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.

International and Regional Evaluation Standards

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Introduction

- The technical requirements under the CRA call for a structured framework for **security and conformity assessment**.
- This framework builds on internationally recognized standards that ensure **traceability**, **repeatability**, and **confidence** in testing and certification results.
- Objective: to ensure that products, services, and organizations demonstrate measurable security aligned with common evaluation criteria.

ISO/IEC 27001 – ISMS standard

- Defines requirements for information security management systems (ISMS).
- It provides the organizational framework ensuring that laboratories and certification bodies manage risks systematically.
- Role in evaluation:
- Ensures objectivity and transparency in processes.
- Guarantees data and result security during testing and certification.

ISO/IEC 27001 in the CRA context

ISO/IEC 27001 is often required for evaluation and certification bodies working with high-assurance or critical products.

ISO/IEC 17025 – Competence of Laboratories

Specifies general requirements for the competence, impartiality, and consistent operation of laboratories.

Applies to:

- Testing laboratories performing measurements or product tests.
- Calibration laboratories ensuring measurement accuracy and traceability.

ISO/IEC 17025 - Key principles

- Validated testing and calibration methods.
- Traceability of results and measurements.
- Management of measurement uncertainty and impartial evaluation.

ISO/IEC 17025 in CRA context

Laboratories testing IoT devices under ETSI EN 303 645 must be accredited to ISO/IEC 17025 to ensure trust in their testing results.

ISO/IEC 17065 – Certification Bodies

Defines requirements for the competence, consistency, and impartiality of bodies certifying products, processes, services and people.

Focus:

- Independence between evaluator, client, and manufacturer.
- Clear certification process – application, evaluation, review, decision, surveillance.
- Confidentiality and conflict-of-interest management.

ISO/IEC 17065 in CRA context

- Certification bodies (notified bodies) apply ISO/IEC 17065 to ensure that the assessment is objective and recognized at EU level.
- Together with ISO/IEC 15408 (Common Criteria), it provides a structured certification and evaluation process.

ETSI EN 303 645 – Security Standard for IoT Devices

The first European cybersecurity standard for consumer IoT devices, developed by ETSI TC CYBER.

Covers:

- Core requirements such as *unique identifiers, software updates, data protection, and encryption*.
- Testing criteria for laboratories performing IoT device evaluations.

ETSI EN 303 645

- The standard is often used for developing **Protection Profiles** under the EUCC scheme.
- Supported by ENISA, it forms the **technical foundation** for conformity assessment of connected products within CRA's scope.

ENISA Recommendations

- Application of **ISO/IEC 15408 and ISO/IEC 17025** in certification schemes.
- Development of **sectoral protection profiles** (IoT, 5G, Cloud, ICS).
- Guidance for **laboratories and certification bodies** on vulnerability assessment and lifecycle management of devices.

ENISA Recommendations

- Transparency in certification processes.
- Mechanisms for vulnerability monitoring and reporting.
- Alignment with the EUCC and CRA frameworks.

Conclusion

- The interrelation of these standards creates an **integrated trust framework**.
- ISO/IEC 17025 and 17065 define *who evaluates*, ISO/IEC 27001 defines *how security is managed*, and ETSI EN 303 645 with ENISA define *what is tested*.
- Together, they form the basis for the unified European approach to cybersecurity evaluation under the CRA.

Thank you!

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