Co-funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Security Level Evaluation with F4SLE

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

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.

Why?

- II and ISMS
- NIS2, GDPR, national regulations
- Reduce uncertainty
- Security level of the organisation(s)
- Collecting data centrally
  - Previous studies
  - Longitudinal study

Motivation

- To motivate the team and stakeholders with preliminary results and engage more organisations into the research

Research Question:

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

Survey approach

- Target group
  - organisations whose services depend on information technology, and which are obliged to implement information security measures due to regulations
- Instrumentation
  - For security evaluation: F4SLE
  - For data collection: MASS
  - Self-assessment
- Processing
  - Immediate organisation-based results and domain benchmarks
  - General calculations
- Metadata set

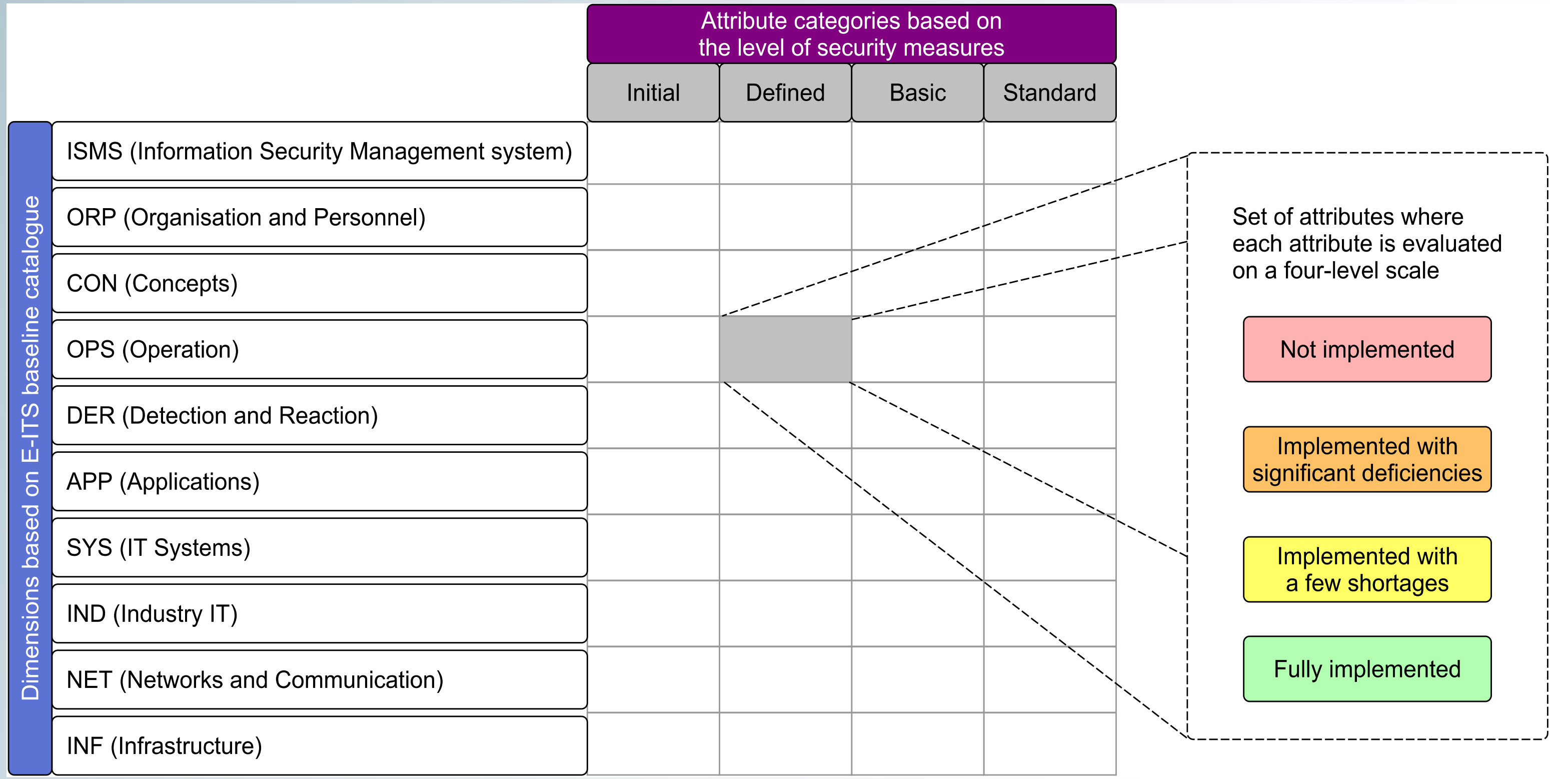
Survey approach

- Target group
  - organizations whose services de are obliged to implement informa
- Instrumentation
  - For security evaluation: F4SLE
  - For data collection: MASS
  - Self-assessment
- Processing
  - Immidiate organisatsion based r
  - General calculations
- Metadata set

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; KüTS (Estonian); NIST CSF; E-ITS (Estonian); BSI IT Grundshutz (German); Act on cyber security, no.181/2014 Coll. (Czech)

F4SLE - Framework for Security Level Evaluation

- An instrument for evaluating organisation security maturity level
- Based on E-ITS, ISO27002 and ENISA Threat Landscape Report
- Yearly updated attributes using MUSE principles [MUSE]
- Does not impose any prerequisites on organisations for self-assessment



Dimensions based on E-ITS baseline catalogue	Initial	Defined	Basic	Standard
ISMS (Information Security Management system)				
ORP (Organisation and Personnel)				
CON (Concepts)				
OPS (Operation)				
DER (Detection and Reaction)				
APP (Applications)				
SYS (IT Systems)				
IND (Industry IT)				
NET (Networks and Communication)				
INF (Infrastructure)				

Attribute categories based on the level of security measures

Set of attributes where each attribute is evaluated on a four-level scale

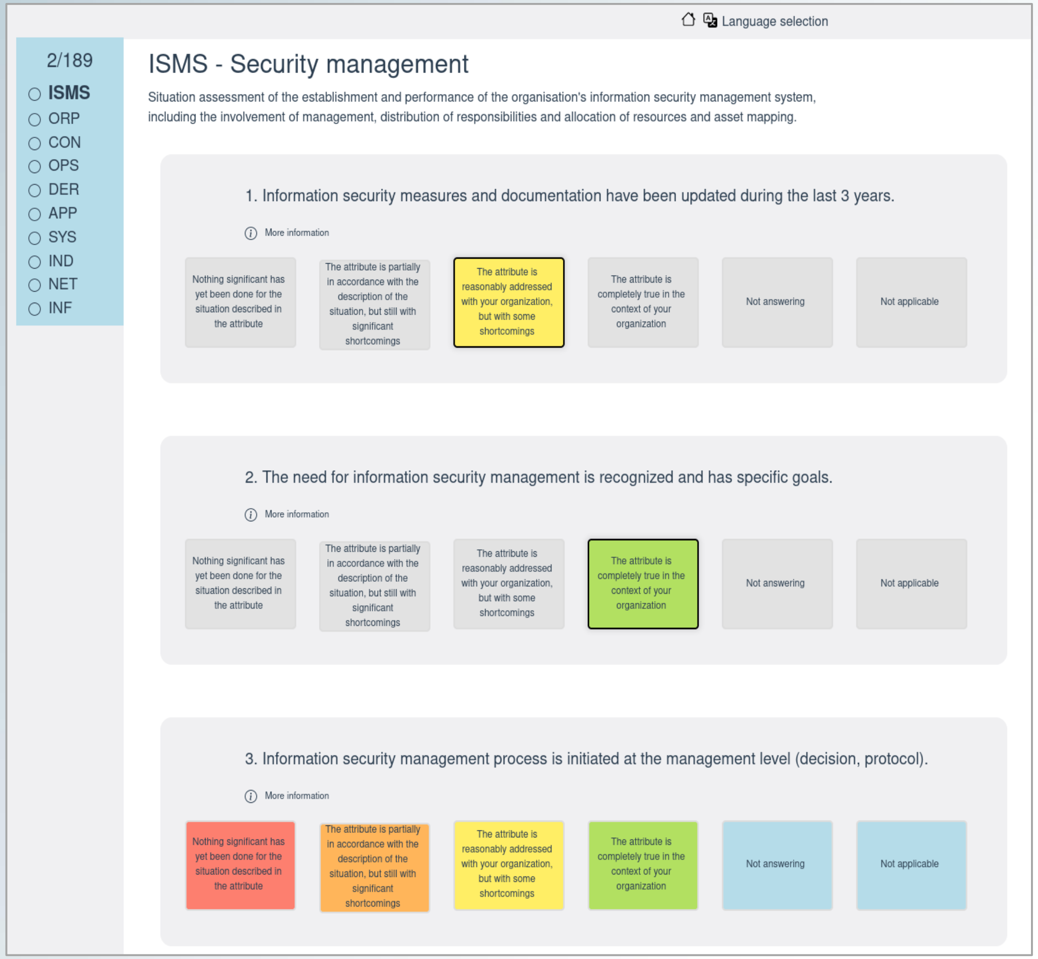
- Not implemented
- Implemented with significant deficiencies
- Implemented with a few shortages
- Fully implemented

MASS - Measurement Application for Self-assessing Security

- Presents the F4SLE to respondents
- Provides immediate results (benchmarks)
- Collects averaged results for cross-organizational analysis
- Privacy principle
  - raw data does not leave from the respondent

Test environment: https://mass.cloud.ut.ee/test-massui/

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



ISMS - Security management

Situation assessment of the establishment and performance of the organisation's information security management system, including the involvement of management, distribution of responsibilities and allocation of resources and asset mapping.

1. Information security measures and documentation have been updated during the last 3 years.

More information

Nothing significant has yet been done for the situation described in the attribute | The attribute is partially in accordance with the description of the situation, but still with significant shortcomings | [✓ The attribute is reasonably addressed with your organization, but with some shortcomings] | The attribute is completely true in the context of your organization | Not answering | Not applicable

2. The need for information security management is recognized and has specific goals.

More information

Nothing significant has yet been done for the situation described in the attribute | The attribute is partially in accordance with the description of the situation, but still with significant shortcomings | The attribute is reasonably addressed with your organization, but with some shortcomings | [✓ The attribute is completely true in the context of your organization] | Not answering | Not applicable

3. Information security management process is initiated at the management level (decision, protocol).

More information

Nothing significant has yet been done for the situation described in the attribute | The attribute is partially in accordance with the description of the situation, but still with significant shortcomings | The attribute is reasonably addressed with your organization, but with some shortcomings | The attribute is completely true in the context of your organization | Not answering | Not applicable

MASS user interface example

Results

Organizational level:

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

Cross organizations:

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

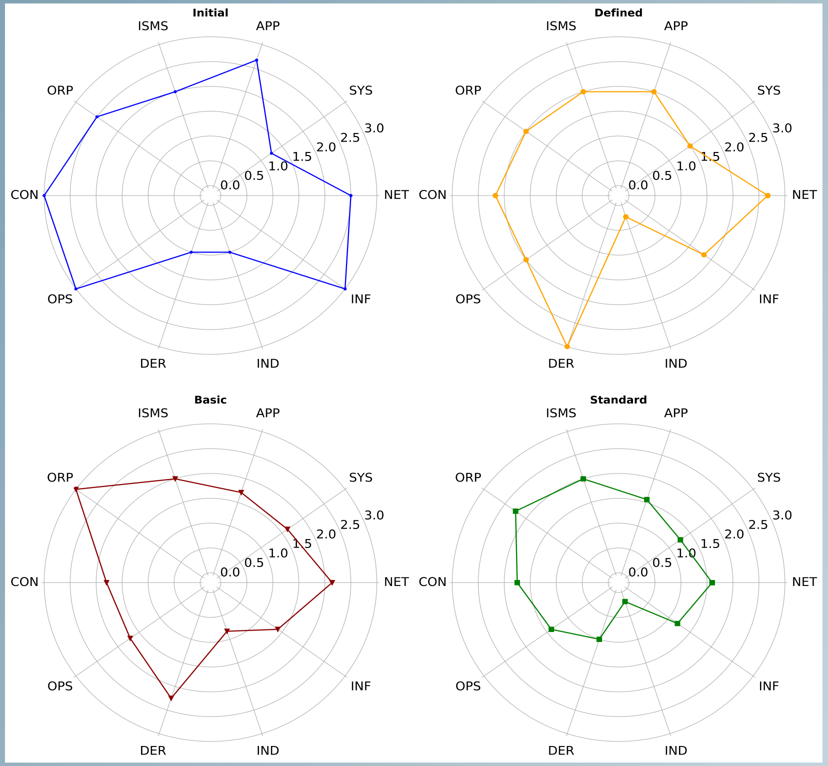
Results

Organizational level:

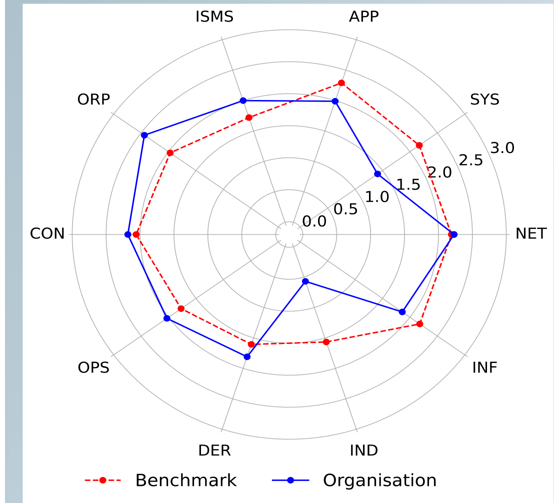
- Maturity levels by security dimensions
- An aggregated result, which can be interpreted as a risk level
- Benchmarks

Cross organizations:

- 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)

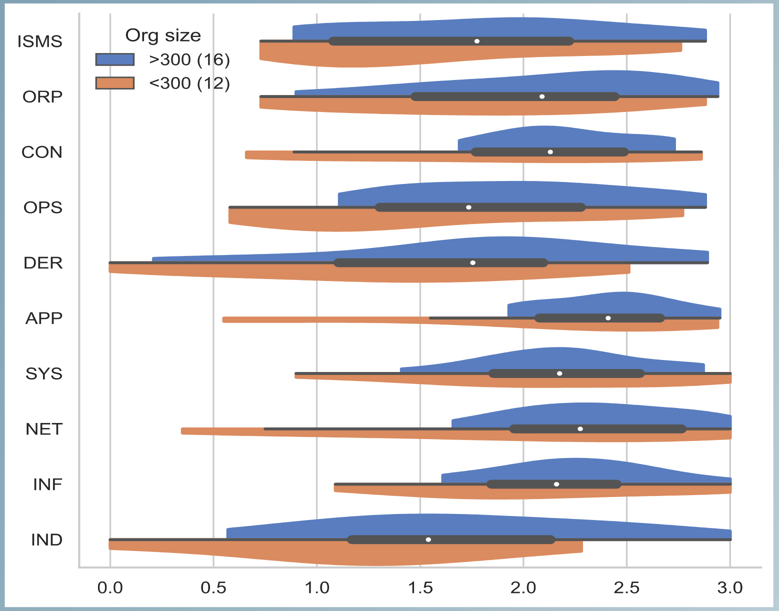
Results

Organizational level:

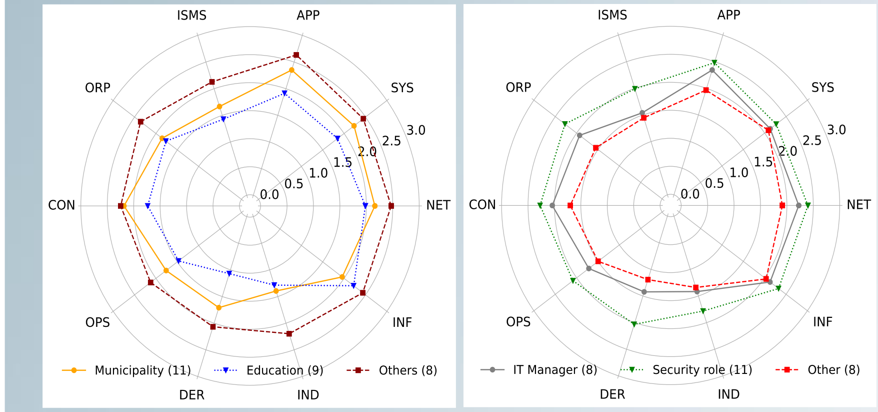
- Maturity levels by security dimensions
- An aggregated result, which can be interpreted as a risk level
- Benchmarks

Cross organizations:

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



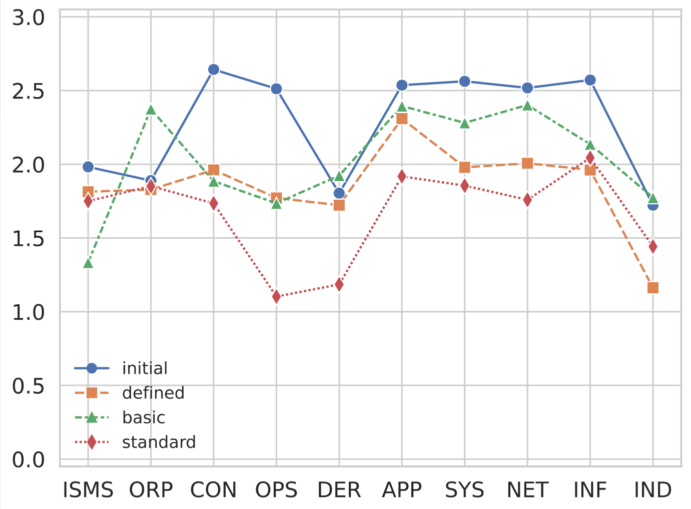
Overall evaluation distribution by dimensions and organization size. The median has been marked with a white dot and 50% by the black thick line.



(a) By domain

(b) By role

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



Overall evaluation results by maturity levels

Limitations

- Selected, voluntary organisations – no random sample
- Dominating domain – municipalities
- Full statistical data analysis is yet to be implemented
- Based on a self-assessment questionnaire
- Respondent's role and awareness could affect the results within an organisation
- 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 organisation 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

Conclusion

- Directions to interpret the the results in
  - organisation level and
  - for cross-organisational level

- Option to present results and engage more respondents
- Continue with data collection

References - Building Blocks

F4SLE- *Framework for Security level Evaluation*

- framework and its principles
  - *Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. In: RCIS 2022. Lecture Notes in Business Information Processing, vol 446. Springer, Cham. https://doi.org/10.1007/978-3-031-05760-1_39*
- Content versions *http://dx.doi.org/10.23673/re-298; http://dx.doi.org/10.23673/re-372*

MUSE - *Method for Updating Security Level Evaluation Instruments*

- How to update the F4SLE: process, principles, inputs
  - Mari Seeba, Abasi-amefon Obot Affia, Sten Mäses, Raimundas Matulevičius. 2023. Create your own MUSE: A method for updating security level evaluation instruments, Computer Standards & Interfaces, Volume 87, 2024, https://doi.org/10.1016/j.csi.2023.103776

MASS- Measurement Application for Self-assessing Security

- tool to present F4SLE https://mass.cloud.ut.ee/test-massui/; https://mass.cloud.ut.ee/massui/
- *Master thesis of Maria Pibilota Murumaa, (2023) Designing a Security Sensitive Self-assessment Framework,* https://chess-eu.cs.ut.ee/2023/08/25/designing-a-security-sensitive-self-assessment-framework/
- immidiate results to respondents and sending the aggregated results to central server

Thank you!

- Discussions on ongoing reserch are welcome!
- Organisations to join are welcome!

- Contact:
  - mari.seeba@ut.ee

CHESS
Cyber-security Excellence Hub in
Estonia and South Moravia

Republic of Estonia
Information System Authority

University of Tartu
1632

Cyber Security Hub

Cybernetica

MUNI Masaryk University

Co-funded by the European Union