



UNIVERSITY OF TARTU

Institute of Computer Science



RIIGI INFOSÜSTEEMI AMET



Framework for Security Level Evaluation

F4SLE

Mari Seeba



Cyber-security Excellence Hub in
Estonia and South Moravia



CyberSecurityHub^{cz}

What is my security situation?

Technical failure

Assets?

Supply chain failure

How to stay competitive?



Cyberattacks

E-ITS

GDPR

ISO27001

NIS2

Reporting of security status to NSCS

F4SLE *Framework for Security Level Evaluation*

Self-assessment

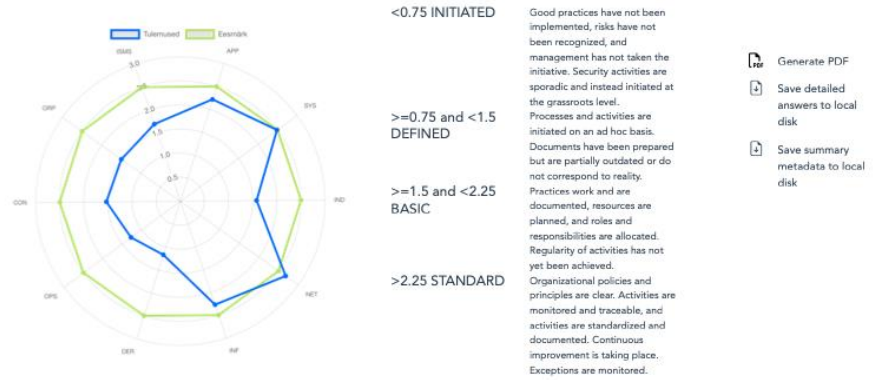
Immediate result

All-hazard approach

ISO27001, NIS2, E-ITS, ENISA Threat landscape report

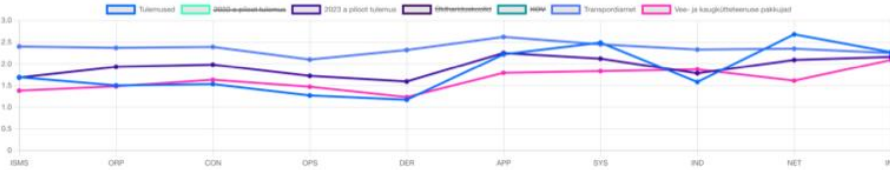
Comparison benchmarks





- Generate PDF
- Save detailed answers to local disk
- Save summary metadata to local disk

Results compared to benchmark



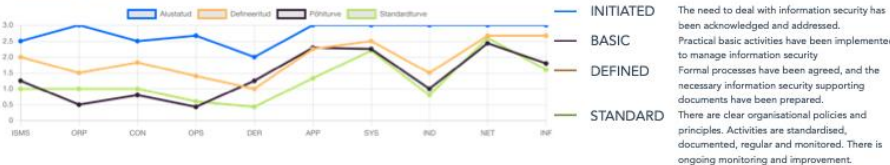
Process dimensions

- ISMS** 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.
- ORP** Situation assessment of information security management, including usage rules for computers and other devices, personnel policy, identity and access rights management, and training.
- CON** Situation assessment of the organisation's basic information security concepts used for all other areas, including backups, archiving, development, personal data protection principles, and cryptography-related procedures and awareness. In addition, data exchange agreements between data exchange partners.
- OPS** Situation assessment of the organisation's IT operation management regardless of specific hardware, software, or network components. This includes the management and documentation of Cloud services and remote work.
- DER** Situation assessment of security incident management, related activities (including IT forensics), audits, and emergency preparedness (including exercises).

System dimensions

- APP** Situation assessment of software, groupware, directory services, and subscription software management, including secure configurations of updates, need-based accesses, and logging.
- SYS** Situation assessment of the hardware solutions and management (including setup, monitoring, and management) like servers, computers, tablets, phones, removable data media, and virtualization solutions.
- IND** Situation assessment of secure management (configuration and monitoring) and safety of machine tool control computers, sensors, robots, lab and diagnostic equipment, warehouse systems and other industrial IT systems.
- NET** Situation assessment of network, network components, telephone communications management, computer network project timeliness, regular updating, and outdated and unsafe solution avoidance (default passwords and manufacturer-unsupported solutions).
- INF** Situation assessment of security management for buildings, rooms, cabling, mobile workplaces, vehicle IT solutions and smart houses. Compliance with building fire safety requirements, special safety requirements and location in facilities for protected rooms, and the inclusion of smart infrastructure in the security policy are considered.

Maturity levels

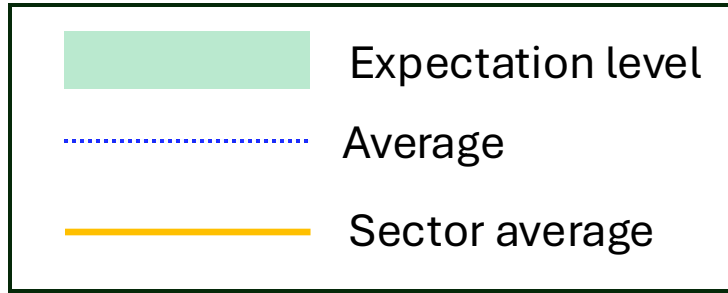


Organization and CISO

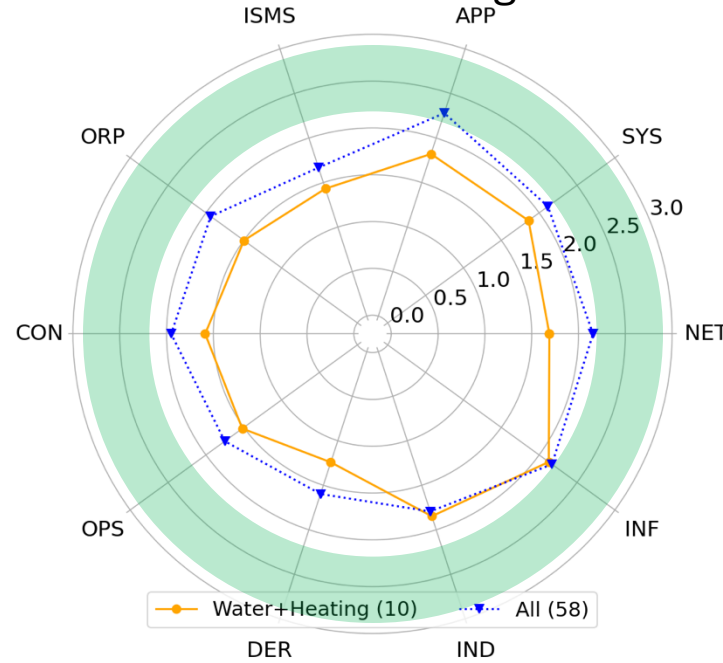
- Security evaluation result in 10 security dimensions
- Risk level values
- Comparing with expectation level (green line)
- Benchmarking with others
- Meanings of Security dimensions
- Details of maturity, documentation, practical measures, continuity



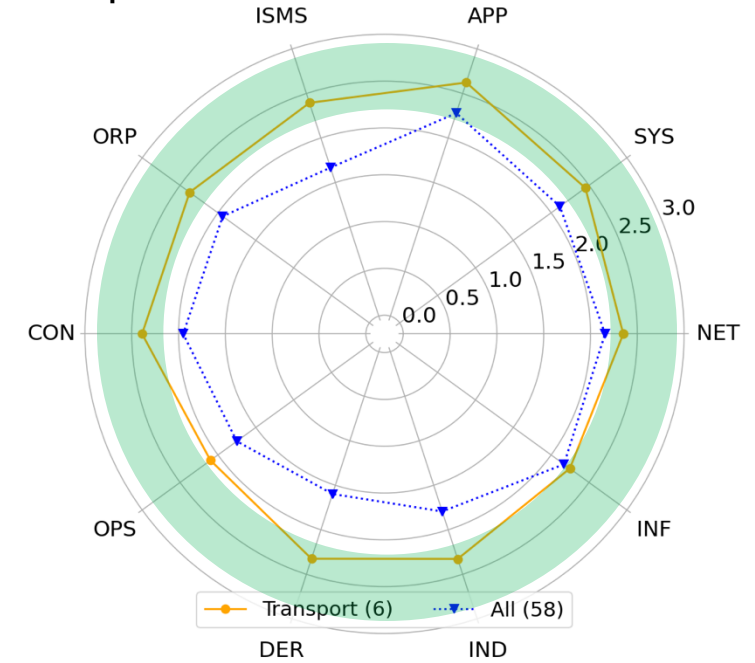
Comparison of Sectors



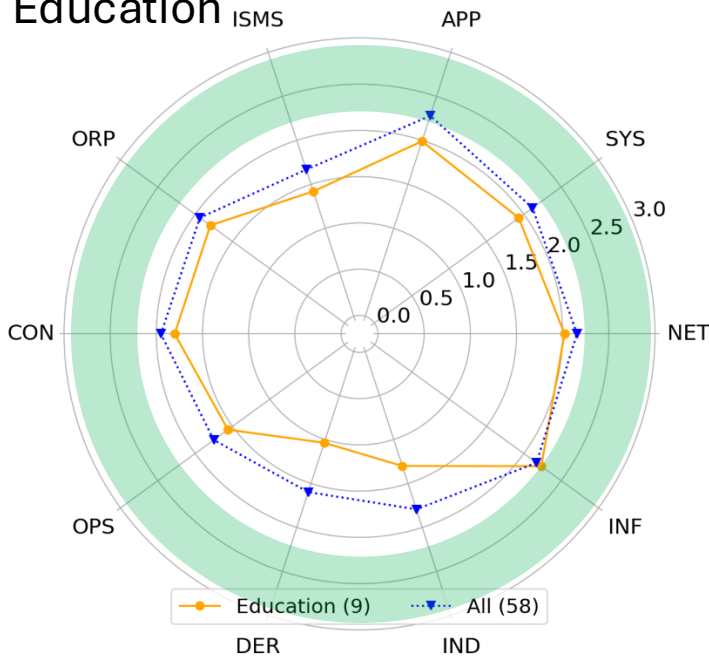
Water and distance heating



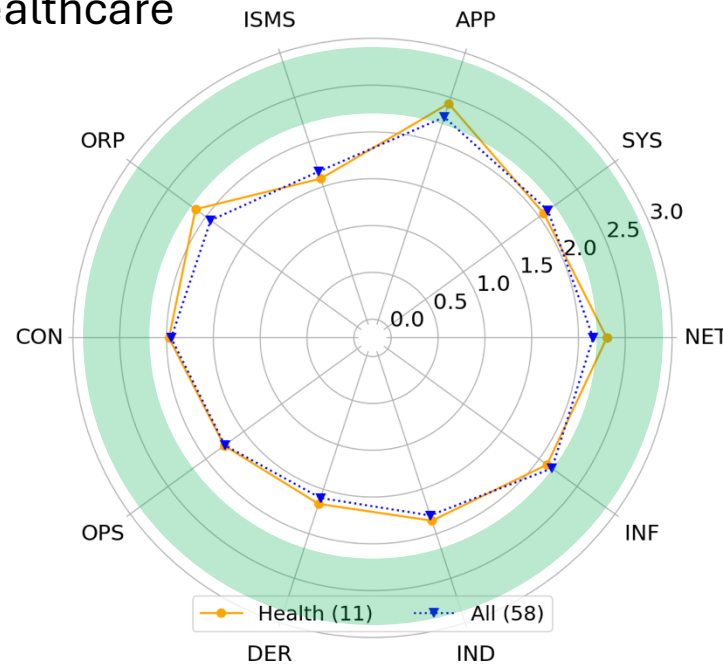
Transport



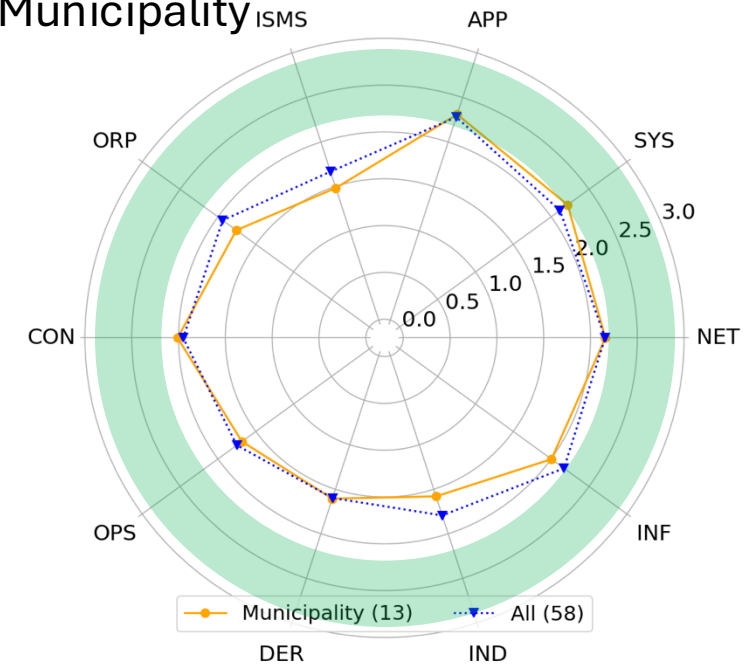
Education



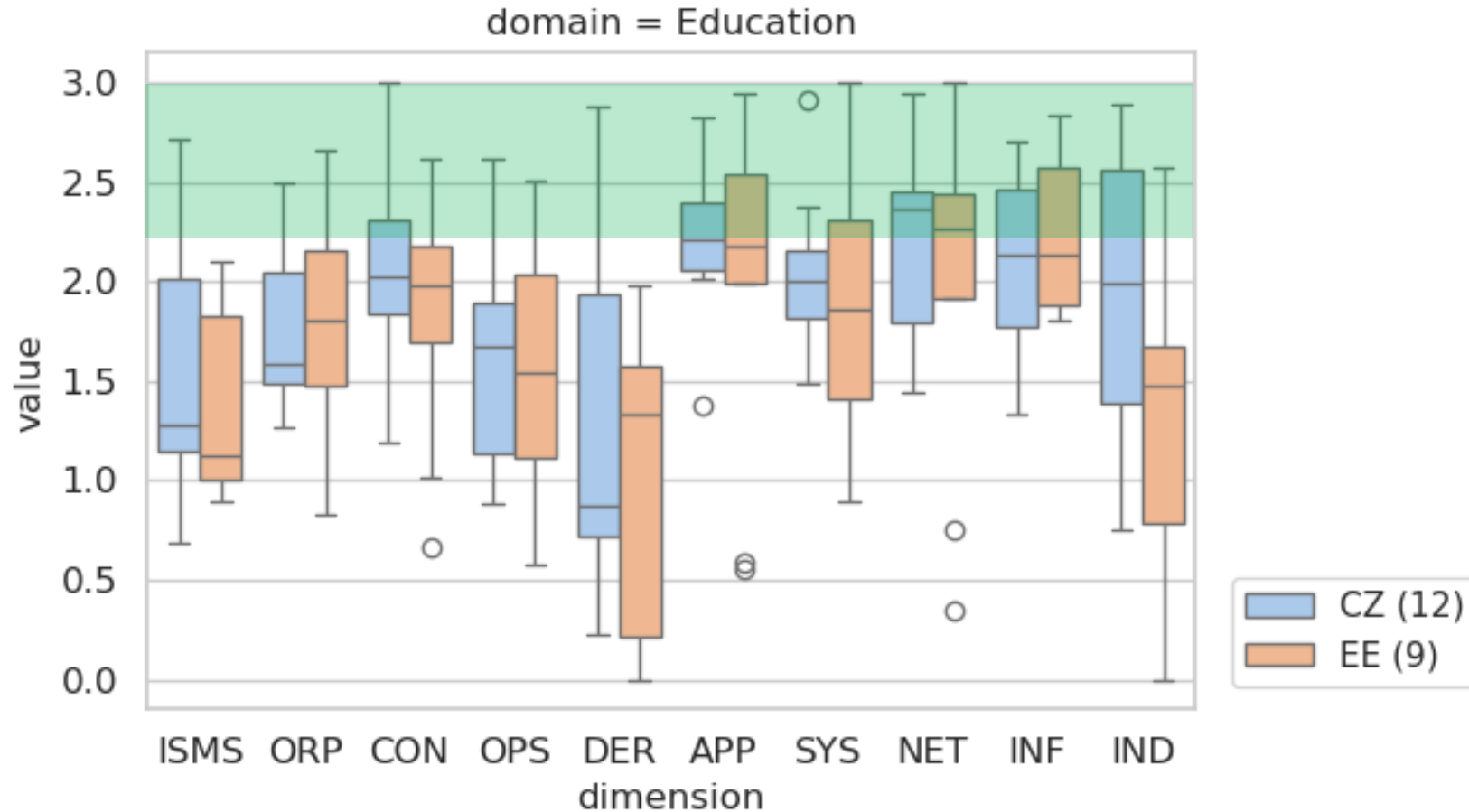
Healthcare



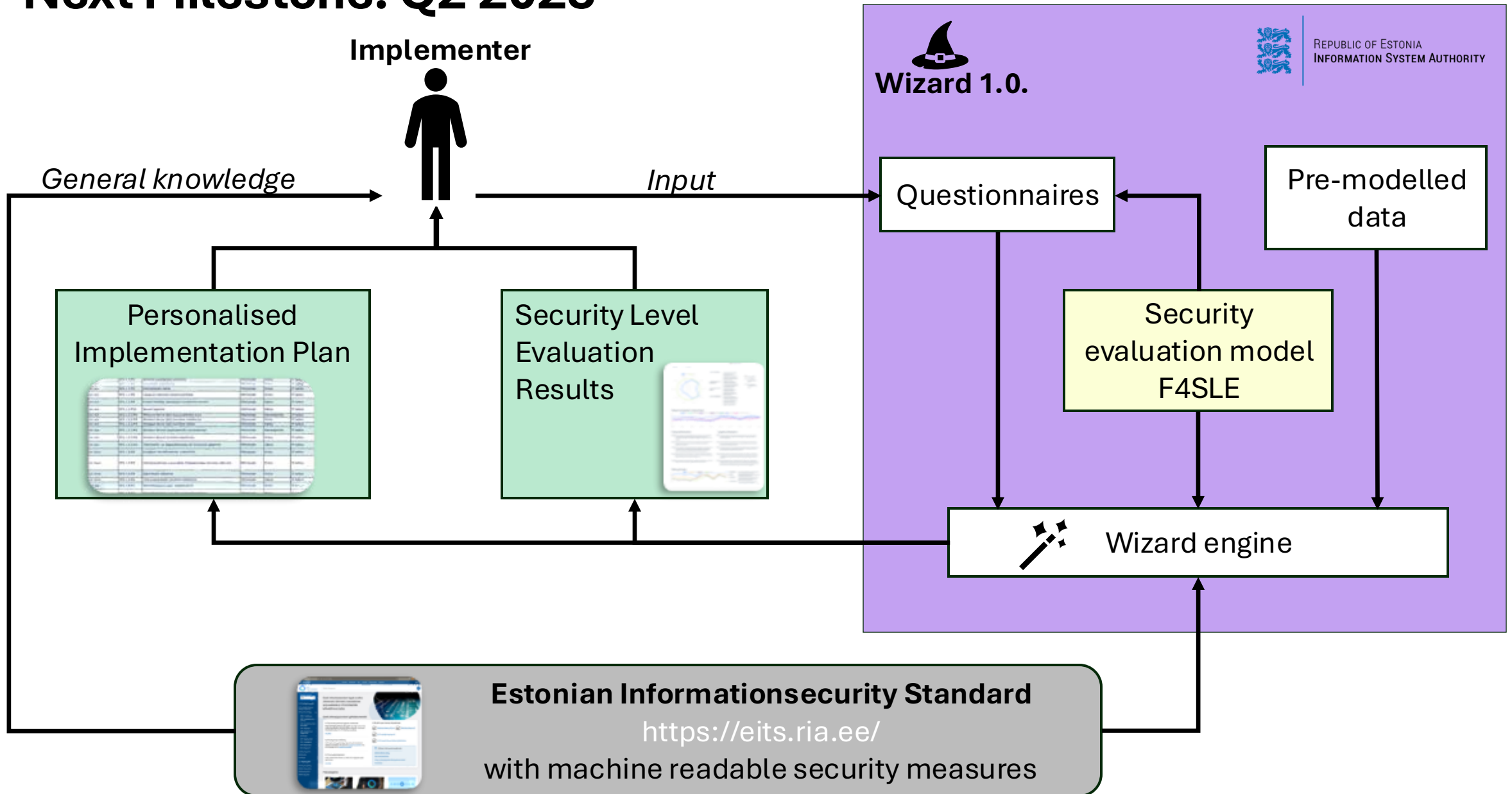
Municipality



Estonia vs Czech - Education



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.

CHESS



Security Level Evaluation with F4SLE¹

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



Cybersecurity 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

	Attribute categories based on the level of security measures			
	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)				

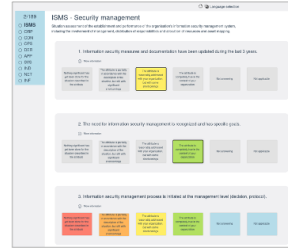
- Set of attributes where each attribute is evaluated on a four-level scale
- Not implemented
- Implemented with significant deficiencies
- Implemented with a few shortages
- Fully implemented

MASS - Measurement Application for Self-assessing Security

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

Collected metadata with options (in Italian 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; NIS2 (Estonian); CIS Controls; NIS2 (Estonian); NIS2 (CZ); ENISA (Estonian); BS IT Grundschutz (German); Act on cyber security, no.181/2014 Coll. (Czech)



MASS user interface example

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

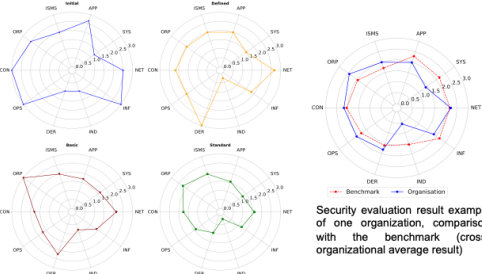
Organizational level:

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

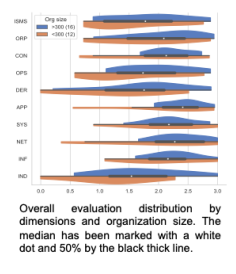
Results

Cross organizations (interpretation principles):

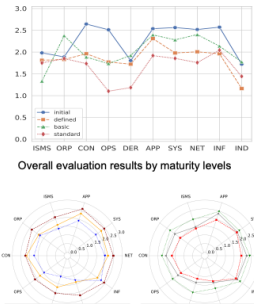
- Difference between organizations (data dispersion)
- Comparison based on individual data points (e.g., mean, median - compare results over time, provide benchmarks)



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



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.

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

Limitations

- Selected, voluntary organizations – 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 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

- 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.