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.

Core Topics of 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

Scope of the Regulation

- Applies to **products with digital elements** placed on the EU market.
- Covers both hardware and software components.
- Annex I:
  - **Part 1**: Essential cybersecurity requirements (secure by design, vulnerability handling, updates).
  - **Part 2**: Requirements for specific risk management and reporting.
  - Categories:
  - **Important products -** (Class I & II)
  - **Critical products** – subject to stricter controls.

Vulnerability Management

- Manufacturers must establish processes for:
  - Vulnerability monitoring, identification, and handling.
  - Security updates (free of charge for users).
  - Timely patch deployment.
- Obligation to notify **ENISA** and designated CSIRTs about actively exploited vulnerabilities and serious incidents.

Obligations of Manufacturers

- Conduct a **risk assessment** for digital products.
- Prepare and maintain **technical documentation** for at least **10 years**.
- Establish a **Quality Management System**.
- Provide **instructions and security information** for users.
- Place the **CE marking** on compliant products.
- Draw up an **EU Declaration of Conformity** (Annex V template).
- Notify about vulnerabilities via the single EU reporting platform.
- **SMEs**: proportionate obligations, but still required to notify vulnerabilities.

Obligations of Importers and Distributors

- Ensure only compliant products are placed on the EU market.
- Verify CE marking and Declaration of Conformity.
- Maintain storage/transport conditions that do not compromise security.
- **Article 21**: obligation to act if they believe a product poses a cyber risk.

Conformity Assessment
Two main paths

- **Self-assessment** (for non-critical products).
- **Third-party assessment** (for critical products) via **notified bodies**.

Accreditation framework for Conformity Assessment

- European Commission
- ENISA
- National notifying authorities
- Notified bodies
- National cybersecurity certification authorities (NCCAs)
- Market surveillance authorities
- Testing laboratories (for innovative products)

Enforcement and Sanctions

- **Administrative fines** (Article 58): corrective measures for non-compliance.
- **Sanctions (Article 64)**: Up to **€15 million** or **2.5% of total worldwide annual turnover**.
- Proportional approach depending on severity and recurrence.

Delegated and Implementing Acts

- Commission empowered to adopt:
  - **Delegated acts** to identify which critical products require mandatory EU certification.
  - **Implementing acts** to define common specifications where harmonised standards are delayed.
- Delegation period: 5 years from December 2024, renewable

Standards

- CRA relies on the **New Legislative Framework** principles and **Regulation (EU) 1025/2012** on standardisation.
- **Harmonised European standards** provide presumption of conformity.
- Where no standard exists → Commission may adopt **common specifications**.
- Relevant standards include ISO 9001, ISO/IEC 27001, ISO 17025, ISO/IEC 15408, ISO/IEC 18045, ETSI EN 303 645, and EUCC (European Common Criteria scheme).

Thank you!

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