs and consult a qualified professional.

1. Inventory the products in scope

- List every product with digital elements you place on the EU market, with versions and support status.
- Include **legacy products** already on the market before 11 December 2027: by way of derogation, the Article 14 reporting obligation applies to them (Art. 69(3)).
- Keep the distinction explicit in your records: Art. 69(3) extends the **reporting** duty to legacy products; Art. 69(2) concerns the **substantive** requirements and its "substantial modification" condition. Do not conflate the two paragraphs.
- For each product, record where its incident and vulnerability information lives (e.g., which Jira / JSM projects).

2. Prepare the reportability decision

- Assign a named role who confirms whether a case is reportable, and record the basis for each call.
- Vulnerability path (Art. 14(1)): the duty concerns an **actively exploited vulnerability** — "actively exploited" is a defined term (Art. 3); the essence is reliable evidence of exploitation, not a severity score alone.
- Incident path (Art. 14(3)): the duty concerns a **severe incident**. Art. 14(5) frames severity: (a) negative impact (actual or capable) on the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; (b) the introduction or execution of malicious code.
- Define how you will record the **awareness time** the moment a case opens — not reconstructed later from chat history.
- Treat boundary cases conservatively: interpretation of "becomes aware" and of severity edge cases depends on official guidance — route them to **human / expert confirmation**, and record the reasoning.

3. Prepare the staged reports — and anchor both final-report clocks correctly

Path	Early warning	Notification	Final report — start point
Actively exploited **vulnerability** (Art. 14(2))	within 24 hours of becoming aware	within 72 hours of becoming aware	within **14 days after a corrective or mitigating measure is available** (Art. 14(2)(c))
Severe **incident** (Art. 14(4))	within 24 hours of becoming aware	within 72 hours of becoming aware	within **one month after the 72-hour notification is submitted** (Art. 14(4)(c))

- Write the **two different final-report start points** into your runbook as two separate lines. Neither clock starts from awareness.
- Instrument your process to capture the trigger events: the date a corrective / mitigating measure becomes available (vulnerability path) and the timestamp your 72-hour notification is submitted (incident path).
- Pre-agree a skeleton for the 24-hour early warning: it is a first signal, not an analysis — decide in advance who may send an incomplete message.
- Rehearse the flow once end-to-end (tabletop) before 11 September 2026.

4. Prepare the two notices beyond the authorities

- Draft the **affected-user notice** template now (Art. 14(8)): users must be informed of an actively exploited vulnerability and, where relevant, of risk-mitigating or corrective measures they can apply.
- Note the consequence of inaction: where the manufacturer fails to inform users, the coordinating CSIRT may inform them directly where it considers that proportionate and necessary (Art. 14(8)).
- Prepare the **upstream component notice**: where a vulnerability sits in an integrated third-party component (open source included), report it to the person or entity that makes or maintains the component (Art. 13(6)).
- Record component provenance in your tickets so the upstream duty is visible when a case opens.

  A complete Article 14 case can require up to five documents: three authority stages plus the two notices above.

5. Prepare for the ENISA Single Reporting Platform

- Structure your internal draft templates around the **per-stage reporting data items ENISA has published** (mandatory / optional / conditional / known-at-the-time markings per stage) — the structure survives form changes.
- Plan for submission via the **single reporting platform** established under Art. 16(1): one submission reaching the coordinating CSIRT and ENISA. Registration procedures and exact forms are still being finalized as of July 2026 — treat dates and onboarding steps as planned, not settled.
- Do not hard-code a submission form. Keep an **export-and-submit** posture: produce a complete draft; a person submits through the official channel in the form it takes at go-live.
- Assign a recurring slot (e.g., biweekly) to check ENISA's SRP pages and the European Commission's CRA reporting page for registration details and the pre-go-live testing period.

Sources: Regulation (EU) 2024/2847 (Cyber Resilience Act) — Art. 3, 13(6), 14(1)–(8), 16(1), 69(2)–(3), 71(2), EUR-Lex; European Commission, "Cyber Resilience Act — Reporting obligations" (digital-strategy.ec.europa.eu); ENISA, Single Reporting Platform pages (enisa.europa.eu). Platform status statements reflect public information as of early July 2026 — verify current status on the official pages. This checklist is general information, not legal advice.