UNIVERSITY OF TARTU
Institute of Computer Science

RIIGI INFOSÜSTEEMI AMET

CYBERNETICA

# Framework for Security Level Evaluation F4SLE

Mari Seeba

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

MUNI Masaryk University

CyberSecurityHub CZ

What is my security situation?

Technical failure

E-ITS

GDPR

Assets?

ISO27001

NIS2

Supply chain failure

How to stay competitive?

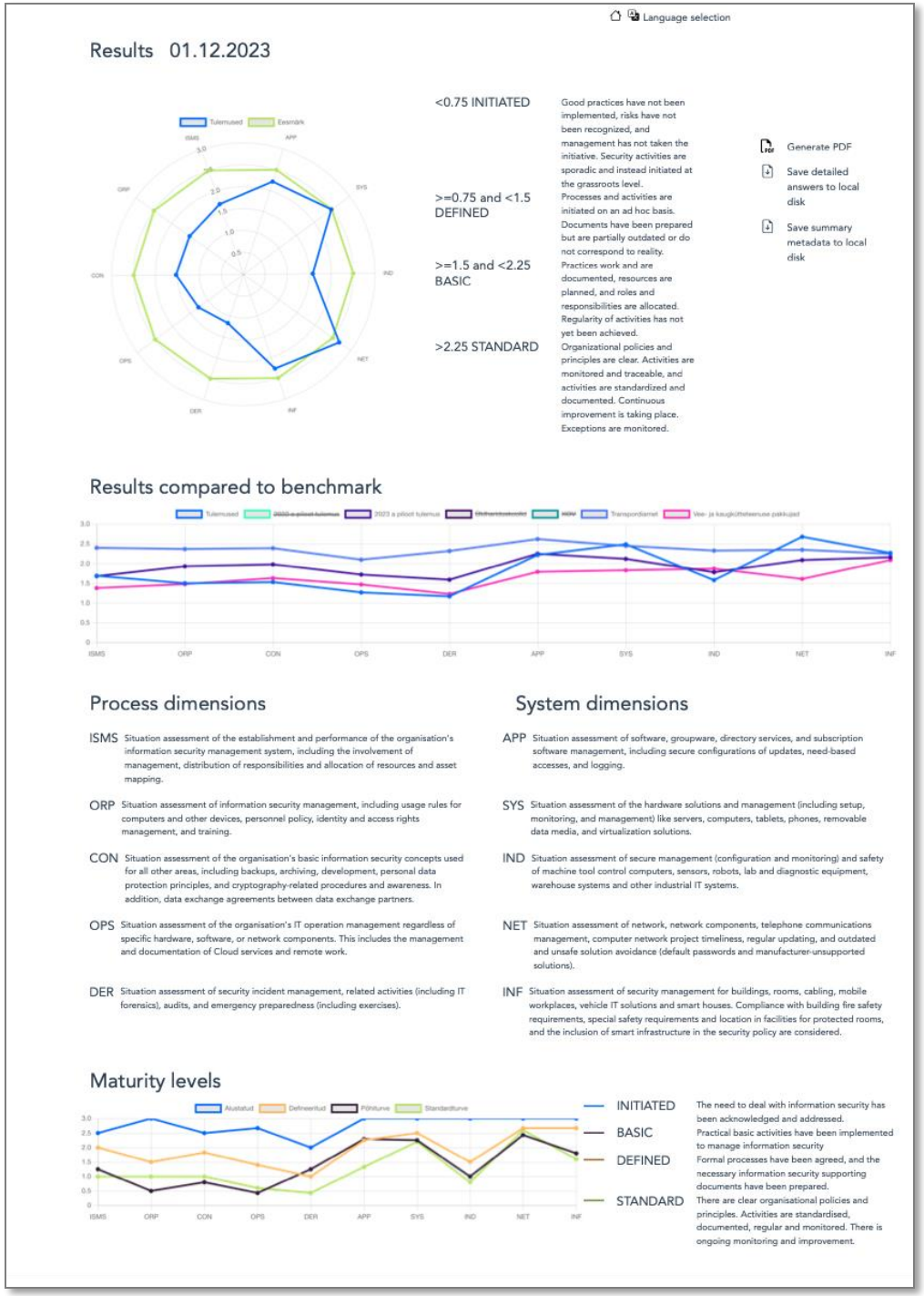
Reporting of security status to NSCS

Cyberattacks

# F4SLE *Framework for Security Level Evaluation*

- Self-assessment
- Immediate result
- All-hazard approach
  ISO27001, NIS2, E-ITS, ENISA Threat landscape report
- Comparision benchmarks

https://mass.cloud.ut.ee/massui/




# Organization and CISO

- Security evaluation result in 10 security dimensions
- Risk level values
- Comparing with expectation level (green line)

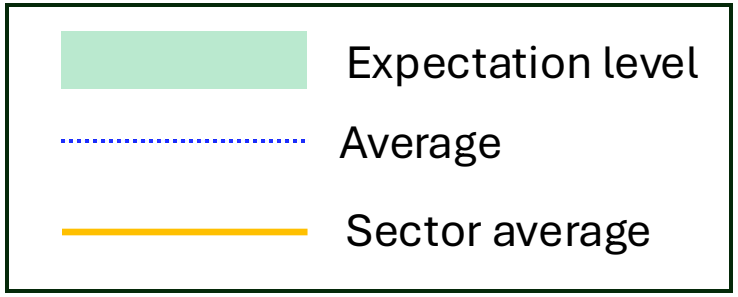
- Bechmarking with others

- Meanings of Security dimensions

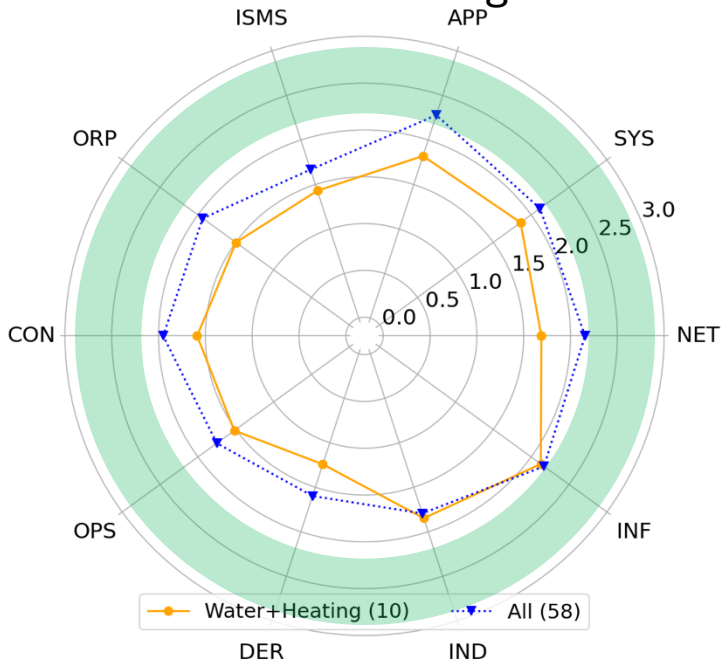
- Details of maturity, documentation, practical measures, continuity

https://mass.cloud.ut.ee/massui/

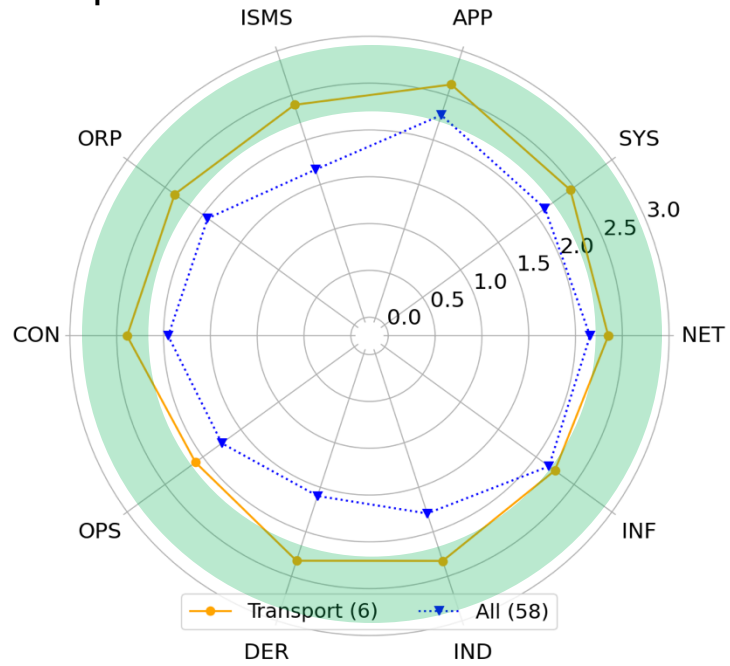
# Comparison of Sectors



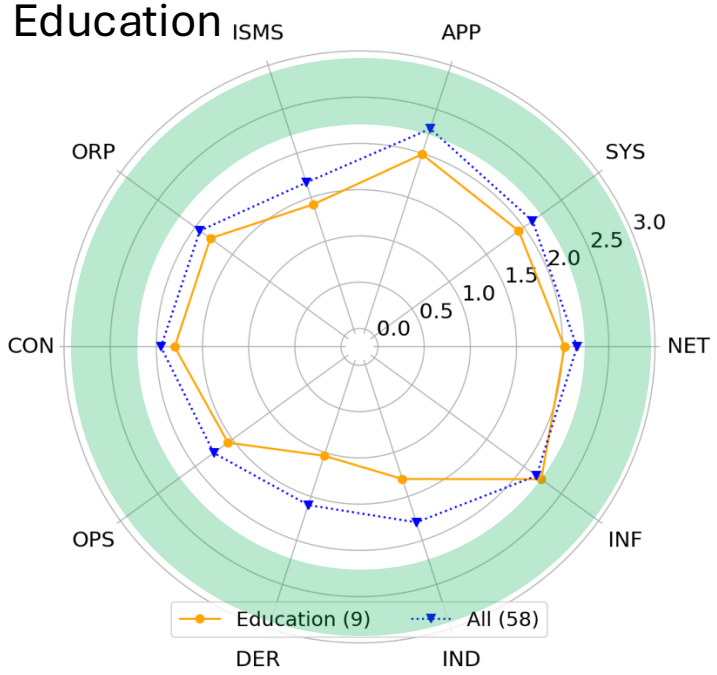

## Water and distance heating



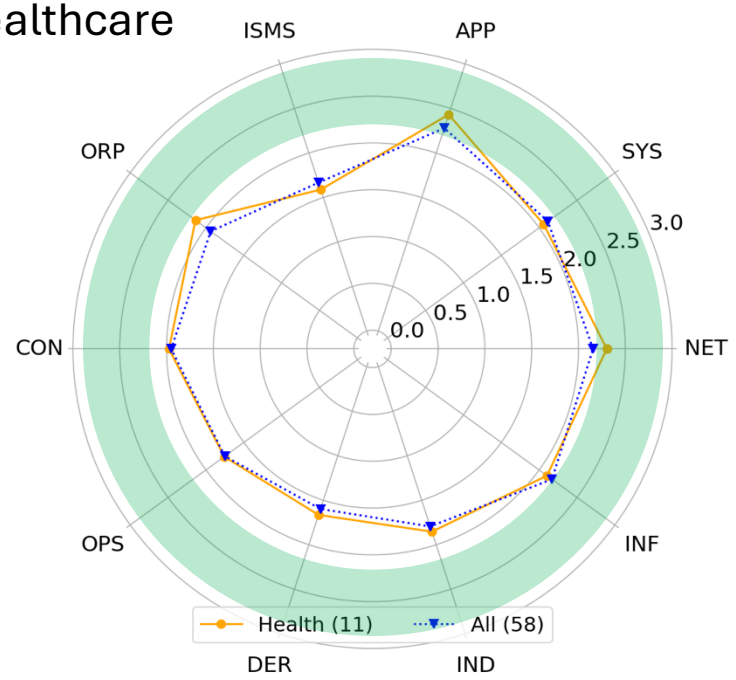

## Transport



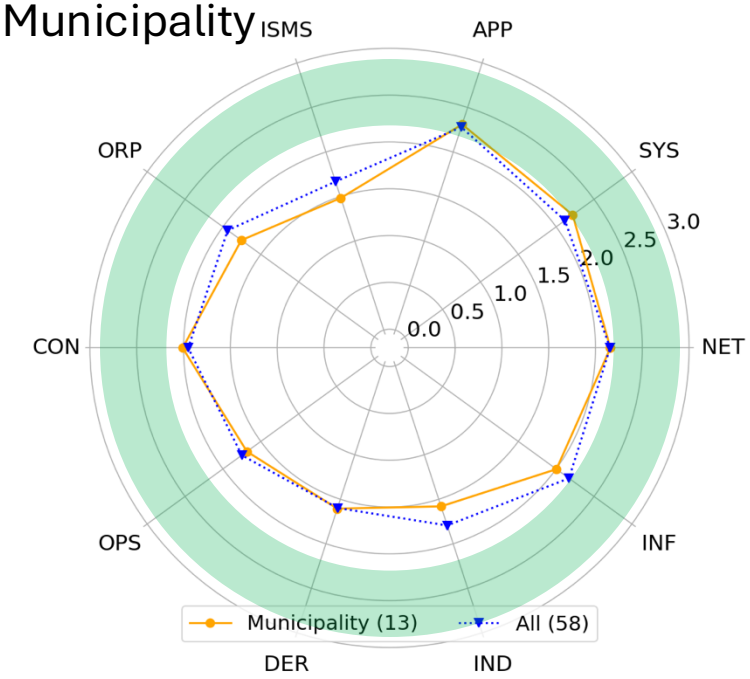

## Education



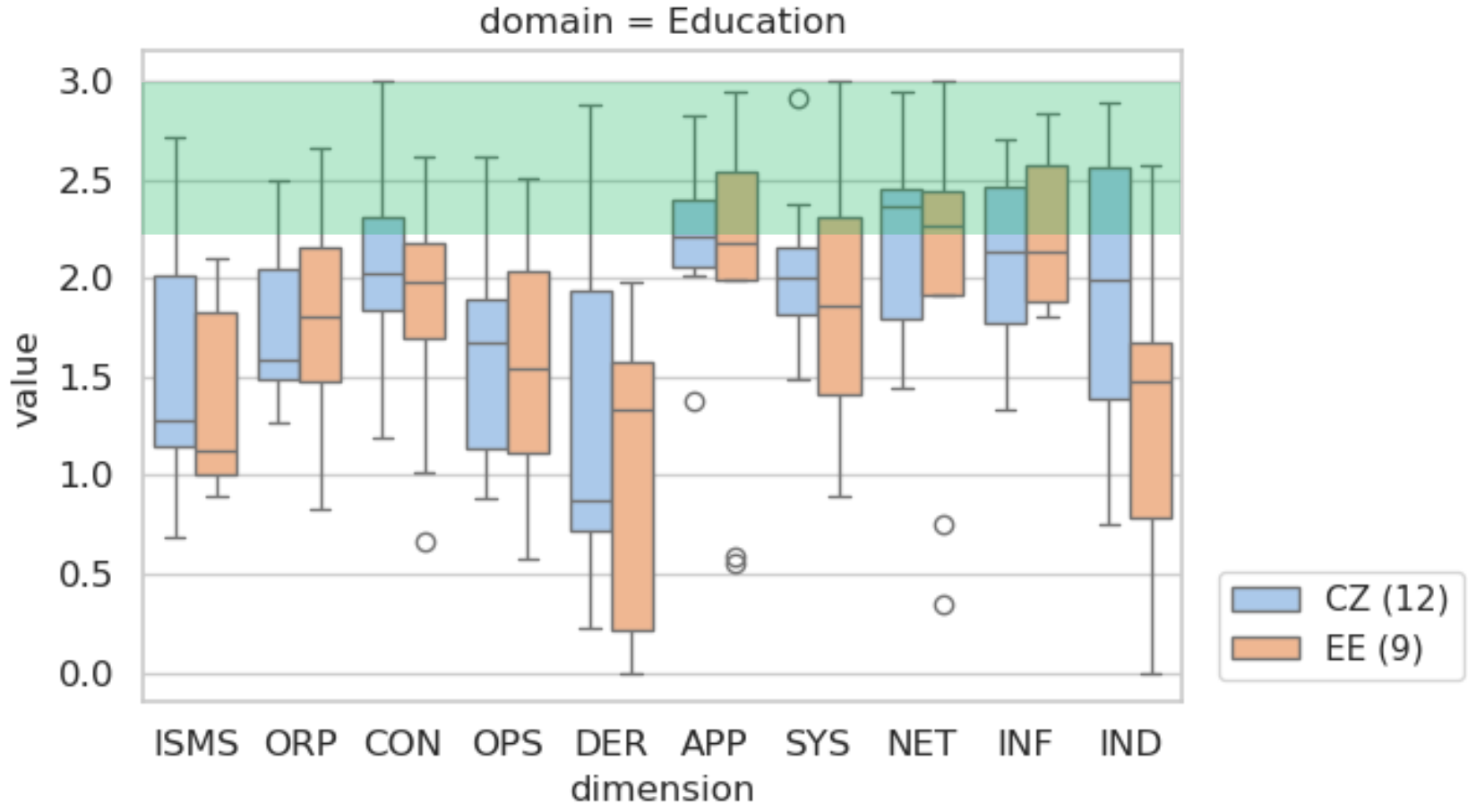

## Healthcare




## Municipality

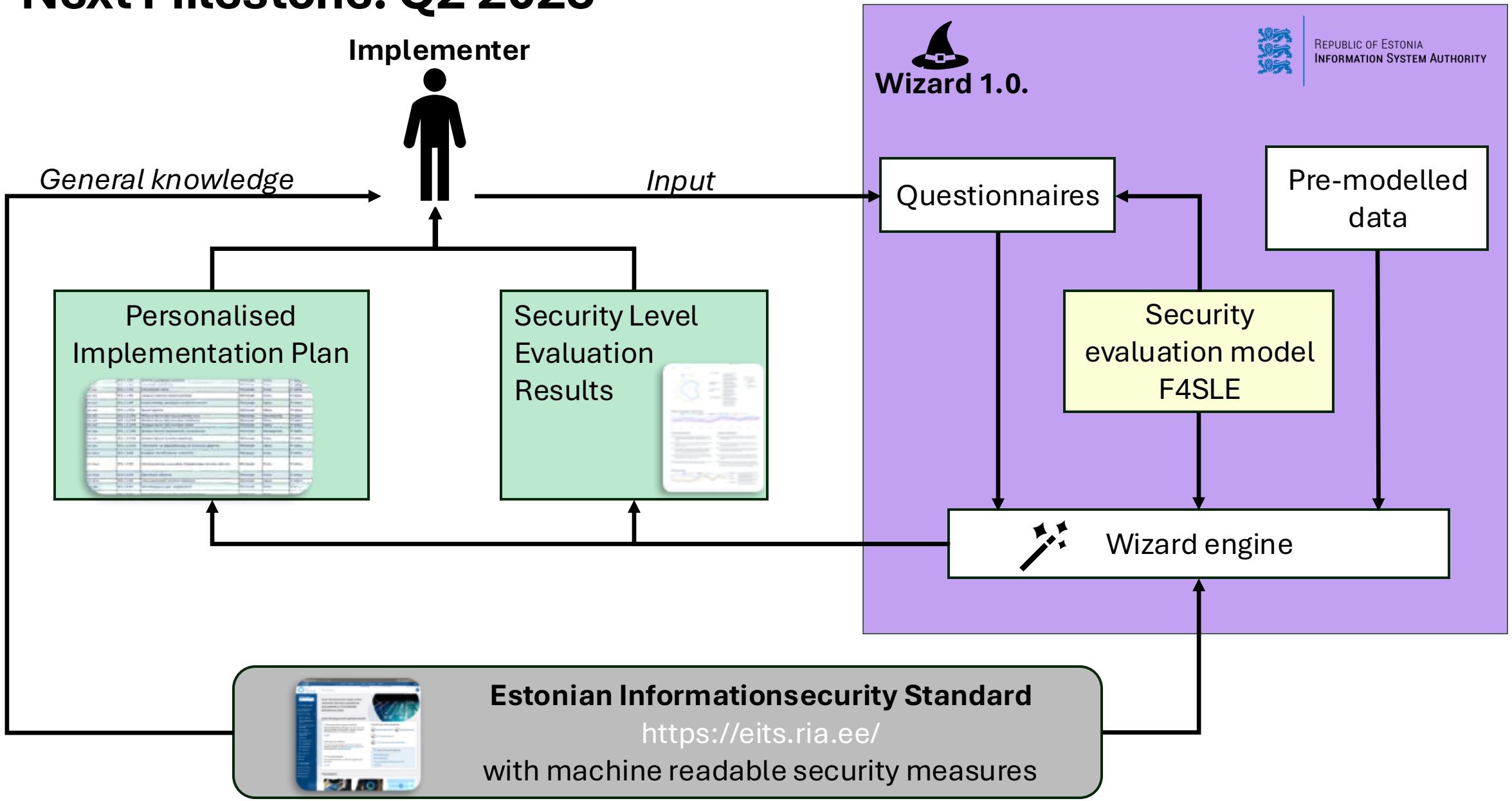


# Estonia vs Czech - Education




https://mass.cloud.ut.ee/massui/

# Next Milestone: Q2 2025



# How to get best value from security level evaluation?

You can not measure security
but
you can evaluate what you have done to be secure.

Mari.Seeba@ut.ee

https://mass.cloud.ut.ee/massui/

# Security Level Evaluation with F4SLE [1]

Mari Seeba*,+, Tarmo Oja*, ◊, Maria Pibilota Murumaa*, Václav Stupka•,△
*University of Tartu, Estonia, +Information System Authority of Estonia, ◊ Cybernetica AS Estonia, • Masaryk University, Czechia, △ CyberSecurity Hub, z.u., Czechia

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

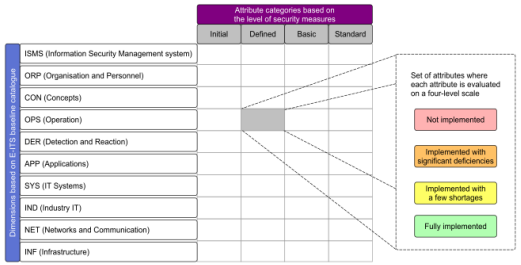
What are the avenues for interpreting the data collected using the security level evaluation instrument F4SLE?

## F4SLE- Framework for Security Level Evaluation

- An instrument for evaluating organization security maturity level
- Based on E-ITS, ISO27002 and ENISA Threat Landscape Report
- Attributes are updated yearly based on method for updating the security evaluation instrument MUSE principles
- Does not impose any prerequisites on organizations for self-assessment

## MASS - Measurement Application for Self-assessing Security

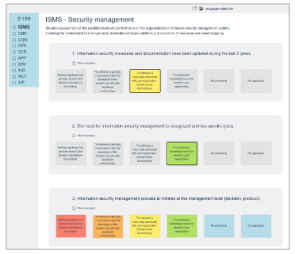
- Presents the F4SLE to respondents
- Provides immediate results on the organization's security status after responding to all security attributes
- Collects averaged results for cross-organizational analysis




F4SLE – Framework for Security Level Evaluation [F4SLE, MUSE]

Collected metadata with options (*in Italic number of respondents*)

| Data type | Options |
|---|---|
| Domain | Healthcare(1); Municipality (11); Government office (4); Education (9); ICT (2); Other private sector; Non-profit (1); Other (specify) |
| Workplaces | 1...30(3); 31...100(9); 101...300(7); 301...1000(5); 1001... (4) |
| Hours | Around 30 minutes; Around 1 hour; 2 hours; 2-4 hours; 4-8 hours; More than 1 working day |
| Role | IT manager(8); Information security manager /specialist(11); Management(4); Network/system administrator; Administrative assistant/lawyer/DPO (1); Other (specify)(4) |
| Country | Czech Republic(2); Estonia(28); Other |
| Implemented standards | ISO/IEC 27001; ISKE (Estonian); CIS Controls; KUTS (Estonian); NIST CSF; E-ITS (Estonian); BSI IT Grundshutz (German); Act on cyber security, no.181/2014 Coll. (Czech) |




MASS user interface example

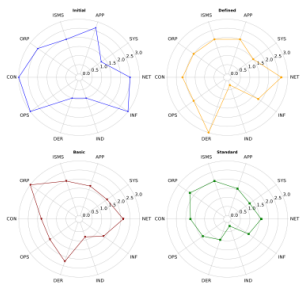
**Organizational level:**

- Maturity levels by security dimensions
- An aggregated result, which can be interpreted as a risk level
- Benchmarks

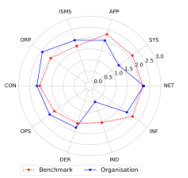
**Results**

**Cross organizations** (interpretation principles):

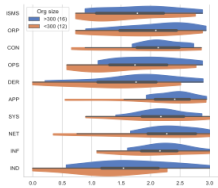
- Difference between organizations (data dispersion)
- Comparison based on individual data points (e.g., mean, median - compare results over time, provide benchmarks)



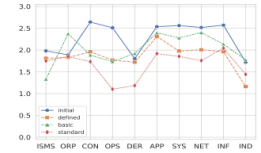

Security evaluation result example of one organization, breakdown by maturity levels



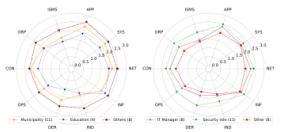

Security evaluation result example of one organization, comparison with the benchmark (cross-organizational average result)




Overall evaluation distribution by dimensions and organization size. The median has been marked with a white dot and 50% by the black thick line.




Overall evaluation results by maturity levels




Overall evaluation result breakdown by (a) organization domain and (b) respondent role.

## Limitations

- Selected, voluntary organizations – no random sample
- Dominating domain – municipalities
- Full statistical data analyzis is yet to be implemented
- Based on a self-assessment questionnaire
- Respondent's role and awareness could affect the results within an organization
- Comparing results between Estonia and other countries may be affected by the Estonian Information Security Standard bias

## Future Work

- Increase the number of respondents in Estonia and South Moravia (Czechia)
- Repeat the data collection at least twice (yearly dynamics)
- Update the F4SLE attributes using MUSE principles
- Compare responses from the same organization but given by different roles
- Conduct more data analytics and link it to other databases (causal relationships, threat landscape, security, and specific regulations)
- Assess the possibility of using the results to develop security-related strategies
- Engage national decision-makers
- Collecting the same data from Estonia and the South Moravia simultaneously

UNIVERSITY OF TARTU
Republic of Estonia Information System Authority
MUNI Masaryk University
CYBERNETICA
CYBER SECURITY HUB

Co-funded by the European Union
Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

# F4SLE *(Framework for Security Level Evaluation)* principles

- ISO27001, E-ITS, NIS2 and relevant threats (regular updates)
- Regularly but once-only (reusable data for interested parties)
- Immediate result to data provider
- Low entrance barrier
- Sectoral benchmarks (comparability)
- Comparability over time (dynamics)
- Security and privacy of data collection tool MASS
- Translation ET, EN, ES

https://mass.cloud.ut.ee/massui/

## Interested Parties by NIS2

- Org. management & CISO
- Supervisory
- External consultant
- Partner (supply chain)
- State level policy-maker


- M. Seeba, R. Matulevičius, I. Toom, Development of the Information Security Management System Standard for Public Sector Organisations in Estonia, 2021, doi:10.52825/bis.v1i.43.
- M. Seeba, S. Mäses, R. Matulevičius, Method for Evaluating Information Security Level in Organisations, 2022, doi:10.1007/978-3-031-05760-1_39
- M. Seeba, T. Oja, M. P. Murumaa, V. Stupka, Security Level Evaluation with F4SLE, 2023. doi:10.1145/3600160.3605045
- M. Seeba, A. amefon Obot Affia, S. Mäses, R. Matulevičius, Create your own MUSE: A method for updating security level evaluation instruments, 2024 doi:10.1016/j.csi.2023.103776.