CRA Readiness Checklist

Cyber Resilience Act – Full Pre-Conformity Assessment Framework

---

1. Product Scope Confirmation (Annex I & Article 2)

Verify whether your product falls under the CRA

☐ The product contains software (embedded, installable or executable).
☐ The product is hardware with integrated software or firmware.
☐ The product has direct or indirect network connectivity.
☐ The product processes, stores or transmits digital data.
☐ The product is placed on the EU market.
☐ The product is not covered by sector-specific legislation (MDR, IVDR, RED etc)
☐ Assessment of "Product with Digital Elements (PDE)" completed.
☐ Final in-scope confirmation documented.

---

2. Economic Operator Role Identification (Articles 13–17)

Define your legal obligations based on your role

☐ Manufacturer
☐ Importer
☐ Distributor
☐ Authorised Representative
☐ Obligations corresponding to each role identified and documented.
☐ A security contact point has been established (Article 11.1).

---

3. Product Classification (Annex III – Default vs Critical Class)

Determine the product's regulatory category

- ☐ Default Class criteria assessed
- ☐ Critical Class criteria assessed
  - ☐ Critical Class I (high-risk product features)
  - ☐ Critical Class II (network security or essential services impact)

- ☐ Final classification documented and archived.
- ☐ Impact of classification on conformity route understood (Annex IV).

---

4. Essential Cybersecurity Requirements (Annex I – Section 1)

Assess technical security, design and architecture

- ☐ Secure-by-design principles applied
- ☐ Secure-by-default configuration implemented
- ☐ Access control and isolation mechanisms in place
- ☐ Secure credential management (no hardcoded secrets)
- ☐ Software integrity protection (firmware signing, secure boot)
- ☐ Use of modern, industry-accepted cryptography documented
- ☐ Secure data processing and transmission
- ☐ Logging and monitoring proportional to product risk
- ☐ Protection against physical tampering (where applicable)
- ☐ Pre-market security validation completed and evidence archived

---

5. Vulnerability Handling Requirements (Annex I – Section 2)

Continuous identification, handling and reporting

- ☐ Vulnerability management process established (intake, triage, prioritisation,

remediation, closure)
☐ Public vulnerability reporting channel available (Article 12)
☐ Coordinated Vulnerability Disclosure (CVD) policy published
☐ Continuous monitoring of SBOM components and CVEs
☐ Assessment of exploitability and impact documented
☐ Vulnerability register maintained per Annex VII
☐ User notification procedure for unpatched vulnerabilities defined

---

6. Update & Patch Management (Annex I – Section 2 + Annex II)

Ensure secure updates throughout the product lifecycle

☐ Secure update mechanism implemented (signed, authenticated, validated)
☐ Rollback prevention in place to block insecure versions
☐ Support and update lifetime defined and communicated
☐ Update validation and regression testing procedures documented
☐ Full update history maintained (Annex VII)
☐ Users informed of security-critical updates

---

7. Secure Development Lifecycle (SDL)

(Annex I + industry best practice)

☐ Documented secure development processes
☐ Regular threat modelling and risk analysis
☐ Security-focused code reviews
☐ Automated security testing and/or penetration testing
☐ Supply chain controls integrated in CI/CD pipelines

---

8. Supply Chain & SBOM

Requirements (Annex I + Annex II)

Full management of dependencies and third-party components

- ☐ Complete SBOM maintained (software, firmware, libraries)
- ☐ SBOM-based vulnerability monitoring established
- ☐ Supplier security requirements defined
- ☐ Cybersecurity clauses included in supplier contracts
- ☐ Supplier → manufacturer incident notification process defined

---

9. Mandatory CRA Technical Documentation (Annex II)

Everything that must exist BEFORE placing the product on the market

- ☐ System architecture and design documentation
- ☐ Cybersecurity risk assessment
- ☐ Security testing evidence
- ☐ Update mechanism documentation
- ☐ Vulnerability handling procedures
- ☐ SBOM included in the technical file
- ☐ Post-Market Monitoring plan (Annex VII)
- ☐ EU Declaration of Conformity prepared
- ☐ User security instructions drafted and verified

---

10. Conformity Assessment Route (Annex IV)

Choose the correct regulatory path

- ☐ Selected conformity assessment procedure:
  - ☐ Internal Control (Default Class)
  - ☐ Third-Party Assessment (Critical Class I/II)

- ☐ Technical documentation reviewed and complete
- ☐ Evidence ready for inspection
- ☐ Legal and regulatory review completed

☐ CE marking prepared

---

11. Post-Market Monitoring Readiness (Annex VII)

☐ Incident register established
☐ Vulnerability register active and maintained
☐ Security KPIs/metrics defined
☐ Procedures for reports to authorities prepared
☐ Continuous monitoring process operational

---

12. CRA Compliance Roadmap (2025–2027)

☐ Gaps identified based on Annex I, II and VII
☐ Prioritised remediation plan created
☐ Resources (budget, personnel, tooling) approved
☐ Timeline aligned with enforcement and deadlines
☐ Key stakeholders informed and assigned

---

13. Final Readiness Assessment

☐ High – product is ready for conformity
☐ Medium – minor gaps remain
☐ Low – major remediation required
☐ Next corrective actions documented