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.

CYBER RESILIENCE ACT

Introduction

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

About the Lecturer

•Lead Auditor for Management Systems (information security, services, quality, and more).

•Chairman of the **Institute for Artificial Intelligence**.

•Deputy Manager of the **Bulgarian Union of Standardizers**.

•Active participant in numerous European and national cybersecurity projects.

•Assistant Professor at **UniBIT**:

- Cybersecurity Standards
- Cybersecurity Management
- Cryptography
- Zero Trust Architectures

Seminar Structure

- **From September 2025 to April 2026**.
- First **four sessions** (Sep–Dec 2025): *theoretical foundations*.
- Next **four workshops** (Jan–Apr 2026): *hands-on training and case studies with OCSRAT*.
- Goal: build both **strategic understanding** and **practical skills** to apply the Cyber Resilience Act.

4 SESSIONS

- Session 1 (September 8, 2025)
- Session 2 (October 13, 2025)
- Session 3 (November 10, 2025)
- Session 4 (December 8, 2025)

Context and Introduction to the Cyber Resilience Act

- Historical and political background: why CRA was created.
- CRA structure, stakeholders, compliance timelines.
- Core topics: products, economic operators, conformity assessment, delegated acts, standards.
- Relation to other EU regulations: DORA, NIS2, GDPR.
- Current state of CRA implementation.

Scope and Obligations under CRA

- Which products are covered: IoT, software, embedded hardware.
- Roles & responsibilities: manufacturers, importers, distributors.
- EUCS (Cloud Services Scheme) – regulating cloud providers.
- Case study: CRA impact on IoT manufacturers.
- Obligations: declarations of conformity, vulnerability reporting.
- Sanctions and consequences of non-compliance.

Technical Requirements and Standards

- Key standards: ISO 9001, ISO/IEC 27001, ISO 17025, ISO/IEC 15408, ISO/IEC 18045, ENISA guidance.
- Horizontal vs vertical standards in CRA.
- Initiatives: CYBERSTAND, STAN4CR.
- Case studies: healthcare IoT, energy systems.
- Vulnerability management and reporting.
- Risk management integration.
- EUCC & Common Criteria: methodology, Security Targets, certification approach.

Preparing Organizations for CRA Implementation

- Steps: gap analysis, policies, compliance roadmap.
- CRA evolution: implementing acts, new schemes.
- Analysis of evaluation reports (TrustBoost example).
- Industry best practices.
- CRA & OCSRAT: project synergies.
- Open discussion: challenges in implementing CRA.

Upcoming Workshops (Jan–Apr 2026)

- Four **practical workshops** linked to OCSRAT.
- Hands-on exercises and implementation guidance.
- Topics:
  - Risk assessment with CRA requirements.
  - Documentation and security target drafting.
  - Vulnerability management in practice.
  - Cross-sector case studies (finance, healthcare, critical infrastructure).

Today’s Agenda

- Historical & Political Context
- Presentation of the CRA
- Core Topics of the Regulation
- CRA & Other EU Regulations
- Implementation Status

Q&A

- **How to ask:** Post questions in the **chat window**
- **When answered**
  - End of the current session
  - Beginning of the next session
- **Special cases**
  - Some questions may require deeper research
  - Answers may be provided later via **email**
- **Future opportunities**
  - Dedicated discussion slots in next sessions
  - Interactive Q&A during the workshops

Thank you!

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