Executive Summary — CRABasics

CRABasics is the leading open and practitioner-focused resource center dedicated to helping organizations understand and comply with the European Union's Cyber Resilience Act (CRA). As the CRA introduces mandatory cybersecurity requirements for all products with digital elements, CRABasics provides clear, practical guidance to accelerate readiness and reduce compliance risk.

A recurring challenge for many IoT vendors and manufacturers of products with digital elements (PDE) is the persistent weakness in vulnerability-management practices, an issue that continues to affect a significant portion of the market. CRABasics experts have repeatedly highlighted these shortcomings as one of the main obstacles vendors face when building secure products.

Our deep experience in designing and operating effective Coordinated Vulnerability Disclosure (CVD) programs reinforces our leadership in this area. This expertise enabled us to contribute to the draft CRA harmonised standard, prEN 40000-1-3, ensuring practical, real-world vulnerability-management requirements are properly reflected.

Vote: AGAINST ("I oppose")

1. Lack of strict alignment with the Cyber Resilience Act (CRA), proportionality, and repeatability

Several requirements go beyond CRA Annex I, impose process mandates that are not legally required, and rely on ambiguous "risk-based" enhancements (RE) that undermine repeatability. All normative "shall" requirements should trace explicitly to CRA Annex I, Part II. Non-essential process prescriptions should be converted to recommendations backed by objective acceptance criteria.

2. Process-prescriptive wording instead of outcome-based principles

The draft often mandates organisational structures, policies, planning artefacts, or frameworks rather than defining capability-based outcomes. SMEs and startups may comply with CRA using lightweight but effective processes. Requirements should therefore focus on outcomes demonstrating CRA conformity rather than prescribing organisational models.

3. Lack of clarity, testability, and drafting quality issues

Terms such as “rigor” or formulations like “shall be considered” are vague and untestable. Several clauses mix policies with processes, use inconsistent terminology, or employ passive voice. Requirements should be rewritten using clear, active language (e.g., “The manufacturer shall…”), define unusual terms, and separate high-level policy expectations from process detail.

High-Priority Changes Requested

1) Structure and taxonomy

- The current draft relies on an overly complex system of four requirement tags (RQ, RC, RE, PM) that must be consolidated to ensure all normative requirements are testable and strictly aligned with CRA Annex I, Part II.
- Requirement Enhancements (RE): remove from normative text or provide objective applicability criteria. Consider relocating RE to an informative annex.
- Documentation/assessment units: add a normative clause defining assessment units, success criteria, and required documentation, including a standard template.

2) CRA alignment

- Replace mandatory continuous monitoring with obligations to identify vulnerabilities. CRA Annex I requires identification and regular testing, not continuous monitoring.
- Accessibility: shift the "Accessibility" section to focus on frictionless discovery (e.g., security.txt, no mandatory user accounts) rather than just file formats.
- Planning: CRA requires remediation “without delay”. Fixed schedules may be infeasible. Use outcome-based timing anchored in “without delay”.
- Severity/advisories: mandate severity when advisories are issued. Allow updates when exploitability changes.
- Updates: CRA requires secure distribution “without delay”, not monitoring installation. Remove obligations to monitor installation or user behavior.
- Include obligations of importers/distributors in scope as per CRA Articles 19/20.

3) Policy vs. process

- Keep policy as high-level principles: place evolving details in processes/guidance.
- Use active voice: “The manufacturer shall establish, implement and adhere to a vulnerability handling policy.”
- Operational security: make it a “shall” with criteria (need-to-know, auditability), while allowing early sharing in high-risk cases.

4) Communication and accessibility

- CVD policy: clarify accessible channels, avoid vague terms such as “sensory channels”, and make ongoing communication mandatory.
- Secure communication: provide non-exhaustive examples (TLS, S/MIME, OpenPGP), allow anonymous reporting, and accept capability evidence even when no reports exist.

5) Identification (product/SBOM/hardware)

- Product ID: avoid requiring separate HW/SW identifiers; treat product identification holistically.
- SBOM: require “all known components” rather than “all components”; remove risk assessment as SBOM input; define machine-readable by criteria (structured/parseable) and allow SPDX, CycloneDX, or structured CSV/Excel.
- Hardware completeness: align assessment criteria with mandated requirements.

6) Verification & Validation, tests, and reviews

- Distinguish SBOM correlation from testing; insert explicit V&V before prioritization.
- Use trigger-based V&V when new intelligence emerges; tailor test cases to vulnerability type.
- Replace fixed annual cadence with CRA’s “effective and regular” approach.

7) Release & advisories

- Include risks and customer impact in advisories. Allow delayed publication only under defined risk conditions and with a disclosure date.
- Define machine-readable advisory criteria (structure, parseability) and allow several formats.

8) Post-release actions

- Recognize offline installations.

Closing Note

CRABasics OPPOSES this version of the draft harmonized standard.

The proposed changes aim to strengthen legal alignment with CRA, enforce repeatability, improve drafting clarity, and ensure feasibility for SMEs. Converting process-prescriptive “shall” requirements to outcome-based, CRA-aligned wording will substantially improve the document.