CHECKLIST by The Embedded Kit

Be CRA-ready from Day One

With the upcoming European regulation known as the Cyber Resilience Act (CRA), device manufacturers must prepare to meet a series of technical and organizational requirements. **Harmonized standards** designed to guide compliance are expected to be published by October 2026, with **mandatory compliance required as early as the end of 2027**.

Here’s a checklist to help you efficiently anticipate and address these requirements:

- □ No exploitable vulnerabilities
  Solutions: SBOM + CVE assessment
- □ Secure by defaul configuration
  Solutions: No default password, key diversification
- □ Security updates
  Solutions: Automated updates, code signing, anti-rollback
- □ Access control mechanisms
  Solutions: Identify and categorize assets, robust authentication, IAM
- □ Ensure confidentiality
  Solutions: Data encryption, secure channels, robust cryptography
- □ Ensure integrity
  Solutions: Data & code signing, secure boot, robust cryptography
- □ Process only necessary data
  Solutions: Data minimization
- □ Ensure availability
  Solutions: Resilience mechanisms, robust authentication
- □ Minimize negative impact to other products
  Solutions: Device authentication, network monitoring & control, code signing, input validation...
- □ Minimize attack surface
  Solutions: Ports, services, code & external interfaces minimization
- □ Reduce impact of incidents
  Solutions: Mitigation mechanisms
- □ Logging & monitoring
  Solutions: Persistent log storage, timestamping, externalization of the logs
- □ Deletion
  Solutions: Secure and atomic deletion, user notification

At The Embedded Kit we’ve integrated those security mechanisms into our software solutions to help you **save time**. Consult our website to know more.

The Embedded Kit