CRA Vulnerability Reporting Readiness Checklist

The Cyber Resilience Act (CRA) introduces a shift from reactive vulnerability handling to structured, time-bound reporting obligations for manufacturers of products with digital elements.

Meeting these obligations requires operational readiness across product knowledge, monitoring capabilities, internal workflows, and external coordination.

The following checklist provides a practical self-assessment to help organizations evaluate their preparedness for CRA vulnerability reporting and identify gaps ahead of the upcoming regulatory milestones.

1. Product Scope

- ☐ Inventory all products currently on the EU market that qualify as "products with digital elements" under the CRA
- ☐ Classify each product as default, Important Class I, Important Class II, or Critical (Annex III/IV)
- ☐ Include legacy products regardless of when they were placed on the market (Article 69(3))
- ☐ Document the intended purpose and reasonably foreseeable use for each product family
- ☐ Document the Member States where each in-scope product has been made available

2. Software Visibility

- ☐ Generate or update a Software Bill of Materials (SBOM) for all in-scope products, including those already on the market
- ☐ Use a machine-readable format (CycloneDX or SPDX)
- ☐ Run SCA tooling against current firmware/software images for legacy products where build-time SBOMs don't exist
- ☐ Produce VEX documents for known CVEs to record whether they are exploitable in your product

3. Vulnerability Monitoring

- ☐ Subscribe to automated feeds for CISA KEV, ENISA EUVD, and NVD
- ☐ Subscribe to vendor advisories for all third-party components in your products
- ☐ Implement automated vulnerability monitoring of disclosed CVEs against your SBOM component inventory
- ☐ Define the criteria for what constitutes an "actively exploited vulnerability" under Article 14(1) for your specific company scenario
- ☐ Define the criteria for what constitutes a "severe incident having an impact on security" under Article 14(1) for your specific company scenario

4. Internal Reporting Workflow

- [ ] Designate a PSIRT lead (or equivalent) who owns triage decisions and signs off on ENISA submissions with a defined process, role, and escalation path
- [ ] Designate an analyst responsible for monitoring feeds and drafting reports
- [ ] Identify a legal/compliance contact who is notified of all submissions
- [ ] Write a runbook (checklist format) for each reporting stage: 24-hour early warning, 72-hour detailed notification, final report
- [ ] Prepare reporting templates with the information mentioned by the CRA FAQ, including product names, versions, and Member States where the product is available, so that early warnings can be drafted quickly during the reporting phase
- [ ] Log evidence (timestamps, decisions, communications) in an audit-ready record for each case
- [ ] Define escalation logic for incidents that may also trigger NIS2, GDPR, or sector-specific reporting obligations, to ensure consistent and non-contradictory notifications
- [ ] Run at least one tabletop exercise simulating a full reporting cycle before September 2026

5. Coordinated Vulnerability Disclosure

- [ ] Ensure the CVD policy (Annex I, Part 2(5)) has a clear contact channel (security.txt, dedicated mailbox, PGP key)
- [ ] Define an acknowledgment timeline and initial severity assessment timeline
- [ ] Set disclosure timing to protect users while avoiding public disclosure before a mitigation is available, unless there is a justified reason
- [ ] Connect the CVD intake process to your internal triage workflow aligned with CRA reporting obligation timelines

6. Supply Chain

- [ ] Request component-level SBOMs from all third-party suppliers to perform security due diligence on component and software suppliers (Article 13(5))
- [ ] Ensure supplier contracts include obligations for vulnerability notification, SBOM provision, and support duration
- [ ] Confirm patch availability commitments for critical components
- [ ] Negotiate these commitments into supplier agreements where they don't already exist

7. User Notification

- [ ] Identify or establish a channel for notifying affected users (security advisories page, email notification list, device-level push notifications)
- [ ] For products without a direct communication channel to end users, determine an alternative path (distributors, resellers, public advisory page)
- [ ] Draft a notification template that can be adapted quickly during an incident

8. ENISA Platform Registration

- ☐ Identify the legal entity (manufacturer or authorized representative) that will submit notifications to the ENISA SRP
- ☐ Actively monitor ENISA SRP page and ENISA FAQ page for new updates
- ☐ Prepare registration data: legal entity information, in-scope product list, designated reporting contacts (primary and backup)
- ☐ Confirm your coordinator CSIRT (based on main EU establishment for EU manufacturers, or authorized representative's Member State for non-EU manufacturers)
- ☐ Participate in the SRP testing period if available to validate your submission workflow before a real incident
- ☐ Register as soon as the platform opens; do not wait for a reportable event