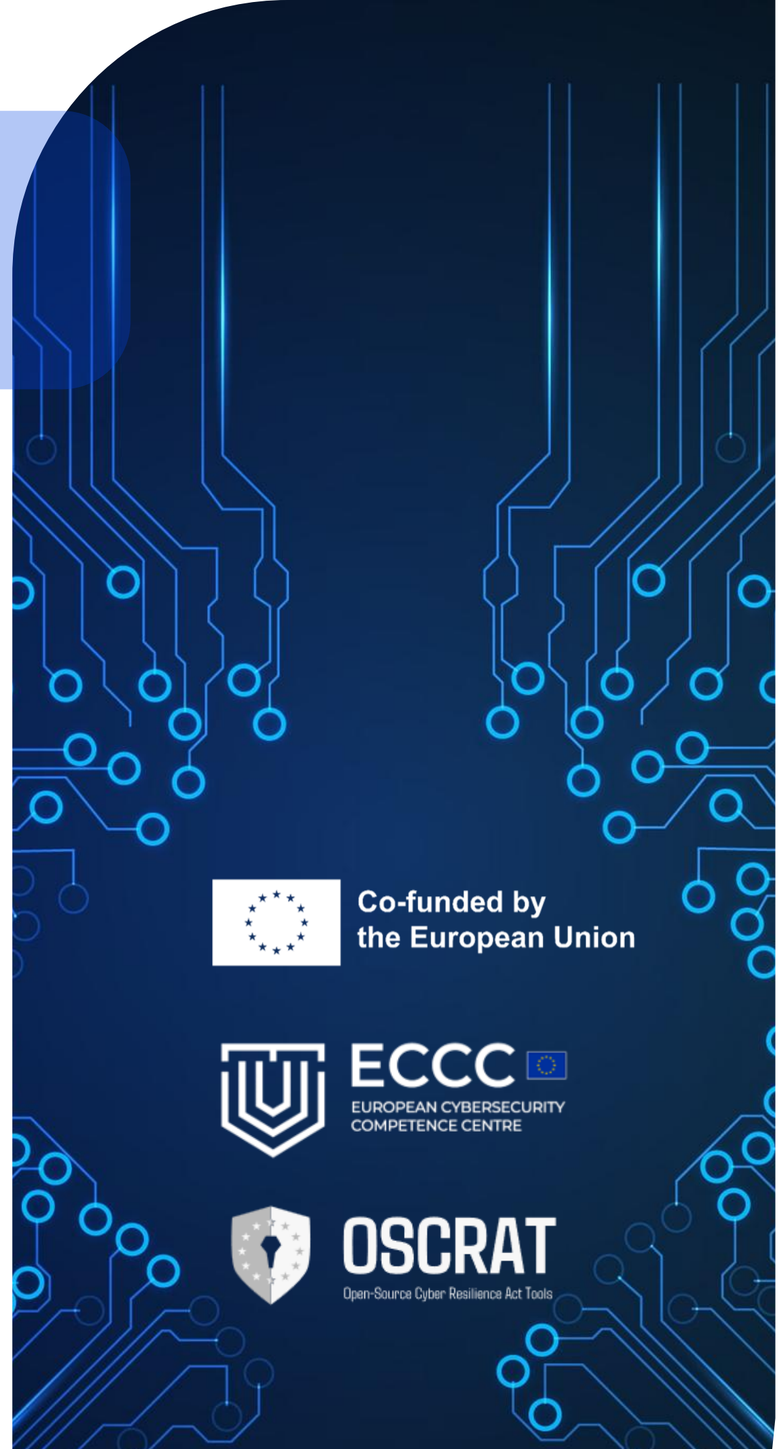
Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Regulation (EU) 2024/2847

Creating a CRA Compliance Roadmap

A practical, structured approach to achieving CRA readiness

December 2025



Digital Innovation Hub
Trakia

What a CRA Roadmap Must Achieve

A roadmap must:

- Close the gaps identified in analysis
- Establish required processes and documentation
- Prepare for CE marking
- Integrate CRA duties into the product lifecycle
- Demonstrate continuous compliance

Core Pillars of a CRA Roadmap

A complete roadmap addresses:

1. **Processes** — SDL, vulnerability handling, risk assessments
2. **Policies** — CVD, incident reporting, update management
3. **Technical controls** — secure-by-default, logging, testing evidence
4. **Documentation** — technical file (Annex VII)
5. **People & roles** — responsibilities, training
6. **Monitoring & maintenance** — ongoing compliance

Roadmap Structure Overview

A clear roadmap is built in **three** phases:

Phase 1: Foundation (0–3 months)

Policies, roles, gap closure planning, documentation structure

Phase 2: Integration (3–6 months)

Process implementation, SBOM, secure development controls

Phase 3: Demonstration (6–12 months)

Evidence collection, internal audits, CE marking readiness

Phase 1: Foundation (0–3 months)

Focus on:

- Formal roles & responsibilities
- Core policies (risk assessment, SDL, CVD, updates, vulnerability handling)
- Initial CRA gap closure actions
- Define support period determination rules
- Establish documentation framework (Annex VII structure)

Phase 2: Integration (3–6 months)

Focus on:

- Embedding secure development practices
- Implementing vulnerability handling workflow
- Automating SBOM generation
- Security testing processes & evidence
- Update management workflow
- Initial monitoring/logging integration

Phase 3: Demonstration (6–12 months)

Focus on:

- Building the full technical documentation package
- Evidence collection & traceability
- Internal audit / conformity check
- Selecting and engaging with notified bodies (if needed)
- Preparing CE marking declarations
- Finalizing incident reporting workflows

Key Roles Needed for Roadmap Execution

- Product Security Lead
- Compliance Manager / CRA Lead
- Engineering Lead (SDL owner)
- Incident Response/Vulnerability Manager
- Documentation Manager

Example Roadmap (High-Level)

Month 1–3:

✓ Policies

✓ Risk assessment method

✓ Documentation structure

✓ CVD setup

✓ Support period definition

Month 3–6:

✓ SDL rollout

✓ SBOM automation

✓ Vulnerability workflow

✓ Update pipeline

Month 6–12:

✓ Technical file (Annex VII)

✓ Internal audits

✓ Final documentation

✓ CE marking package

CRA Compliance Roadmap

PHASE 1 – 📋 FOUNDATION (0–3 months)

- Define roles & responsibilities
- Establish core CRA policies (SDL, CVD, Vulnerability Handling, Updates)
- Design Technical Documentation structure (Annex VII)
- Begin SBOM tooling & evaluation
- Start cybersecurity risk assessment approach

PHASE 2 – 🛠️ INTEGRATION (3–6 months)

- Implement SDL practices in development workflows
- Deploy SBOM automation pipeline
- Implement vulnerability triage workflow & evidence tracking
- Secure OTA updates (signing & verification)
- Strengthen logging & monitoring on device/platform
- Start collecting evidence for the Technical file

PHASE 3 – 🧭 DEMONSTRATION (6–12 months)

- Build full Annex VII Technical File
- Collect evidence: tests, logs, SBOMs, risk assessments
- Internal conformity assessment
- Prepare CE marking package
- Finalize Article 14 reporting workflow (24h/72h)
- Pre-market readiness validation

Final Takeaways

To build an effective CRA roadmap:

- Start with reality (gap analysis)
- Build the foundation (policies, roles, structure)
- Integrate processes into daily work
- Collect evidence continuously
- Treat CRA as an ongoing lifecycle, not a project

THANK YOU

FOR YOUR ATTENTION

December 2025

Sashka Boncheva

m: +359 888 800 222

s.boncheva@dihtrakia.org

CYBER 4 ALL STAR

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION BULGARIA

Digital Innovation Hub Trakia