HSbooster.eu
Horizon Standardisation Booster

Standards for compliance with regulations of the Cybersecurity Act

Dr. Elzbieta Andrukiewicz
CEN/CLC/JTC13 Standardization expert,
National Institute of Telecommunications, Poland

The HSbooster.eu has received funding from the European Union's Horizon Europe Framework Programme (HORIZON) - under grant agreement no 101058391.

Few words about the Author

- Deeply involved in international and European standardization in the field of cybersecurity
  - Editor of ISO/IEC 27005 „Guidance on managing information security risks”
  - Co-editor of ISO/IEC 15408-1 „Evaluation criteria for IT security — Part 1: Introduction and general model (CC part 1)
  - Co-editor of EN 17640 „Fixed-time cybersecurity evaluation methodology”
  - Editor of European standard (draft) „Guidelines on Sectoral Cybersecurity Assessment”
- Involved in designing first European cybersecurity certification scheme based on Common Criteria (at ENISA’s adhoc group) and European cybersecurity certification scheme for 5G Network Equipment (under development)
- Manager of IT Security Evaluation Facility (ITSEF) at National Institute of Telecommunications, accredited testing laboratory performing IT security evaluations for ICT products

Cybersecurity Act (CSA): first pillar - conformity assessment AND standardization

- European cybersecurity certification schemes are to be designed and then implemented considering the following:
  - Proven quality regarding technical competence and specific characteristics of conformity assessment, such as transparency, independence and impartiality of conformity assessment bodies confirmed by the accreditation
  - AND
  - Standardization rules, i.e. widely recognized and approved reference standards, developed and maintained according to appropriate EU regulations

Cybersecurity Act: second pillar – security AND assurance

- ICT security stands for the target of keeping the confidentiality, availability and integrity of information assets
- Assurance is the confidence that the supplier implements ICT security so that the risk of successful attacks is reduced to an acceptable level
- *Assurance level:* means a **basis for confidence** that an ICT product, ICT service or ICT process meets the **security requirements** of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been **evaluated** but as such does not measure the security of the ICT product, ICT service or ICT process
- Assurance levels defined in the CSA: basic, substantial, and high.

Example: definition of assurance level „substantial”

A European cybersecurity certificate at assurance level ‘**substantial**’ shall provide **assurance** that the ICT products, ICT services and ICT processes for which that certificate is issued:

meet the corresponding **security requirements**, including security functionalities

← **security requirements** to be defined

evaluated at a level intended to minimize the **known cybersecurity risks**, and **the risk of incidents and cyberattacks** carried out by actors with **limited skills and resources**.

← **assurance & security requirements** to be defined and aligned

risk of intended use to be assessed

attack potential to be assessed

The evaluation activities to be undertaken shall include **at least** the following:

- a review to demonstrate the absence of known vulnerabilities
- testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities

scope, depth and rigor of evaluation

Funded by the European Union

CEN/CLC/JTC13 response to CSA: EN 17640:2022 „Fixed-time cybersecurity evaluation methodology” [FIT-CEM]

- Standard based on several national so-called „lightweight” cybersecurity certification schemes (CSPN – France, LINCE –Spain, BSZ – Germany, to name some of them)
- It is a security requirements’ agnostic standard dedicated to cybersecurity evaluation only; in fact, it can complement any standard describing cybersecurity requirements for ICT products
- It covers all assurance levels defined in the CSA
- Amendments to [FIT-CEM]:
  - Currently under development: Composite evaluation
  - In the queue: Evaluation of the life-cycle of the product (ICT process)

HSbooster.eu
Horizon Standardisation Booster

[FIT-CEM] –scope of evaluation

Evaluation tasks	Short description what is needed by [FIT-CEM]
Completeness check	TOE (required number of samples), testing environment, complete set of documentation
Review of security functionalities	Clear presentation of security functionality in documentation (FIT ST)
FIT Security Target Evaluation	Simplified version of ASE/APE assurance class in Common Criteria
Development documentation	Simplified version of ADV assurance class in Common Criteria
Evaluation of TOE Installation	Simplified version of AGD assurance class in Common Criteria; SUG (Secure Use Guide) concept
Conformance Testing	Simplified version of ATE_IND assurance family in Common Criteria
Vulnerability review	Research in publicly available datebases of known vulnerabilities; (optional) developer's documentation of vulnerability scans
Vulnerability testing	Devising tests based on the test strategy; Developer's documentation on risk management related to publicly known vulnerabilities
Penetration testing	Superset of Vulnerability testing evaluation task based on the Flaw hypotesis concept.
Basic crypto analysis	Tests of correctness of cryptoalgorithm's implementations
Extended crypto analysis	Advanced analysis of source code (optional)

Funded by
the European Union

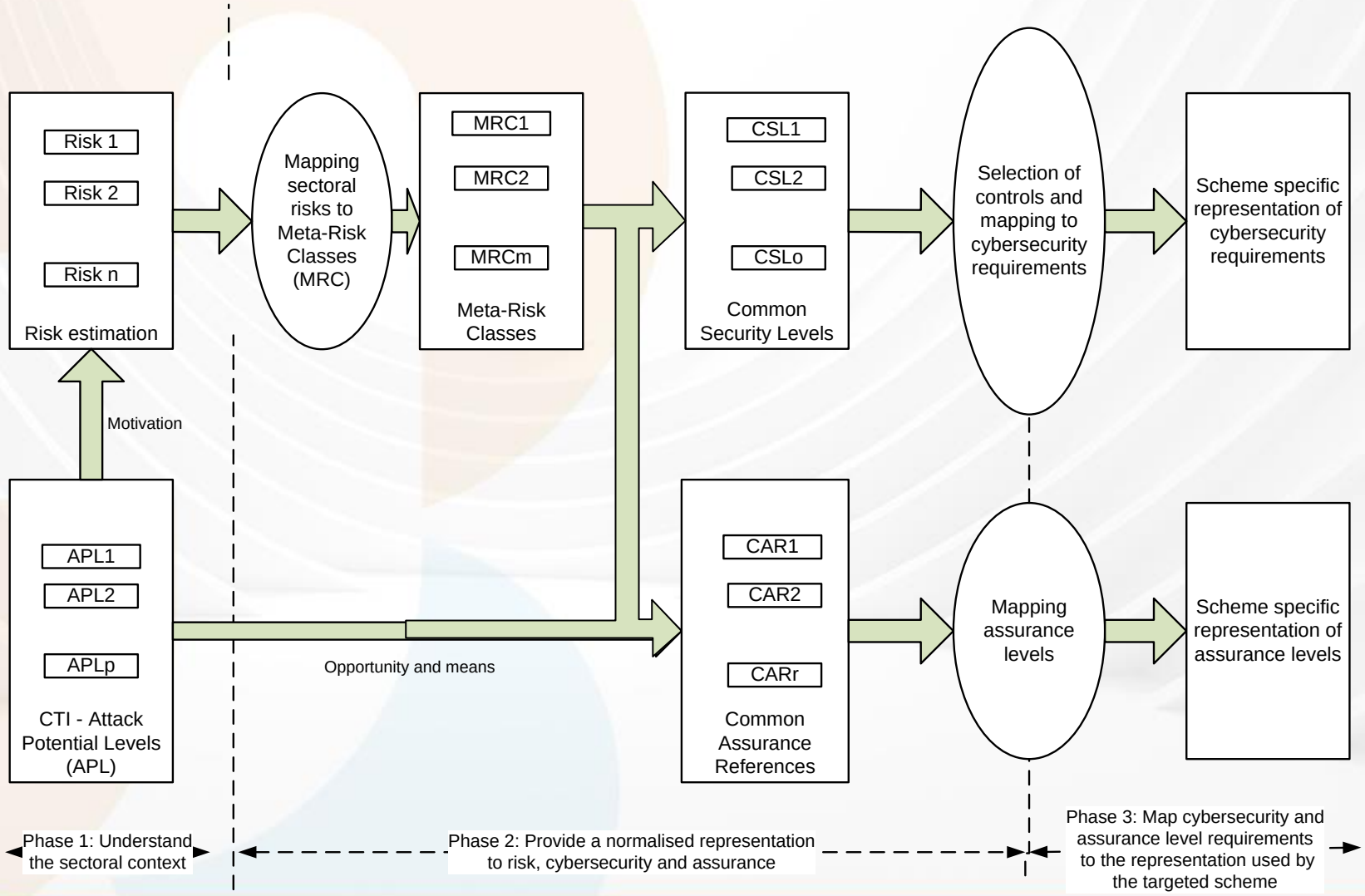
[FIT-CEM] – content of an evaluation

- All evaluation tasks consist of:
  - **Aim** (what is the objective of a given evaluation task)
  - **Evaluation method** (what the evaluator shall do)
  - **Evaluator's competence** (what kind of knowledge, skills and experience is required from the individual who is performing the evaluation task)
  - **Evaluator's work unit(s)** (contains a detailed description of the evaluation task)

New project – JTC13053 „Guidelines on Sectoral Cybersecurity Assessment”

- Designed to support the sectoral cybersecurity certification schemes’ development
- Based on the ENISA’s document published in September 2022 https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment
- The content of the draft:
  - Clarification of the concept of security and assurance: attack potential analysis for cybersecurity and assurance requirements
  - Analyzing the sectoral ICT systems that consist of ICT services and ICT systems, both operated by (possibly) several sectoral stakeholders
  - Risk-driven analysis of the landscape
  - Risk treatment dependent on the ICT product robustness to the defined attack potential
  - Evaluation’s scope, rigour and depth related to the defined attack potential
  - Normalized levels of risks, security and assurance
- The project is waiting for a formal announcement of the opening of public consultation by the CEN/CLC Management Committee

Guidelines concept presentation



Funded by the European Union

THANKS!

GET IN TOUCH WITH US!

www.hsbooster.eu @HSboosterEU /company/hsbooster-eu HSboosterEU

HSbooster.eu
Horizon Standardisation Booster