SECURiMENT

No More Cyber Threats

EU Cyber Resilience Act (CRA) Compliance Services

REGULATION (EU) 2024/2847

REGULATORY SCOPE
Applies to all Products with Digital Elements (PDEs) placed on the EU market.

Dec 10, 2024	Sept 11, 2026	Dec 11, 2027
Entry into Force	Mandatory Reporting (24h / 72h)	Full CE Marking Compliance

1. APPLICABILITY & RISK TIERS

- **Portfolio Audit:** Identify affected hardware, embedded software, and connected services.
- **CRA Classification:** Categorize products across Default, Class I, and Class II (Annex III/IV) risk tiers.
- **Obligation Mapping:** Assess legal duties for manufacturers, importers, and integrators.
- **Framework Alignment:** Harmonize CRA with NIS2, DORA, EU AI Act, IEC 62443, ETSI EN 303 645, and ISO 27001.

2. GAP AUDIT & PROCESS MATURITY

- **Maturity Assessment:** Evaluate organizational maturity, SDLC phase gates, and security governance.
- **Technical Controls Review:** Audit SBOM capabilities, patch management, and OTA update security.
- **Core Deliverables:** Executive Dashboard, Gap Report, Risk Matrix, and Action Roadmap.

3. SECURITY-BY-DESIGN & SBOM

- **Secure Product Lifecycle:** Implement threat modeling, secure architecture, and DevSecOps controls.
- **Automated SBOM Engine:** Establish open-source vulnerability management and supply-chain tracking.
- **Vulnerability Response:** Build Coordinated Vulnerability Disclosure (CVD) and 24h CSIRT / ENISA reporting.

4. TESTING & CAPABILITY BUILDING

- **Security Validation:** Penetration testing, firmware analysis, container, and IoT security reviews.
- **CE Technical File:** Prepare the EU Declaration of Conformity and technical documentation packages.
- **In-House Competence:** Train internal engineering teams in product risk assessment and vulnerability triage.

END-TO-END CRA COMPLIANCE JOURNEY

01	02	03	04	05
DISCOVERY	**ROADMAP**	**IMPLEMENTATION**	**VALIDATION**	**OPERATIONS**
PDE inventory & risk-tier scoping	Action plan, resource & risk strategy	Security-by-Design, SDLC & SBOM controls	Testing & CE technical-file readiness	Monitoring & 24h / 72h reporting

TARGET INDUSTRIES & PRODUCTS

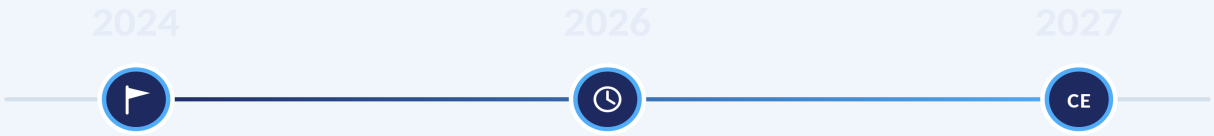
- Software Vendors
- Connected Devices
- Critical Infrastructure
- SaaS Providers
- IoT Manufacturers
- Industrial Technology

WHY SECURIMENT?

- Independent cybersecurity specialists with 10+ years of hands-on SOC experience.
- Practical engineering execution — not just static compliance reports.
- End-to-end guidance from initial scoping to complete CE-marking readiness.

CRA COMPLIANCE ROADMAP

Key enforcement milestones — Regulation (EU) 2024/2847



10 Dec 2024	11 Sep 2026	11 Dec 2027
Entry into Force	**Mandatory Reporting**	**Full CE Marking**
CRA formally enters into force	24 h / 72 h incident reporting to ENISA	Conformity assessment & CE marking required

TURN CRA COMPLIANCE INTO YOUR COMPETITIVE EDGE

Schedule your CRA Readiness Assessment with Securiment today and secure your European market access.

www.securiment.com | info@securiment.com | +31 62 026 92 32