CRA READINESS CHECKLIST

Quick wins for SBOM, vulnerability handling, risk assessment, and evidence you can show

HOW TO USE

- ◯ Print or duplicate into your workspace.
- ◯ Assign owners and due dates.
- ◯ Store proof in a single evidence location (repo/folder) you can show during audits.

cetome
we make cyber work

RS Strategy

Technical excellence + Regulatory expertise

EU Cybersecurity Specialists
25+ Years Combined Experience
Active EU Policy Contributors

SCOPE AND ROLES

Who are you under the CRA?

- ◯ Manufacturer
- ◯ Importer
- ◯ Distributor
- ◯ Authorised representative

***Manufacturers** carry primary duties; importers/distributors verify CE/DoC and act on suspected non-compliance).*

NAMED OWNERS

- ◯ SBOM:
- ◯ Vuln handling:
- ◯ Risk assessment:
- ◯ Documentation:

*Converge towards a **security support period** and an **update policy** (per product family).*

SBOM (SOFTWARE BILL OF MATERIALS)

***Why:** CRA expects accurate component transparency to manage risk and inform users/authorities on request—SBOMs are how to do this.*

- ◯ Choose SBOM format and toolchain (SPDX or CycloneDX).
- ◯ Generate SBOM per release; include all first/third-party components and versions.
- ◯ Request and ingest supplier SBOMs for key dependencies; define validation checks.
- ◯ Decide publication method and access policy.
- ◯ Version and store SBOMs + generation/validation logs with the build artifacts.

***Proof to keep:** SBOM files, tool configs, generation logs, supplier requests/responses, validation checklist results.*

info@crabasics.com

VULNERABILITY HANDLING (PSIRT/CVD)

Why: *CRA requires a public vulnerability reception point, timely triage/remediation, coordinated disclosure, and free security updates during the declared support period without undue performance degradation. A disciplined process is critical.*

- ◯ Publish intake: security.txt or VDP page with contact, scope, and expectations.
- ◯ Acknowledge all reports within 3 business days; authenticate reporters as needed.
- ◯ Triage rubric defined (severity, exploitability, impact) and remediation SLAs agreed.
- ◯ Advisory template + approval path ready; define when/how to notify users.
- ◯ Case log in place to track from report → fix → disclosure; link to commits/tests.
- ◯ Prepare update packaging and testing so security updates are fast and don't unduly degrade performance.

Proof to keep: *VDP policy, intake records, triage decisions, fix evidence, advisories, notification lists.*

TRANSPARENCY, UPDATES, AND SUPPORT PERIOD

Why: *CRA requires clear user information on configuration, security instructions, update policy, and the declared security support period; security updates must be free during that period.*

- ◯ Publish security instructions (intended use, config/install, etc.).
- ◯ Publish update policy and support period; ensure teams honour it.
- ◯ Make updates easy to apply and, where feasible, reversible; communicate impact and downtime.

RISK ASSESSMENT (LIFECYCLE)

Why: *CRA expects ongoing, product-lifecycle risk management from design to end-of-life; decisions and residual risk should be recorded.*

- ◯ Define scope (product, interfaces, data flows, environments).
- ◯ List top threats per use case; rate likelihood and impact.
- ◯ Document mitigations with owners/dates; validate and link to tests/artifacts.
- ◯ Record residual risk and rationale; set review cadence.

Proof to keep: *Risk register and change history, mitigation tickets/PRs, validation evidence, approvals.*

TECHNICAL DOCUMENTATION (YOUR "TECHNICAL FILE")

Why: *Under the EU product-law (NLF) model, you need auditable technical documentation to support CE/DoC and market surveillance requests.*

Your technical file must include:

- ◯ Design and architecture overview
- ◯ Threat/risk assessment and decisions
- ◯ Secure development practices and test results
- ◯ SBOM/component list and license posture
- ◯ Vulnerability handling/PSIRT procedures and case log
- ◯ User instructions, update policy, and security support period
- ◯ Post-market surveillance plan or records

Brought to you by

cetome
we make cyber work

RS Strategy

info@crabasics.com