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 Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Obligations under the Cyber Resilience Act

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

The CRA Compliance Cycle

Prepare	• Prepare documentation
Ensure	• Ensure conformity
Monitor	• Monitor vulnerabilities
Notify	• Notify authorities
Message	• Message: CRA compliance is a continuous process — not a one-time event.

Declaration of Conformity: Purpose

- What is the DoC? A formal statement by the manufacturer declaring that the product meets CRA requirements.
- Legal basis: Article 28 & Annex V.
- Must be signed by authorized representative.
- Must accompany every product on the EU market.

Contents of the Declaration

- Product identification (model, type, batch)
- Manufacturer details
- Reference to applicable EU legislation
- Standards or specifications used
- Name and signature of the responsible person

CE Marking and Conformity

- CE marking = visible proof of compliance.
- Only applied after the conformity assessment is complete.
- Two routes:
- **Module A** – self-assessment (for standard products)
- **Module B** – third-party assessment (for critical products)
- Connection between CE marking, DoC, and technical documentation.

Technical Documentation: What It Is

- Purpose: to prove that the product meets essential cybersecurity requirements (Annex I).
- Must be ready before the product is placed on the market.
- Stored for **10 years**.
- Includes evidence for both design and lifecycle security.

What Technical Documentation Must Contain

- General product description
- Risk analysis and mitigation measures
- Security architecture
- Software Bill of Materials (SBOM)
- Vulnerability management plan
- Testing results and conformity evidence

Vulnerability Management Obligations

- Based on Article 11.
- Every manufacturer must have a **vulnerability handling process**.
- Must identify, assess, and fix vulnerabilities promptly.
- Applies to both known and newly discovered weaknesses.
- Emphasize link with **coordinated vulnerability disclosure (CVD)**.

Reporting and Notification Duties

- Two main types:
1. **Incident notification** – for exploited vulnerabilities.
2. **Vulnerability disclosure** – when a weakness is found.

- Timeframe: **within 24 hours** after awareness (for active exploitation).
- Notify **ENISA** and **national competent authority**.
- Include details on affected products, risks, and mitigation measures.

Coordination with ENISA

- ENISA acts as the EU hub for vulnerability reporting.
- Manufacturers must:
- Register a contact point for vulnerability handling.
- Use secure communication channels.
- Follow ENISA’s CVD templates.
- Example: how reports flow from manufacturer → ENISA → other member states.

Post-Market Surveillance

- Manufacturers must monitor security even after release.
- Collect information from distributors, importers, and users.
- Maintain update and patch policy during the support period.
- Must withdraw or recall products if they pose significant risk.

Record-Keeping and Retention

- All documents (DoC, technical file, communication logs) kept for at least **10 years**.
- Must be available to authorities upon request.
- Applies to manufacturers, importers, and distributors.

Practical Example: Vulnerability Handling

Detect → Fix → Notify → Improve

Common Challenges

- Companies often face issues with:
- Missing or incomplete technical documentation.
- Slow patch deployment.
- Poor internal communication between teams.
- Lack of clear responsibility for notifications.
- Solutions: automation, standardized templates, CVD policy.

Key Takeaways

- Compliance under CRA means **continuous responsibility**.
- Declaration + Documentation + Vulnerability Handling + Notification = trust.
- Transparency and speed build credibility and legal protection.
- Final message: *“Security by design also means accountability by default.”*

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
m.mitev@dihtrakia.org