CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Co-funded by
the European Union

Organisations Security Level Evaluation

Ongoing pilot project in Estonia and South Moravia (Czech Republic)

Mari Seeba

Leading Cybersecurity expert, Information System Authority of Estonia, NCSC-EE

PhD student, University of Tartu, Estonia

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.

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 - Framework for Security Level Evaluation
        - <200 statements in 10 dimensions to evaluate
    - For data collection: MASS tool
    - Self-assessment
- Processing
    - Immediate organisation-based results and domain benchmarks
    - General calculations
- Metadata set

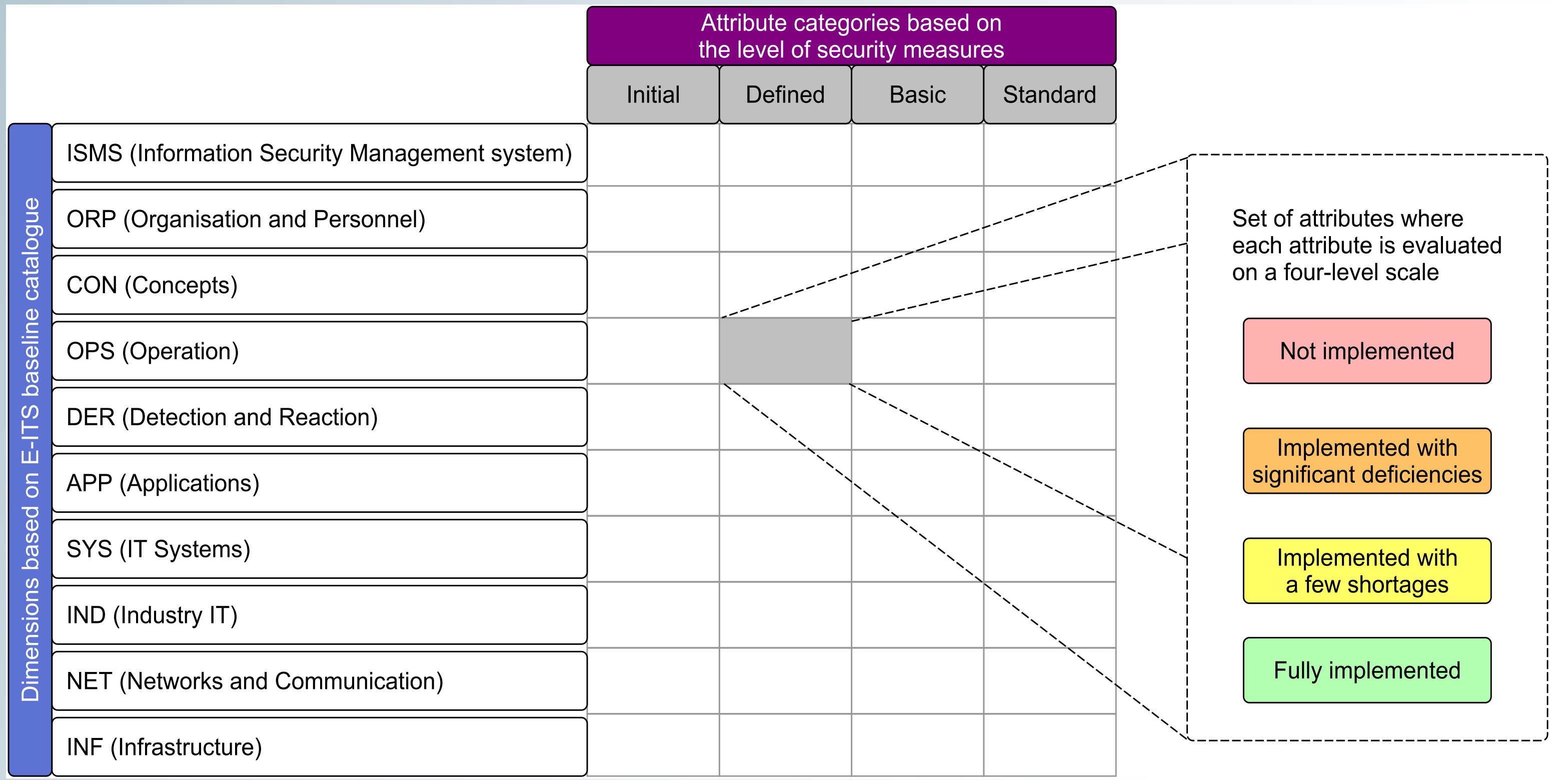
Survey approach

- 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; Municipality; Government office; Education; ICT; Other private sector; Non-profit ; Other (specify)
Workplaces	1...30; 31...100; 101...300; 301...1000; 1001...
Hours	Around 30 minutes; Around 1 hour; 2 hours; 2-4 hours; 4-8 hours; More than 1 working day
Role	IT manager; Information security manager /specialist; Management; Network/system administrator; Administrative assistant/lawyer/DPO; Other (specify)
Country	Estonia; Czech Republic; 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 (BSI IT Grundshutz Kompendium),
  - ISO27002
  - ENISA Threat Landscape Report (suggestion part)
- Yearly updated attributes using MUSE principles
- Does not impose any prerequisites



	Attribute categories based on the level of security measures			
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)				

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

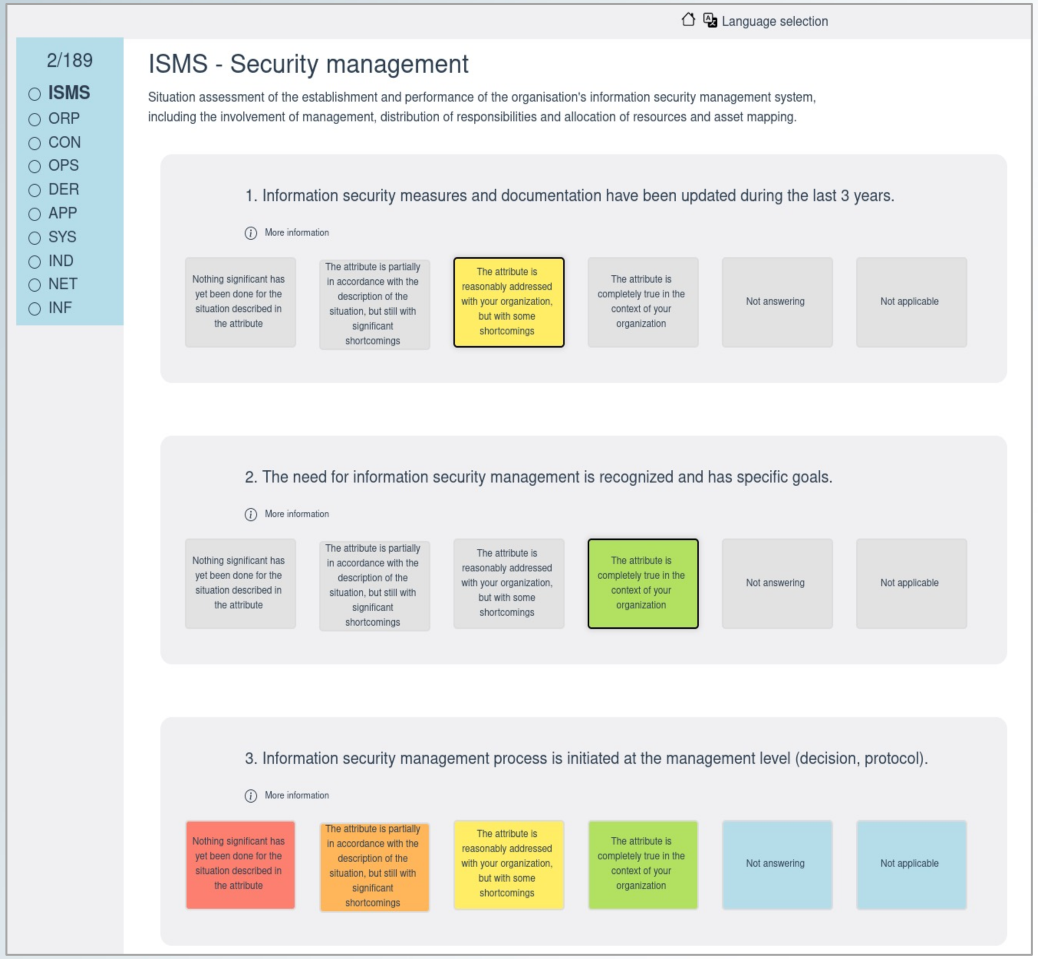
- Not implemented
- Implemented with significant deficiencies
- Implemented with a few shortages
- Fully implemented

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/



2/189

○ ISMS
○ ORP
○ CON
○ OPS
○ DER
○ APP
○ SYS
○ IND
○ NET
○ INF

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.

- 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.

- 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).

- 🟥 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

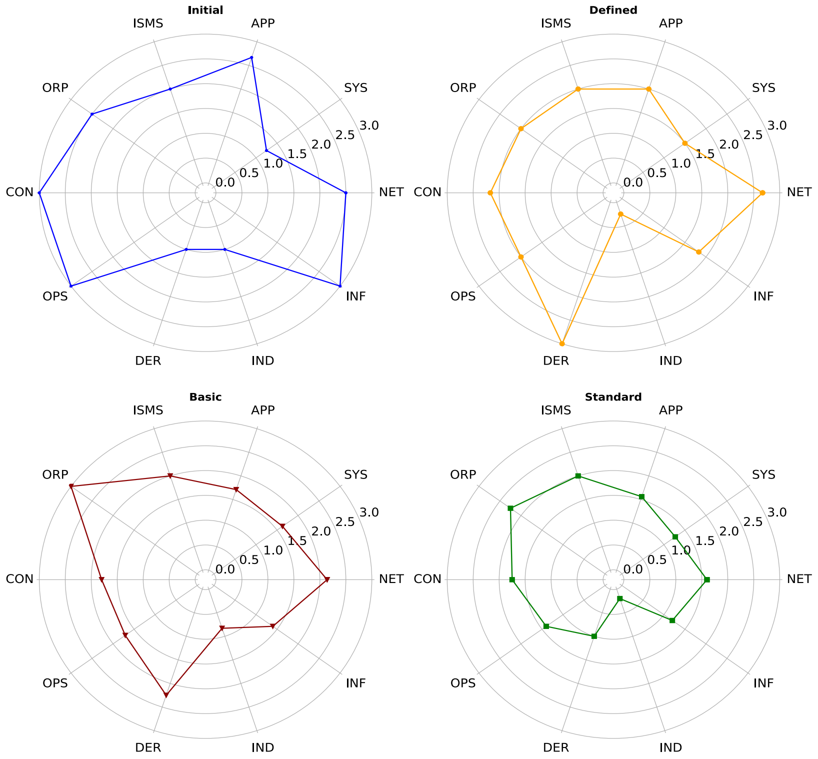
Results

Organizational level:

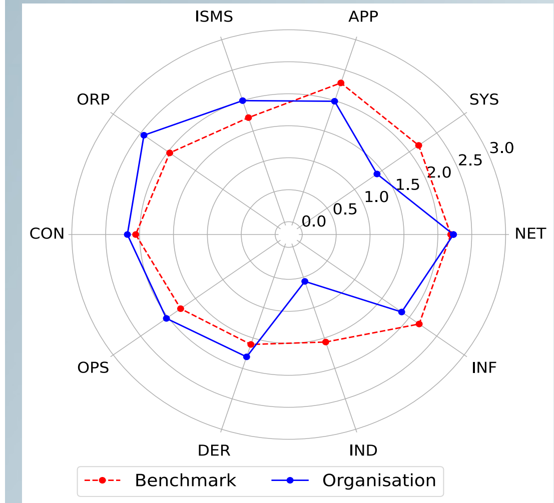
- Immediate results
- Maturity levels by security dimensions
- Can be interpreted as a risk level
- Benchmarks

Cross organizations:

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



One organization, breakdown by maturity levels



One organization, comparison with the benchmark

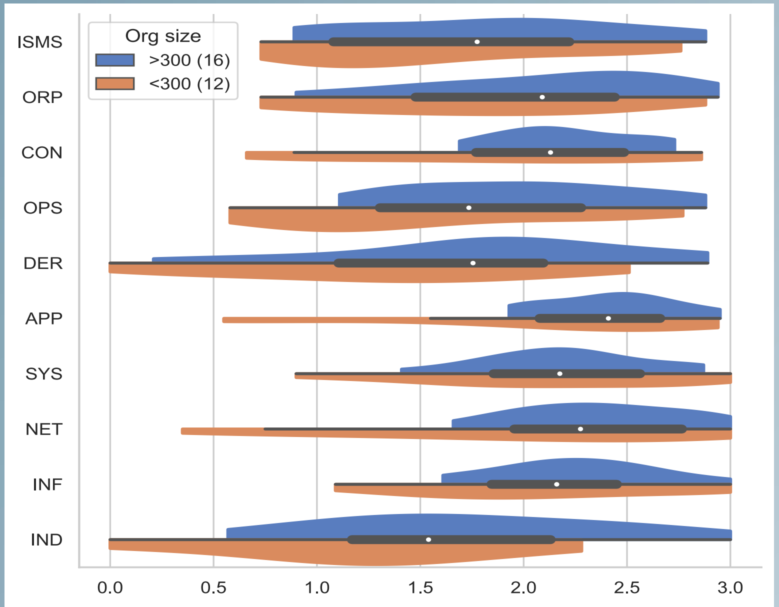
Results

Organizational level:

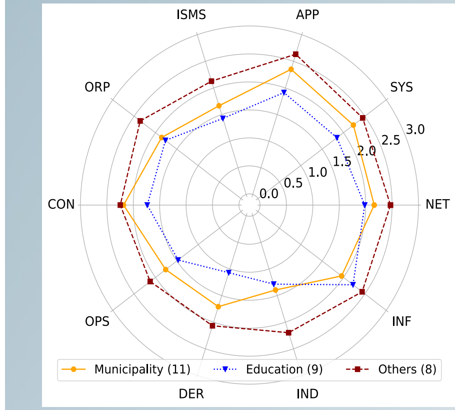
- Maturity levels by security dimensions
- Can be interpreted as a risk level
- Benchmarks

Cross organizations:

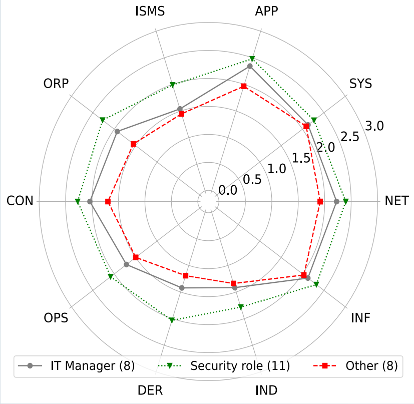
- Difference between organizations (data dispersion)
- Comparison based on individual data points (e.g., mean, median - compare results over time, provide benchmarks)



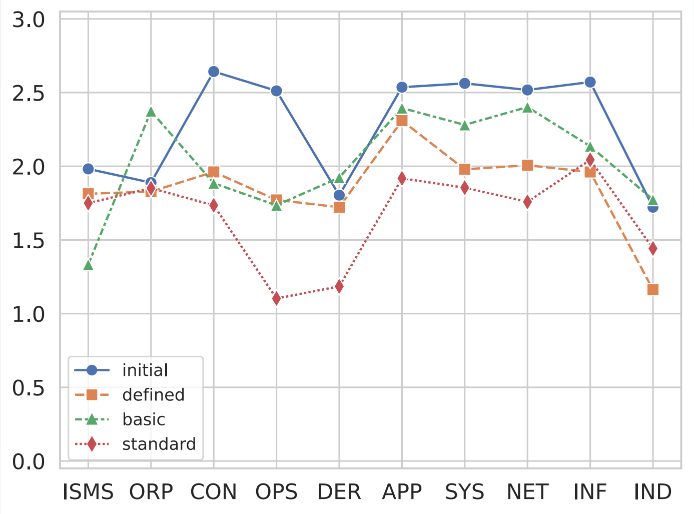
Overall evaluation distribution by dimensions and organization size.



(a) By domain



(b) By role



Overall evaluation results by maturity levels

Plans

- From PoC to official version provided by NCSC-EE
- Update the F4SLE attributes using MUSE principles (yearly)
- Repeat the data collection to follow yearly dynamics
- Conduct more data analytics and link it to other databases (causal relationships, threat landscape, security, and specific regulations)
- Assess the option of using the results to develop security-related strategies
- Engage more decision-makers
- CHESS project: Collecting the same data from Estonia and the South Moravia simultaneously to compare and find differences

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Thank you!

- Contact:
  - mari.seeba@ut.ee
  - mari.seeba@ria.ee

Partners:

UNIVERSITY OF TARTU 1632

CYBERNETICA

Republic of Estonia Information System Authority

CyberSecurityHub cz

MUNI Masaryk University

Red Hat

TAL TECH

BRNO UNIVERSITY OF TECHNOLOGY

guardtime

Associated partners:

NÚKIB

JIC

Appendix

References

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*

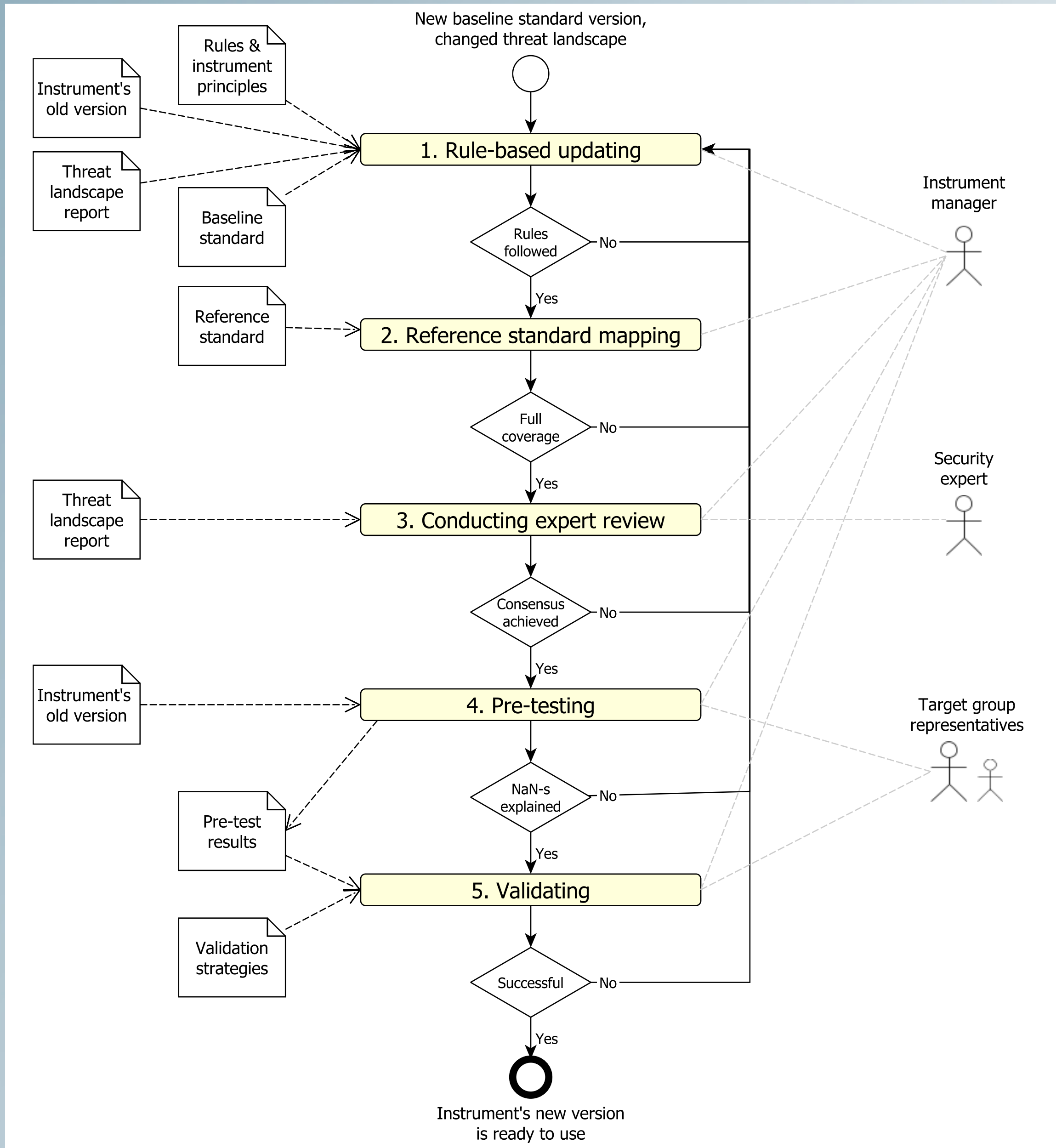
MASS- Measurement Application for Self-assessing Security

- tool to present F4SLE https://mass.cloud.ut.ee/test-massui/; https://mass.cloud.ut.ee/massui/
- immidiate results to respondents and collecting data to server
- *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/

Data interpretation options

- *Mari Seeba, Tarmo Oja, Maria Pibilota Murumaa, and Václav Stupka. 2023. Security level evaluation with F4SLE. In Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). Association for Computing Machinery, New York, NY, USA, Article 132, 1–8. https://doi.org/10.1145/3600160.3605045*

Method to update security evaluation instrument *MUSE*



- Baseline
  - Source of attributes - security controls, principles, regular updateing
  - E-ITS 2022
- Threat landscape report (attributes relevance):
  - ENISA Threat Landscape Report 2022,
  - RIA annyal cybersecurity book (2023 predictions)
- Reference standard
  - fixed scope:
  - ISO27002:2022

Dimensions

Organisational dimensions

Technical dimensions

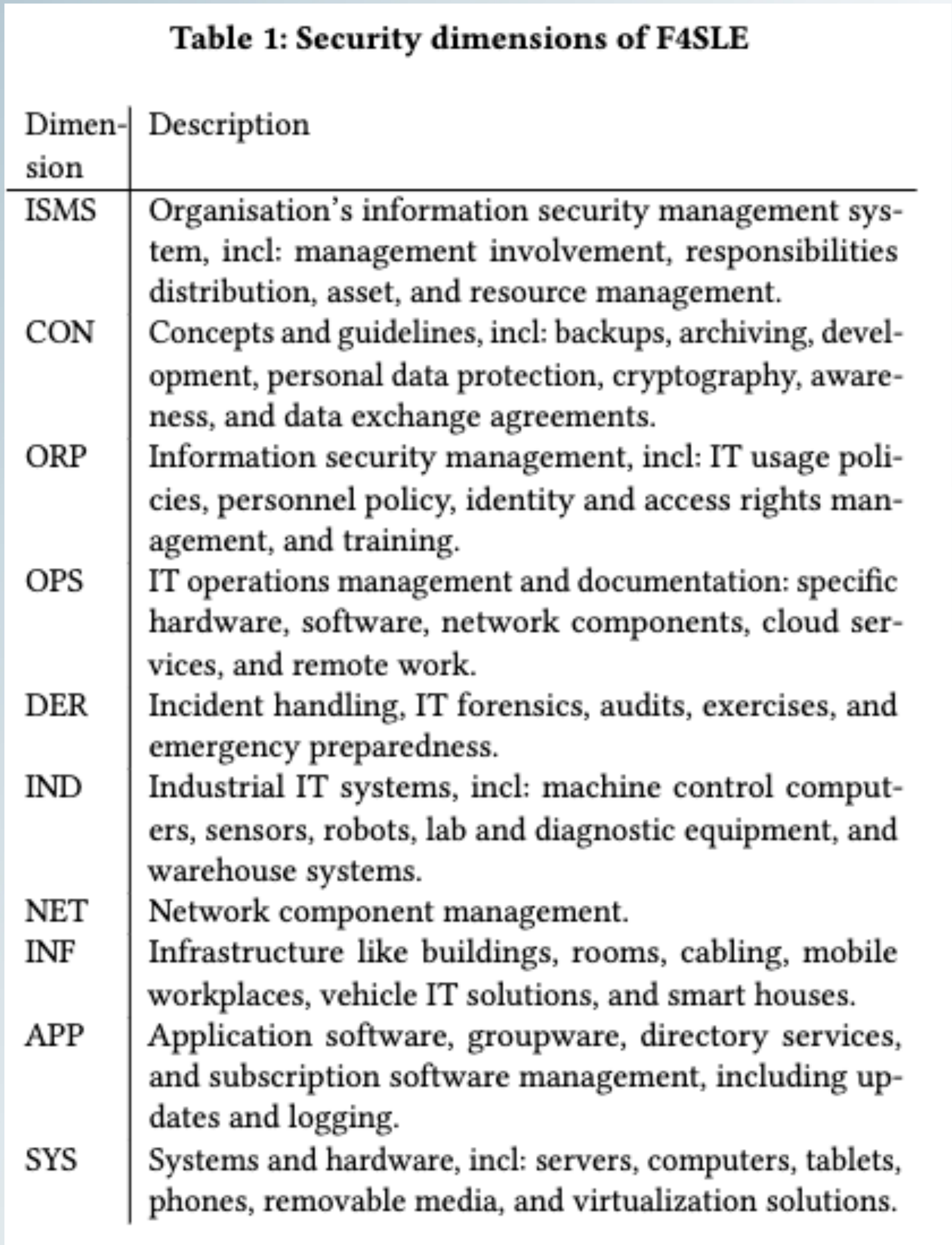


Table 1: Security dimensions of F4SLE

Dimension	Description
ISMS	Organisation's information security management system, incl: management involvement, responsibilities distribution, asset, and resource management.
CON	Concepts and guidelines, incl: backups, archiving, development, personal data protection, cryptography, awareness, and data exchange agreements.
ORP	Information security management, incl: IT usage policies, personnel policy, identity and access rights management, and training.
OPS	IT operations management and documentation: specific hardware, software, network components, cloud services, and remote work.
DER	Incident handling, IT forensics, audits, exercises, and emergency preparedness.
IND	Industrial IT systems, incl: machine control computers, sensors, robots, lab and diagnostic equipment, and warehouse systems.
NET	Network component management.
INF	Infrastructure like buildings, rooms, cabling, mobile workplaces, vehicle IT solutions, and smart houses.
APP	Application software, groupware, directory services, and subscription software management, including updates and logging.
SYS	Systems and hardware, incl: servers, computers, tablets, phones, removable media, and virtualization solutions.

https://eits.ria.ee/