UNIVERSITY OF TARTU
1632
Institute of Computer Science

SEMINAR

"We'll Deal With Cybersecurity Later" – Strategy or a Ticking Time Bomb?

January 29 • 14:00 • Seminar room 2

Mari Seeba

Leading Cybersecurity Expert at the Estonian State Information System Authority National Cyber Security Centre

NATIONAL CYBER SECURITY CENTRE
NCSC-EE

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

STARTUP DAY

Mari Seeba <mari.seeba@{ut|ria}.ee>

Affilation

- 2020 - … Estonian Information System Authority NCSC-EE,
  - Leading cybersecurity expert developing E-ITS
- 2007 - … ISACA Estonia Chapter board member
  - Prerident, Vice President, Program Chair
- 2005 – 2019 Cybernetica AS
  - Information Security Auditor, consultant, project manager of cryptography projects and other projects related with reaseach
- Science Teacher

Education

- 2021 - … Information security PhD student in Tartu University
  - Security evaluation, Risk Management, Security Standards
- 2017 – 2019 MSc
  - Conversion to IT – ISMS (ISO27001) integration into work flow management system (JIRA)
- Science Teacher Diploma, Bachelor in Physics

ideation – main concerns are related to privacy and communication security

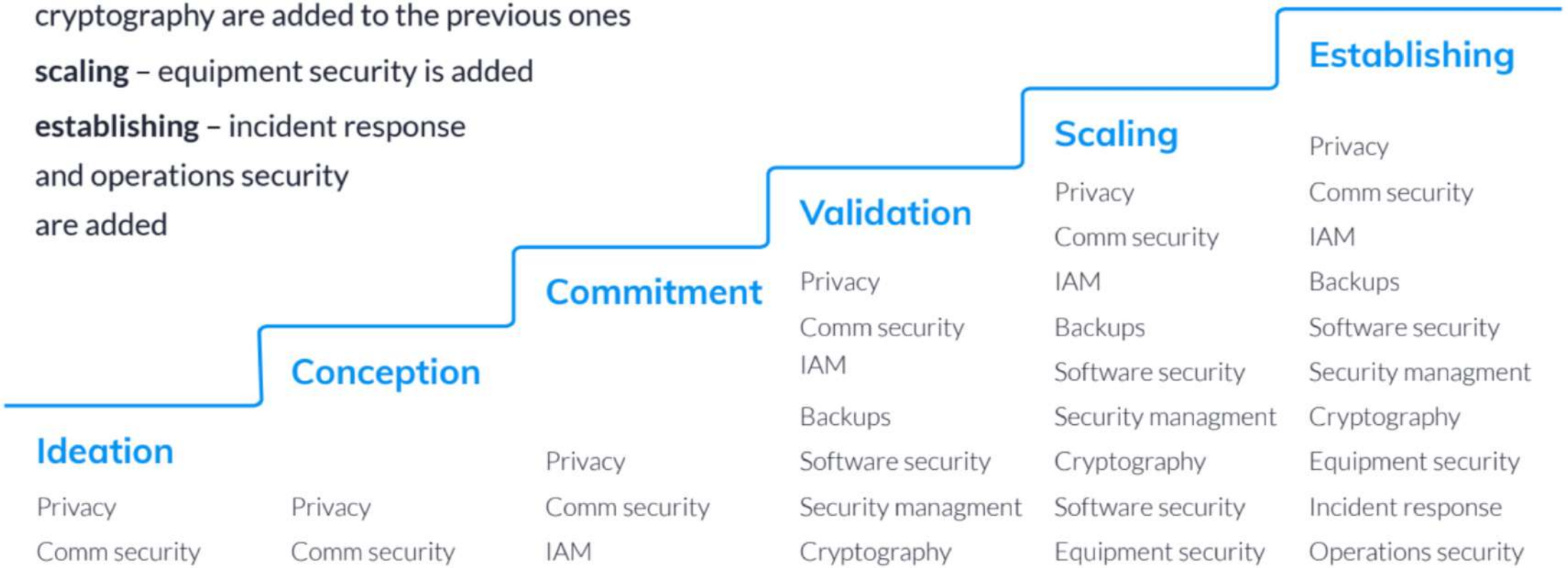
conception – main concerns remain the same as in the previous stage, but are needed to be more specified

commitment – IAM (identity and access management) is added to this stage

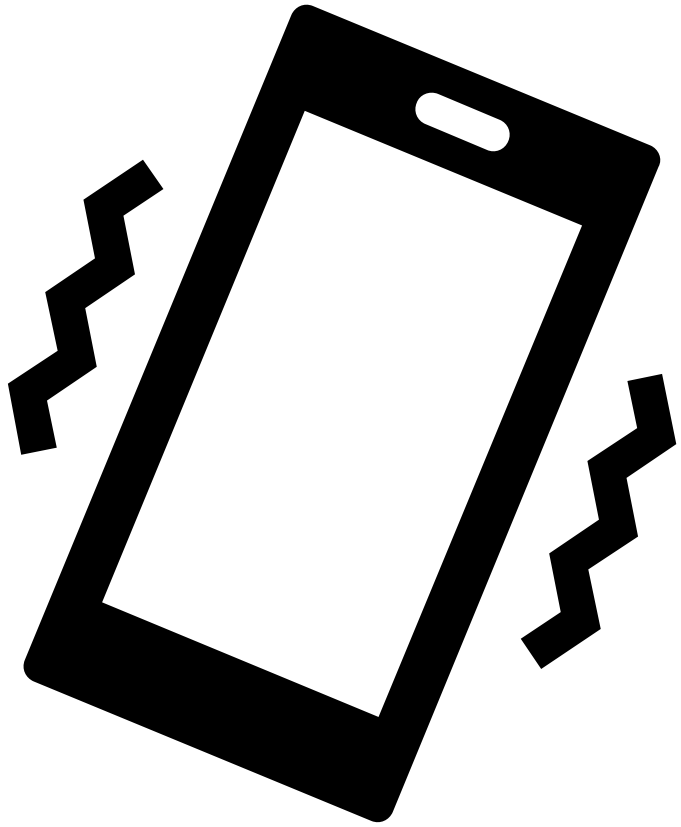
validation – backups, software security, security management and cryptography are added to the previous ones

scaling – equipment security is added

establishing – incident response and operations security are added



SecureMVP, Garage 48 #Cybersecurity (2019)



Implementing information security management

What we protect?	Protection area or scope (assets and processes)
Why we protect?	Protection need (C-I-A), risk levels, damage scenatious, requirements
How we protect?	risk management and risk management measures (controls)- (E-ITS, ISO27001) implementation
Did we succeeded?	Monitoring, auditing, self-assessment

Why to evaluate security?

- How secure am I?
- Am I better than I was this time last year?
- Is my security spending appropriate?
- How secure am I compared to others?
- What risk transfer options do I have?

- Compliance
- Progress (As-Is -> To-Be)
- Knowledge of vulnerabilities and risks
- Reducing uncertanty
- Trusting the partners
- Comparing with others
- Budget

Hubbard, D.W., Seiersen, R., How to measure anything in cybersecurity risk, (2014)

Why evaluation of security is so… hard?

- We cannot measure all security requirements
- Environment, abstraction level, and context affect security
- Measurement as a process affects security
- No system is independent
- Security is multi-layered
- Adversary changes the environment

- We are too optimistic
- We perceive benefits and losses differently, even though they are numerically comparable
- Measurement is both feedback and a goal

Pfleefer, S., L., Cunningham, R., K., Why Measuring Security is Hard (2010), IEEE Computer and Reliability Societies

Cybersecurity Assessment Methods by Leszczyna (2021)

- checklist-based evaluation & compliance checking
  - verifying the presence of specific attributes
- vulnerability identification
- penetration testing
- simulation
- formal analysis

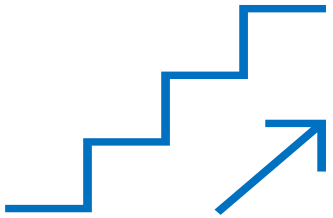
Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. Computers & Security.

Security Measurement Models by Khalenghi et al. (2022)

- Graph-based models (utilizing nodes and edges)
- Stochastic models (applying probability theory)
- Logic-based models (using formal logic)
- Ontology-based models (leveraging semantic relations)
- Hierarchical & decision-making models

Khaleghi, M., Aref, M. R., & Rasti, M. (2022). Comprehensive Comparison of Security Measurement Models. Journal of Applied Security Research,

Maturity models



	Cyber Security Maturity Models (CSM2)	Organizations or Author	Purposes and Strengths	Maturity Levels				
				1	2	3	4	5
1	Information Security Evaluation Maturity Model (ISEM), 2000	City Group	Security awareness and evaluation	Complacency	Acknowledgement	Integration	Common practice	Continuous improvement
2	Systems Security Engineering Capability Maturity Model (SSE-CMM), 2001	The US National Security Agency (NSA)	Evaluation of software security engineering processes	Performed informally	Plan and track	Well defined	Control	Continuous improvements
3	Information security management system (ISMS-ISO 27001), 2005	ISO	Information security risk management through security standards	Performed	Managed	Established	Predictable	Optimized
4	Information Security Management Maturity Model (ISM3), 2007	ISM3 Consortium	Prevent and mitigate incidents and Optimise the use of information, money, people, time and infrastructure	Undefined	Defined	Managed	Controlled	Optimized
5	Information Security Maturity Model (ISM2), 2007	NIST-PRISMA	Provides a framework for review and measure the information security posture of an information security program	Polices	Procedures	Implemented	Tested	Integrated
6	Gartner's Information Security Awareness Maturity Model (GISMM), 2009	Gartner	Security awareness, and risk management in large international organizations	Blissful ignorance	Awareness	Corrective	Operations excellence	
7	Information Security Framework (ISF), 2009	IBM	Security gap analysis between business and technology	Initial	Basic	Capable	Efficiency	Optimizing
8	Resilience Management Model (RMM), 2010	CERT	A capability-focused process model for managing operational resilience	Incomplete	Performed	Managed	Defined	
9	Community Cyber Security Maturity Model (CCSMM), 2011	White	Community effort and communication capability in communities	Initial	Advanced	Self-Assessed	Integrated	Vanguard
10	NICE's Cyber Security Capability Maturity Model, 2012	The US DHS	Workforce planning for cyber security best practices	Limited	Progressing	Optimized		
11	Cyber Security Framework (CSF-NIST), 2014	NIST	Improves federal critical infrastructure through a set of activities designed to develop individual profiles for operators	Identify	Protect	Detect	Respond	Recover
12	Cyber Security Capability Maturity Model (C2M2), 2015	Curtis	Assessment of implementation and management in Critical Infrastructure	Not performed	Initiated	Performed	Managed	

N. T. Le and D. B. Hoang, "Can maturity models support cyber security?," (2016), doi: 10.1109/PCCC.2016.7820663.

Information Security Maturity Models

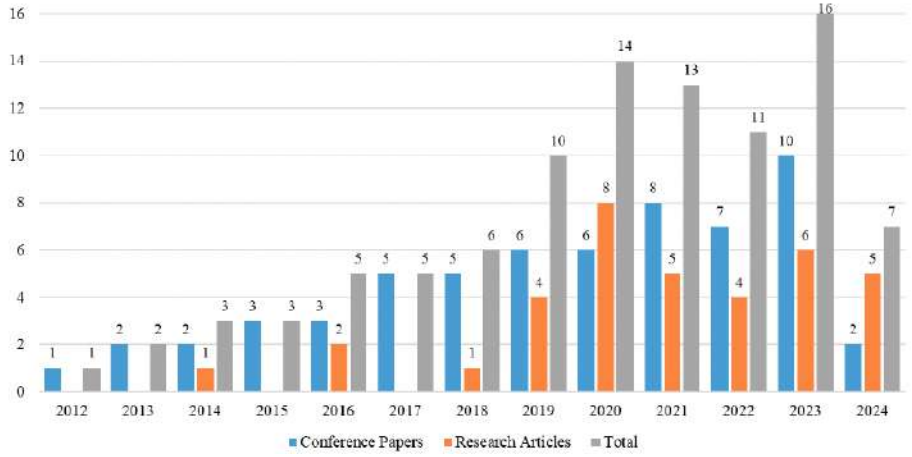
- Only 33% of the published metrics analyzed in the study have been tested in a real-world environment
- 43% of the study models do not even plan to continue working with the metric or implement it in the future
- The impact of metrics is relatively poorly studied
- Stronger public sector (industry) cooperation with academia is needed

Rabii, Anass, et al. (2020) Information and cyber security maturity models: a systematic literature review.

Recent trends of Maturity Assessment

Why – key drivers

- Regulatory compliance
- Cyber security threat resilience
- Data protection
- Risk management and mitigation
- Incident responce preparedness
- Investment in cybersecurity
- Enhancing security culture
- Improving business continuity
- Cost-effective security solutions



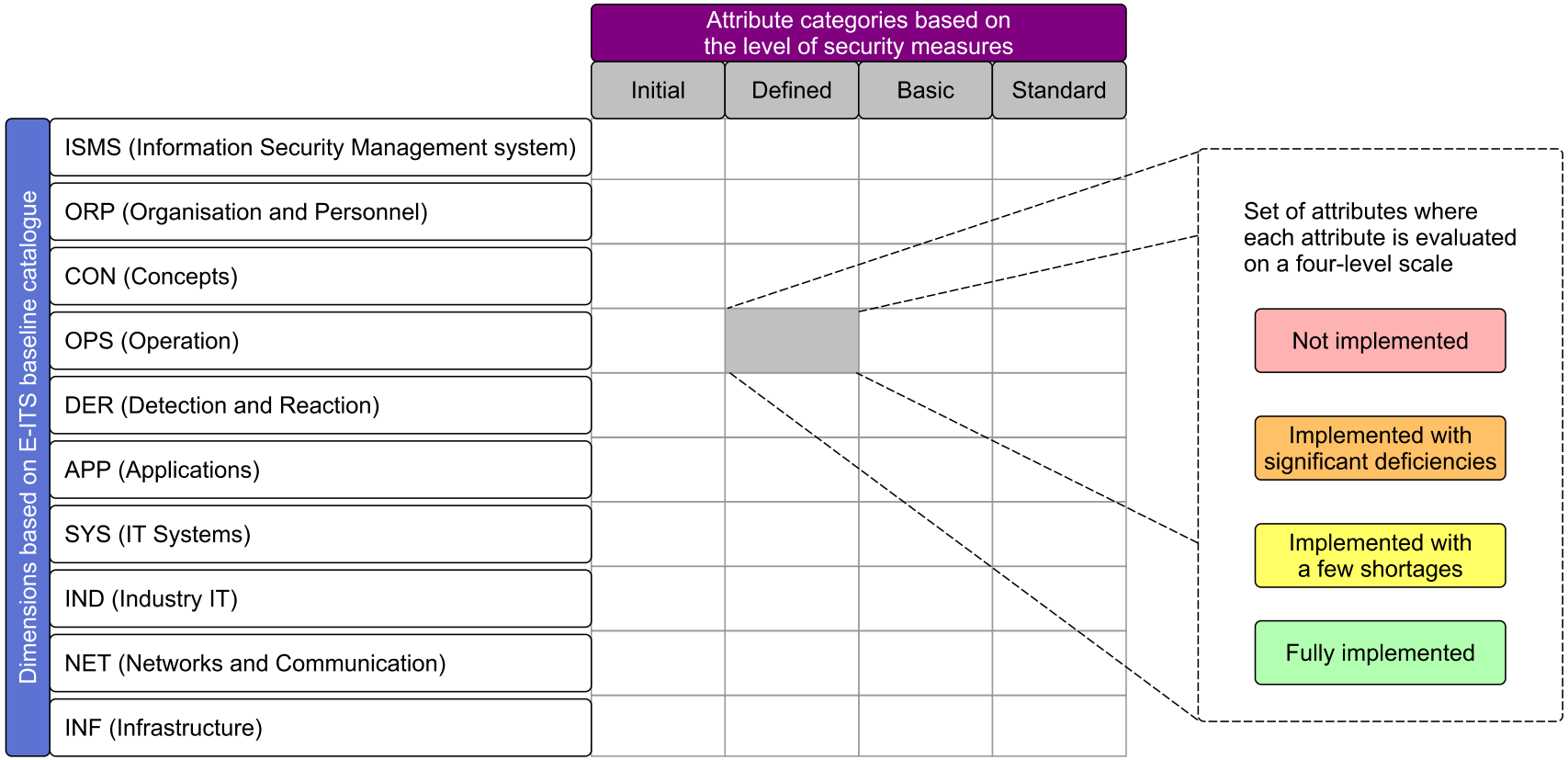
Main gaps

- Resource constrants (designed usually for larger organisations)
- Complexity of models
- Customisation to specific sectors
- Lack of practical guidance
- Cultural and human factor barriers (low awareness, resistance to change)
- Alignment with business objectives
- Lack of automation and tool support
- Inconsistem metrics and evaluation (standardisation to provide benchmarks, comparability)
- Integration with existing systems
- Financial barriers
- Limited focus on emerging technologies
- Time consuming assessment

Alenka Brezavšček , Alenka Baggia (2024), Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review

Req. 1	Framework should cover a wide area of security-related topics.
Req. 2	Framework should produce quantifiable and comparable results.
Req. 3	Framework should be quick and easy to implement and understand.
Req. 4	Framework should be aligned with a security standard.

F4SLE structure



INITIAL - Awareness

- The need to deal with information security has been acknowledged and addressed

DEFINED- Documentation

- Formal processes have been agreed, and the necessary information security supporting documents have been prepared

BASIC - Practical

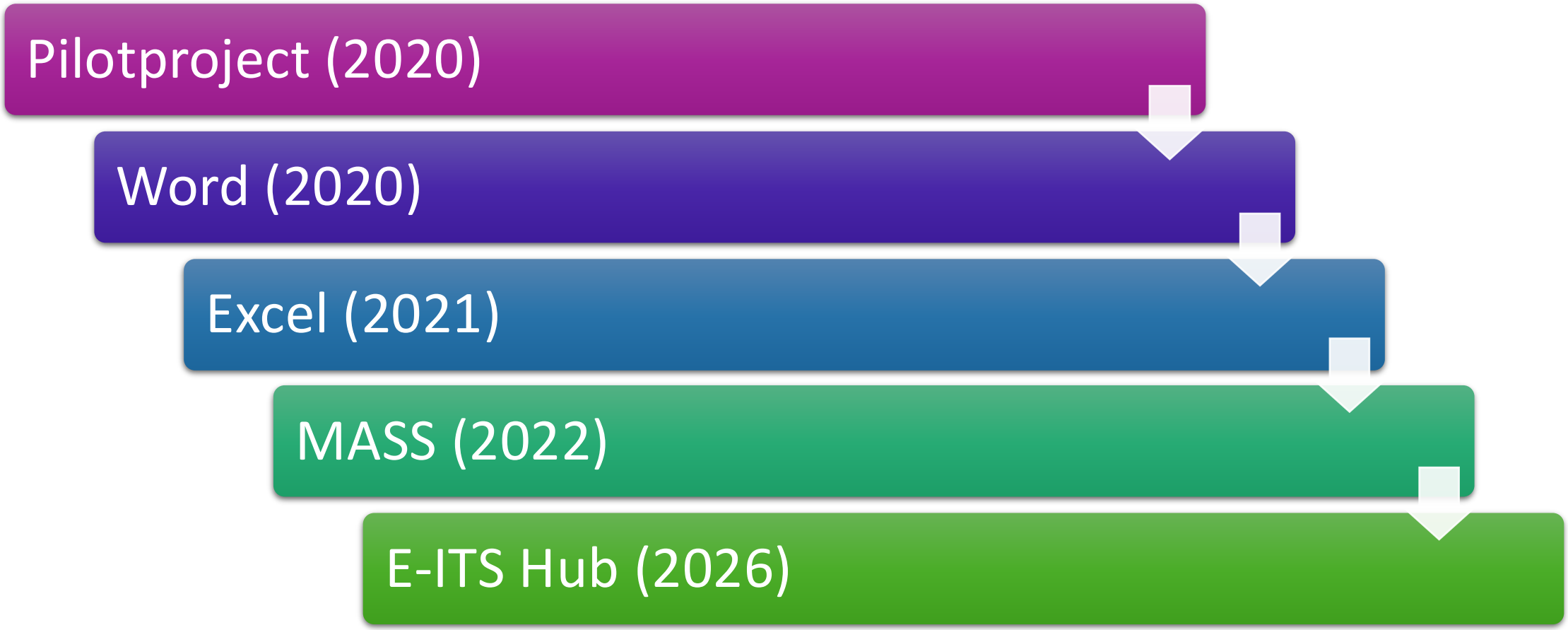
- Practical basic activities have been implemented to manage information security

STANDARD – Continuity and maturity (resiliance)

- There are clear organisational policies and principles. Activities are standardised, documented, regular and monitored. There is ongoing monitoring and improvement.

Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations.

F4SLE - Framework for Security Level Evaluation



F4SLE Framework for Security Level Evaluation

Immediate response

Benchmark with others, expectation, risk level

Compliance and comprehensiveness (E-ITS, ISO27001, NIS2, ENISA TLR)

Lowest possible entry barrier

Upgradability so that comparability is maintained (MUSE)

Data collection tool (automation) and data privacy (MASS)

- Immediate response
- Benchmark with others, expectation, risk level

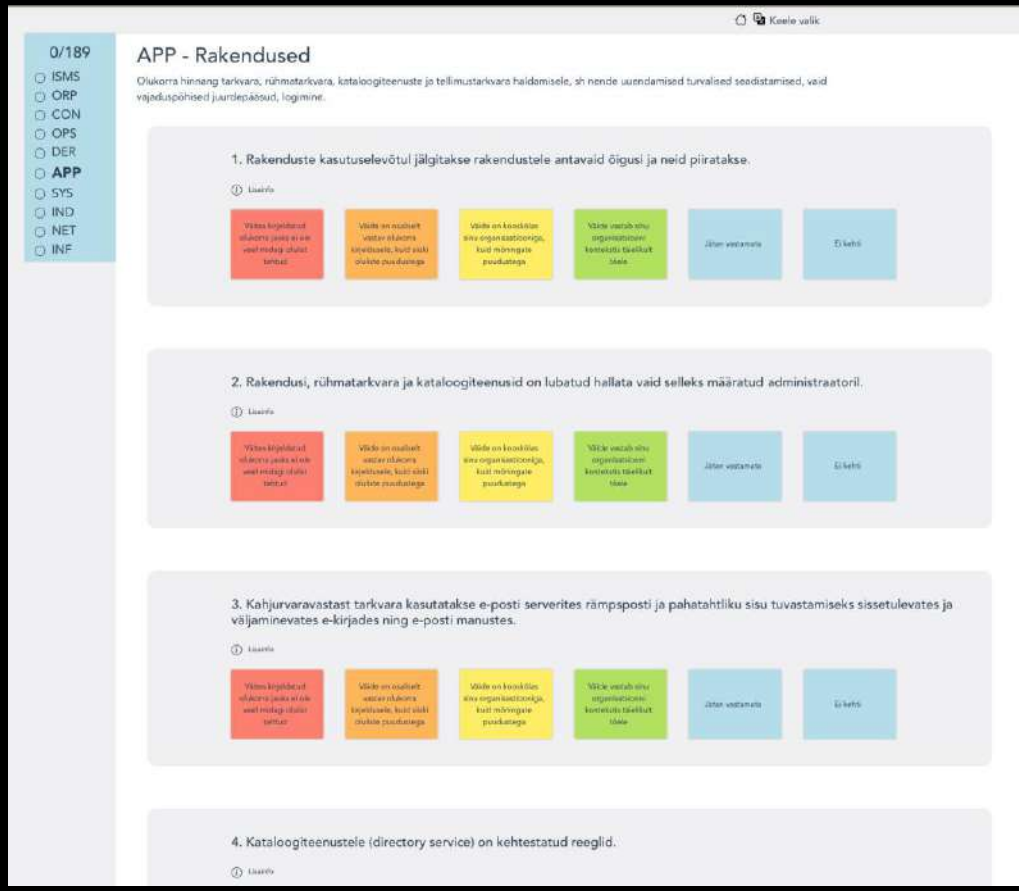
Repeated evaluation

Data reuse for different stakeholders

Multilingualism

MASS – web-based tool for using F4SLE and collecting data

- Privacy principle – raw data does not leave the respondent PC
- Only aggregated (averaged) data is sent to the server
- Immediate results to the respondent
- Providing a benchmark to the respondent
- Data reuse



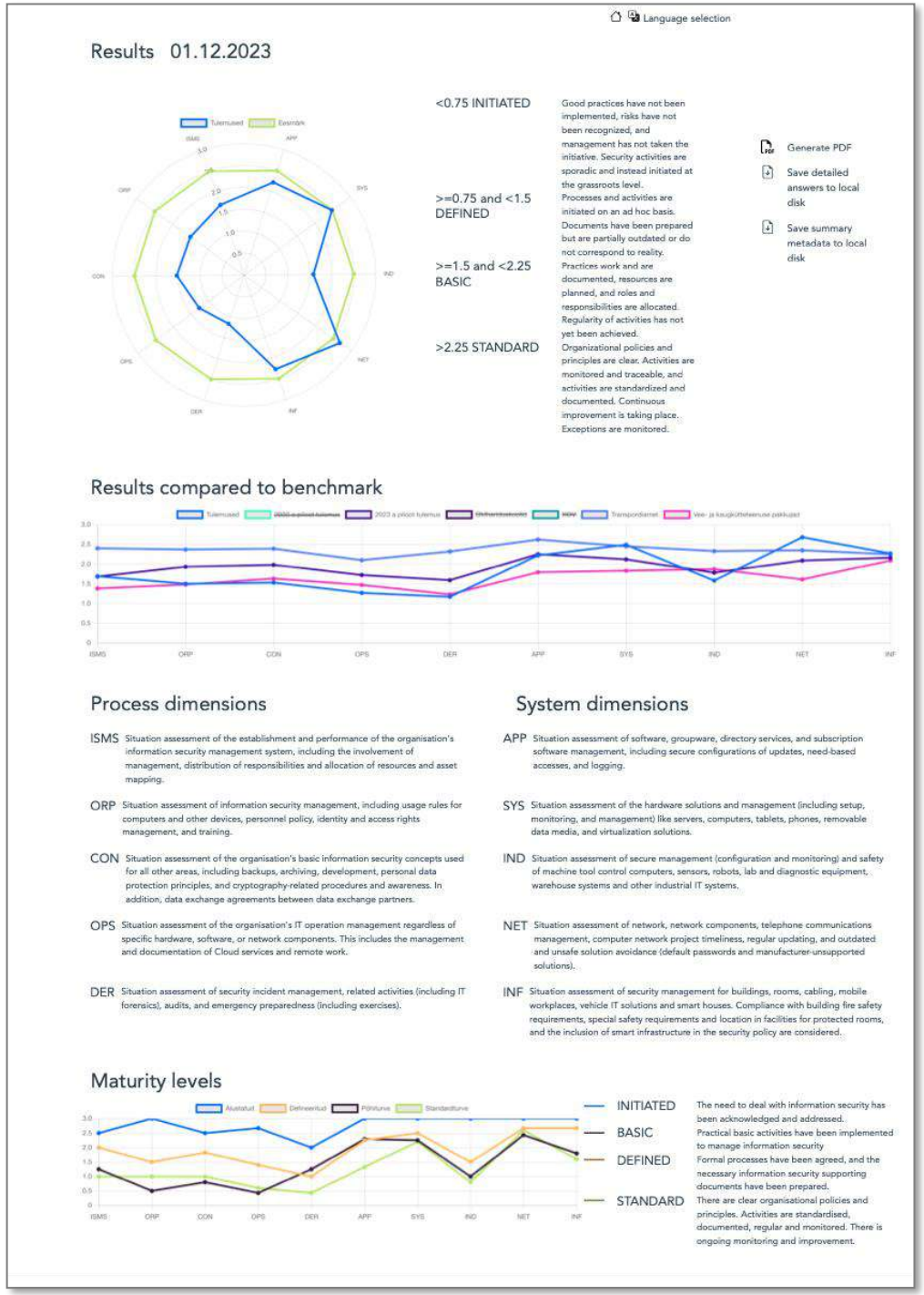
Test environment: https://mass.cloud.ut.ee/test-massui/#/

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

RIIGI INFOSÜSTEEMI AMET

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL
arvutiteaduse instituut



Results page

- Rating in 10 dimensions
- Risk levels
- Comparison with expectation (green line)

- Benchmark with other sectors

- Explanations of security dimensions

- Maturity levels in more detail

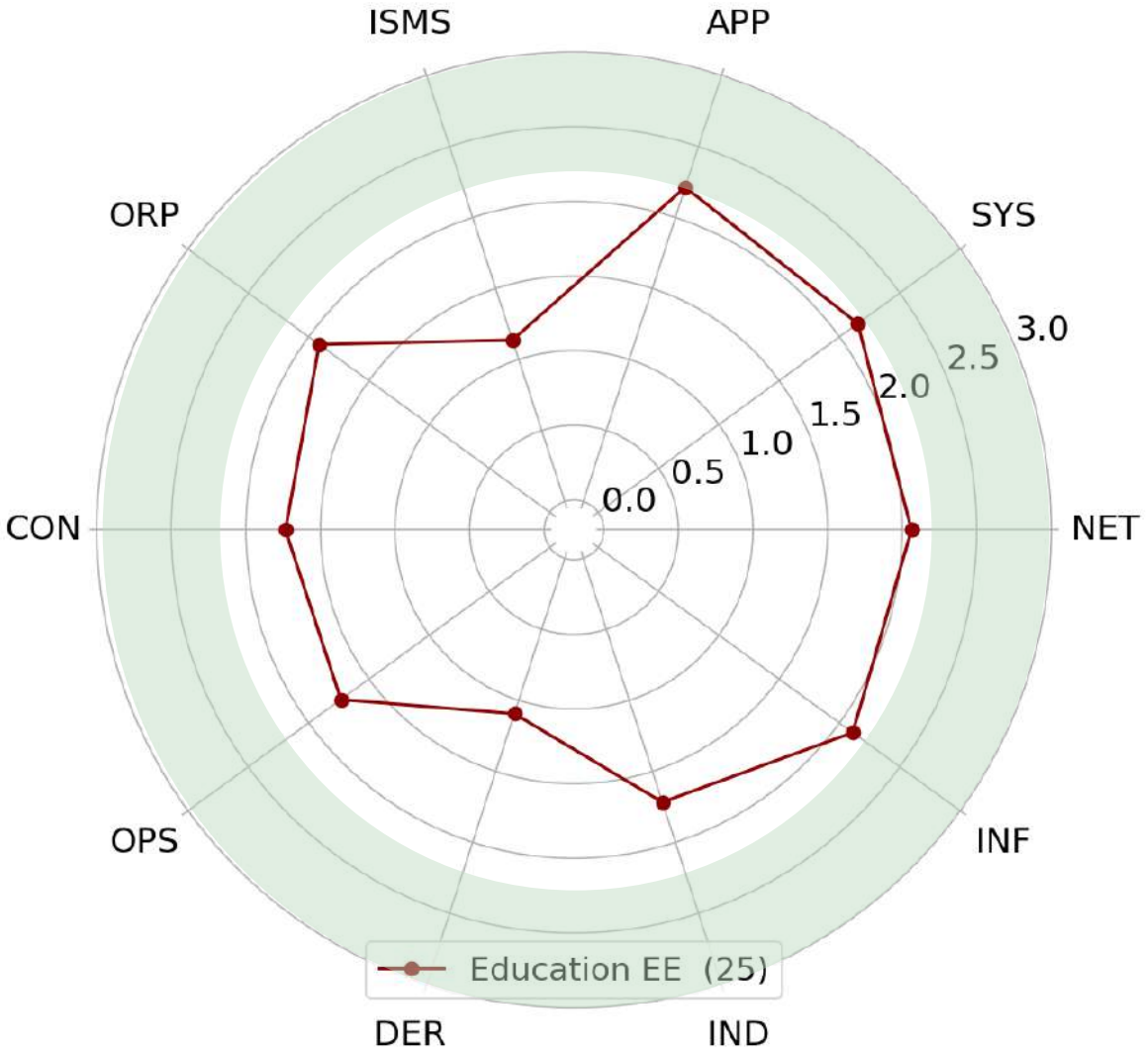
https://mass.cloud.ut.ee/massui/

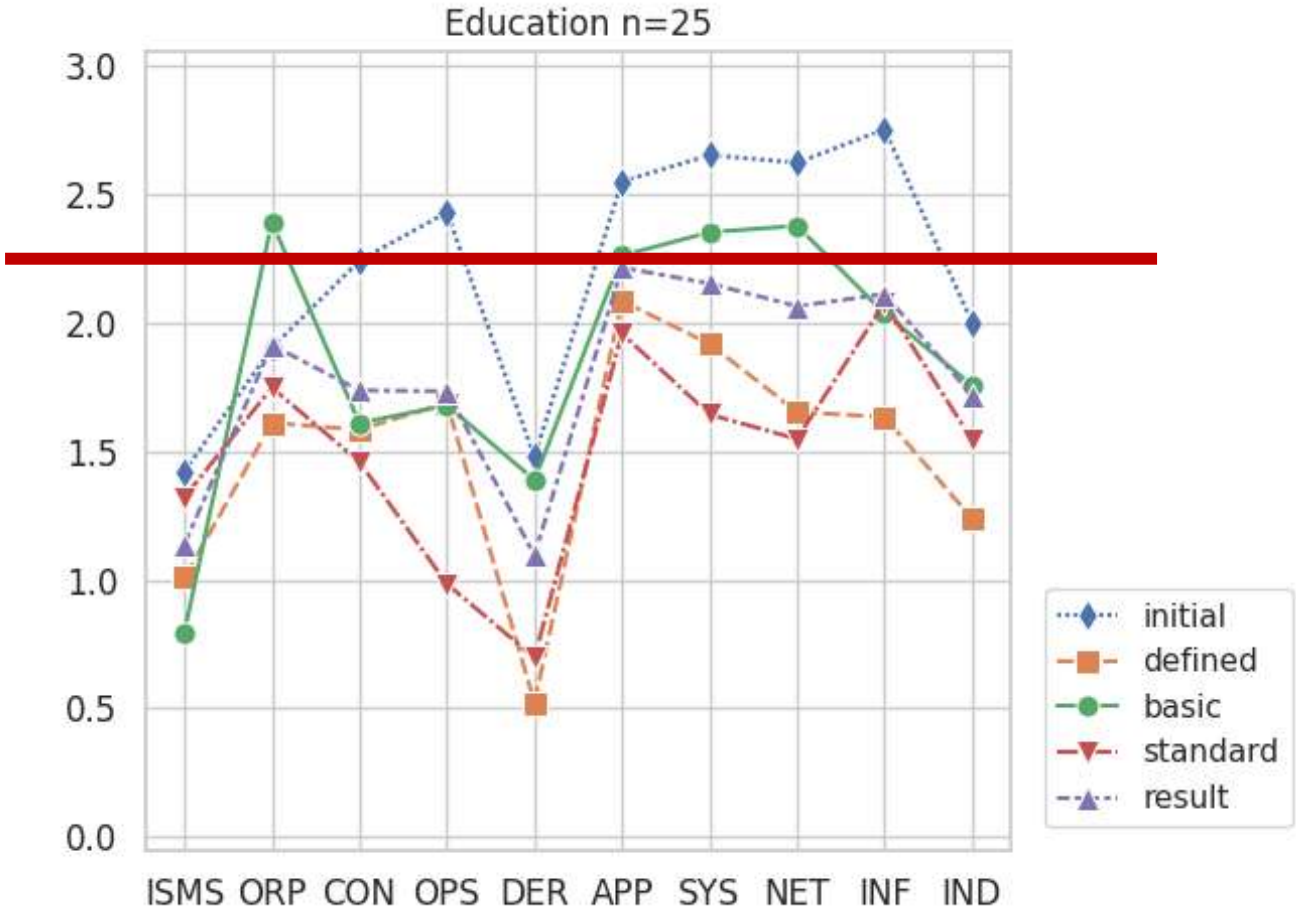
Stakeholders?

User stories (data reuse by NIS2 Directive)

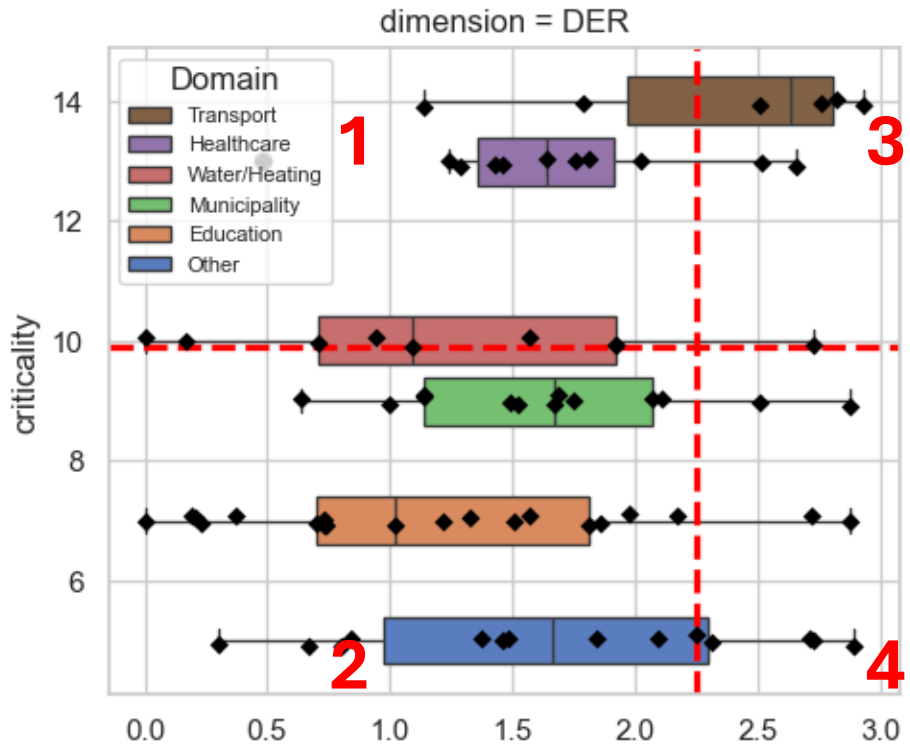
Policymaker	• Awareness, support measures, monitoring of changes
Supervisory	• Automatization, effectiveness
ENISA	• Awareness, comparability with oters (standardised sec. eval.)
Consultant	• Focuspoints, monitoring of changes
Organization	• Awareness, planning, benchmarking, replacement of audit?
Supplier	• Awareness, compliance, benchmarking

Policy maker: Education (2024)

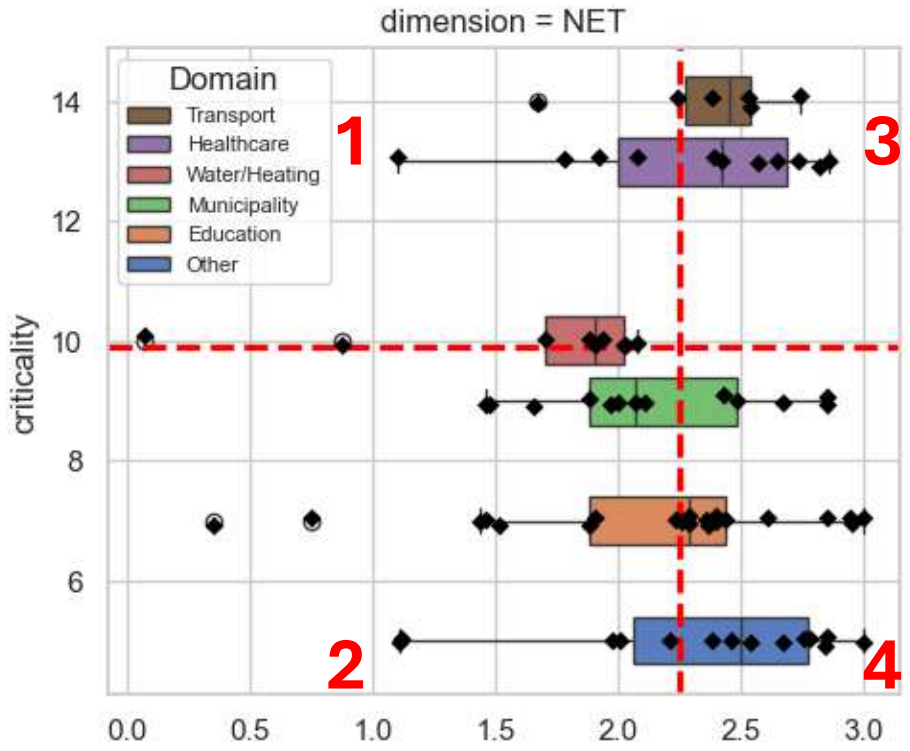




Supervisory

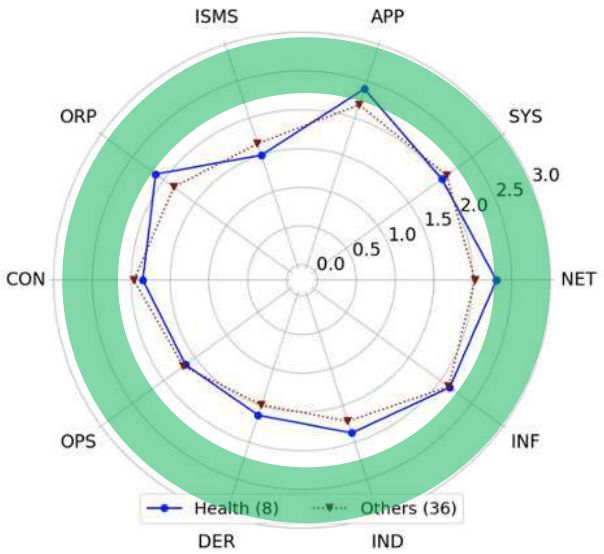


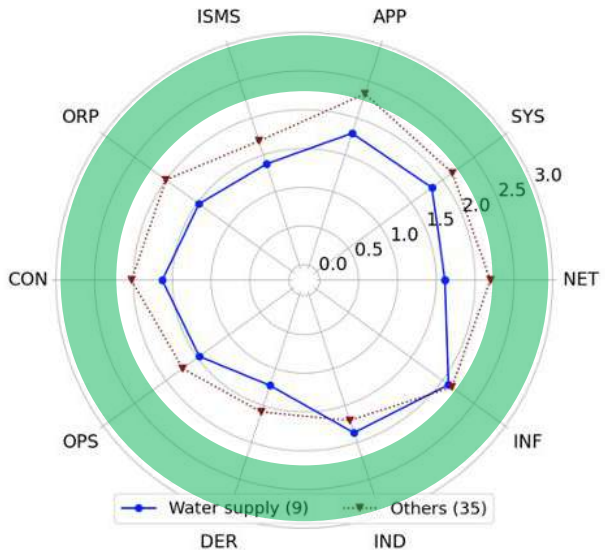
DER – Incident handling, forensics, auditid, exercises ja preparedness.

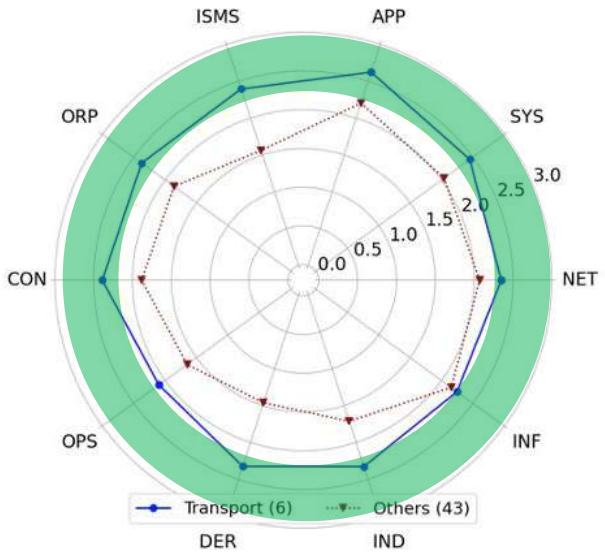


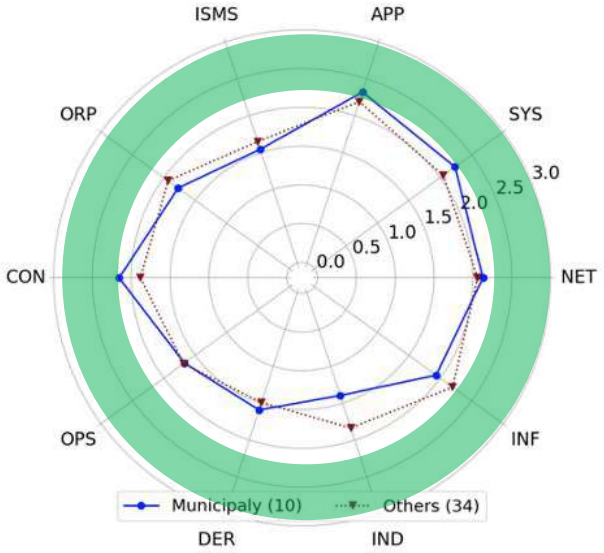
NET Network management.

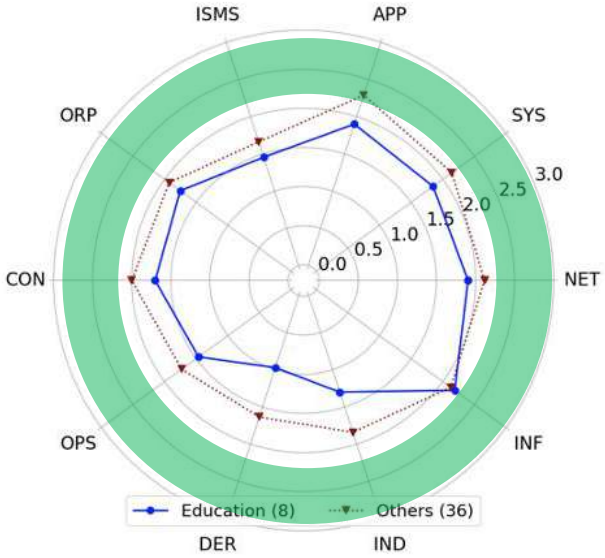
idee: ENISA

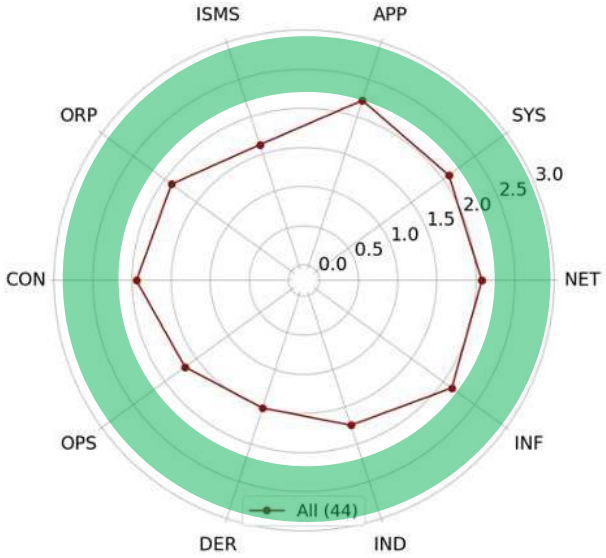

ISMS
APP
SYS
NET
INF
IND
DER
OPS
CON
ORP
0.0
0.5
1.0
1.5
2.0
2.5
3.0
Health (8)
Others (36)


ISMS
APP
SYS
NET
INF
IND
DER
OPS
CON
ORP
0.0
0.5
1.0
1.5
2.0
2.5
3.0
Water supply (9)
Others (35)


ISMS
APP
SYS
NET
INF
IND
DER
OPS
CON
ORP
0.0
0.5
1.0
1.5
2.0
2.5
3.0
Transport (6)
Others (43)


ISMS
APP
SYS
NET
INF
IND
DER
OPS
CON
ORP
0.0
0.5
1.0
1.5
2.0
2.5
3.0
Municipaly (10)
Others (34)


ISMS
APP
SYS
NET
INF
IND
DER
OPS
CON
ORP
0.0
0.5
1.0
1.5
2.0
2.5
3.0
Education (8)
Others (36)


ISMS
APP
SYS
NET
INF
IND
DER
OPS
CON
ORP
0.0
0.5
1.0
1.5
2.0
2.5
3.0
All (44)

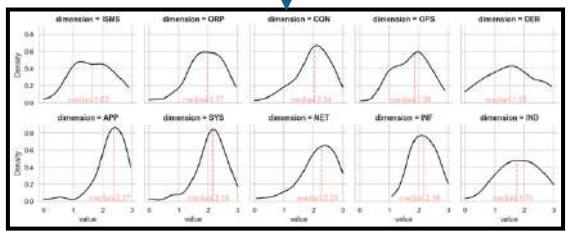
Policy maker

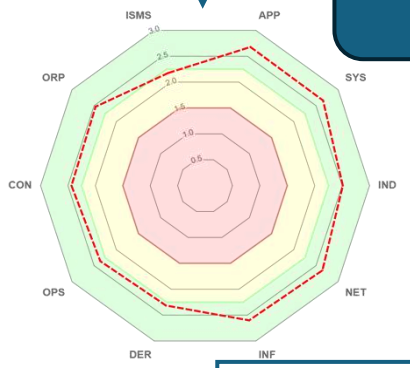
Supervisory

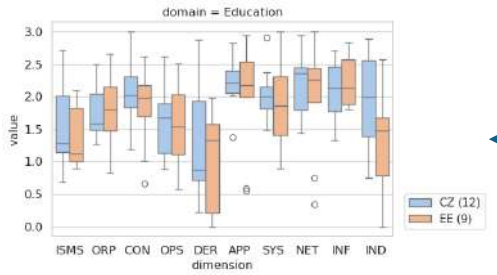
Organization

Consultant

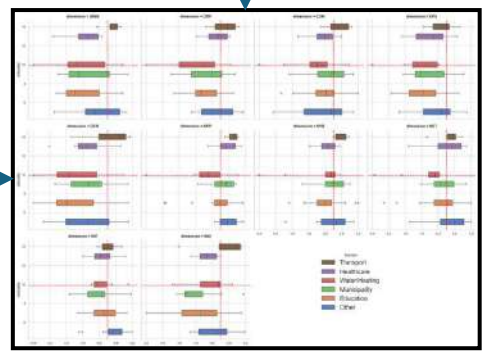
Supplier / Partner assessment

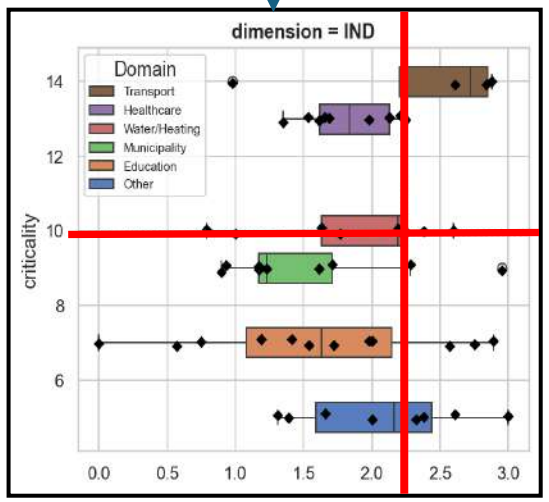


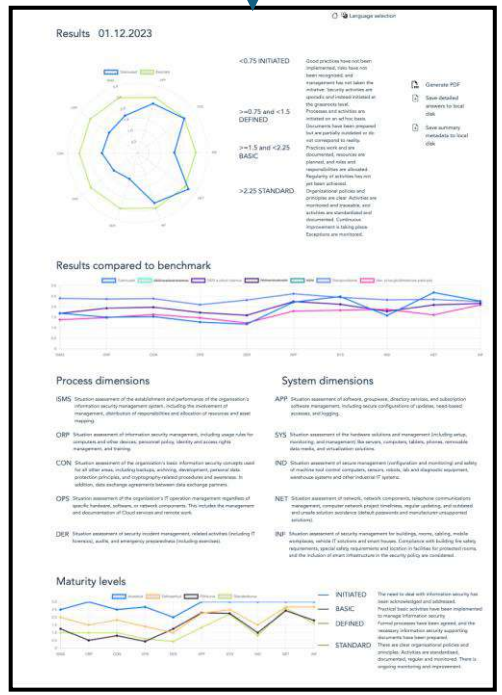




dimension	Czech Republic mean	median	std	Estonia mean	median	std
ISMS	1.59	1.5	0.657	1.66	1.66	0.695
ORP	1.82	1.67	0.396	1.94	2.05	0.652
CON	2.0	2.02	0.502	1.96	2.06	0.653
OPS	1.72	1.82	0.547	1.75	1.9	0.63
DER	1.34	1.02	0.866	1.59	1.64	0.797
APP	2.26	2.22	0.328	2.28	2.4	0.589
SYS	2.06	2.01	0.367	2.11	2.19	0.571
NET	2.17	2.36	0.522	2.15	2.24	0.652
INF	2.15	2.23	0.453	2.16	2.15	0.43
IND	1.95	2.0	0.733	1.79	1.71	0.688







Findings

- Immediate results to organizations
- Benchmarking - scalability
- Missing security vocabolary
- Missing statistical literacy – use of metadata
- Security evaluation instrument isn’t a standard
- Need for integration to other tools
- **Motivation**
- Reuse of the data – standardization, scalability

F4SLE- *Framework for Security level Evaluation*

- Preparatory work by choosing standard
  - *Seeba, M., Matulevičius, R., & Toom, I. (2021, July). Development of the Information Security Management System Standard for Public Sector Organisations in Estonia. BIS2021* https://doi.org/10.52825/bis.v1i.43
- framework and 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
  - *Seeba,M., Affia, A.-a.,O., Mäses, S., Matulevičius, R. (2024) Create Your Own MUSE: a Method for Updating Security Level Evaluation Instruments. Computer Standards & Interfaces* https://doi.org/10.1016/j.csi.2023.103776

MASS – presenting and collecting tool

- tool to present F4SLE and collect data: https://mass.cloud.ut.ee/massui/#/
- immidiate results to respondents and collecting privately aggregated results to central server
  - *Master thesis project of Maria Pibilota Murumaa. (2023)* Designing a tool for security level evaluation framework https://thesis.cs.ut.ee/92895428-9fc4-4248-bc78-4a00b3e90101

User Stories of Stakeholders

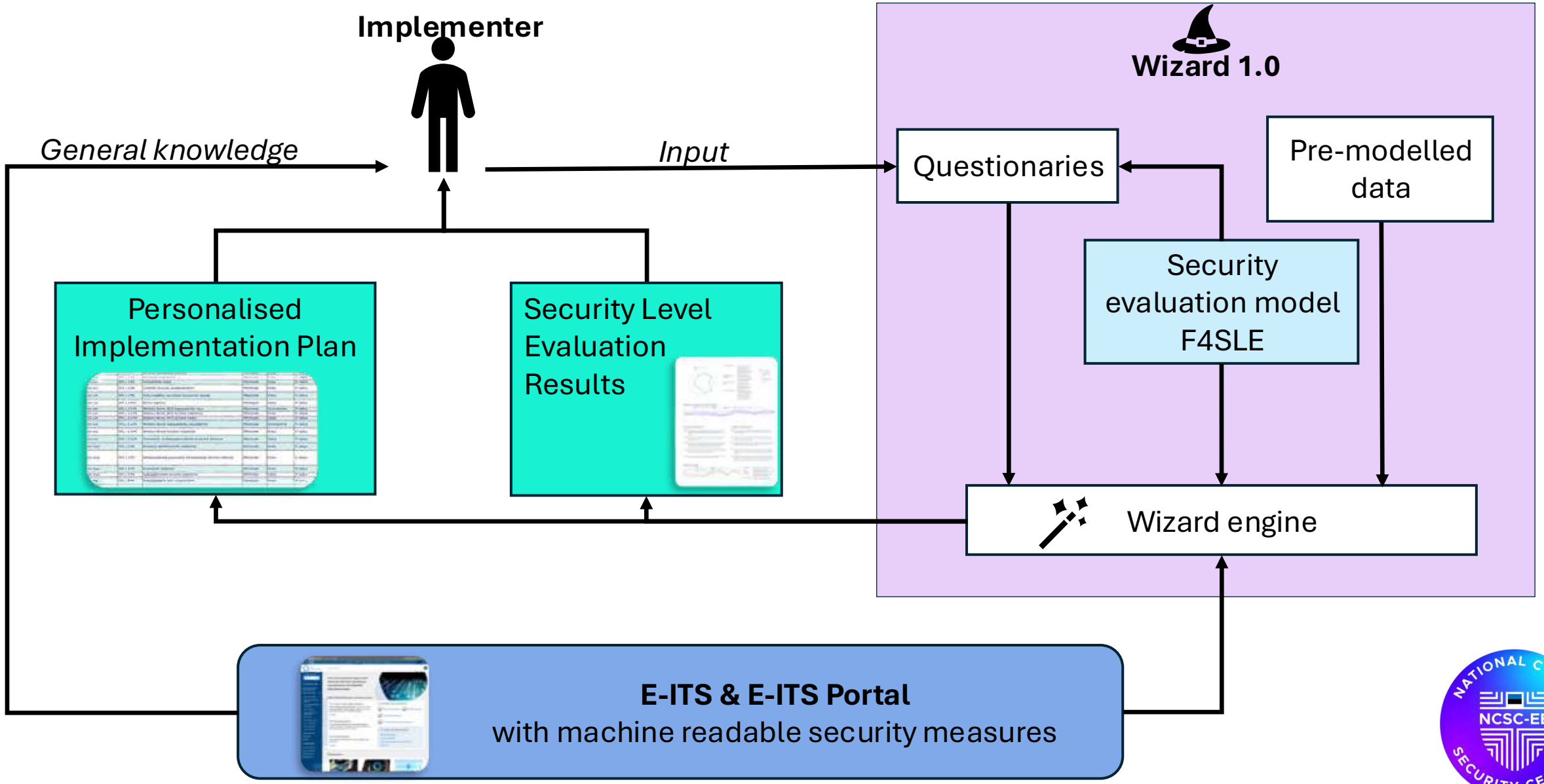
- Stakeholders who need security data of organisastions
- Collect data once and share with stakeholders
  - *Seeba, M., Oja, T., Murumaa, M., P., and Stupka, V. (2023). Security level evaluation with F4SLE. ARES2023* https://doi.org/10.1145/3600160.3605045
  - *Seeba, M., Valgre, M., Matulevičius, R. 2025. Evaluating Organization Security: User Stories of European Union NIS2 Directive* https://doi.org/10.1007/978-3-031-94569-4_4
  - *Seeba, M., Oja, T., Mäses, S., Murumaa, M. P., & Matulevičius, R. (2025). Toward NIS2 Compliance for Multiple Stakeholders with Security Level Evaluation Framework..* https://doi.org/10.7250/csimq.2025-45.07

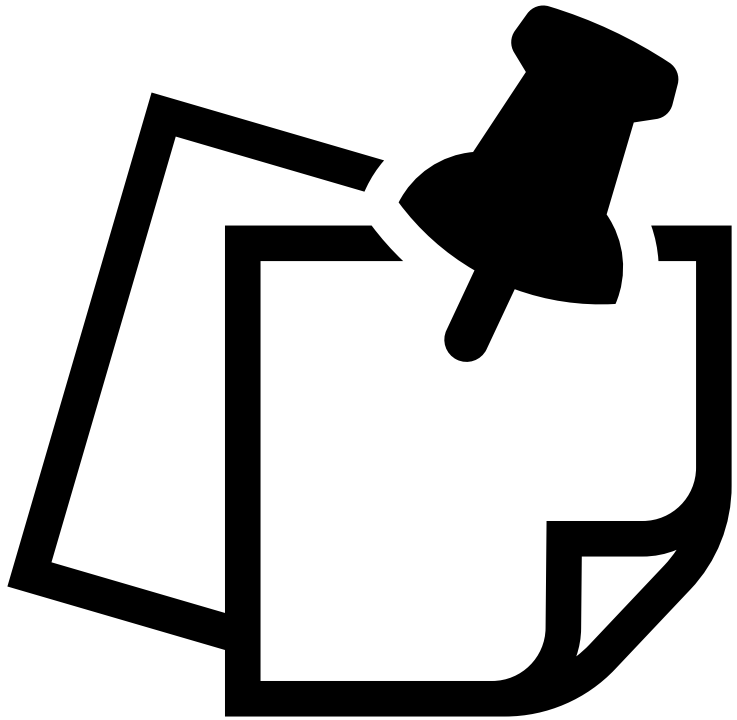
UNIVERSITY OF TARTU
Institute of Computer Science

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

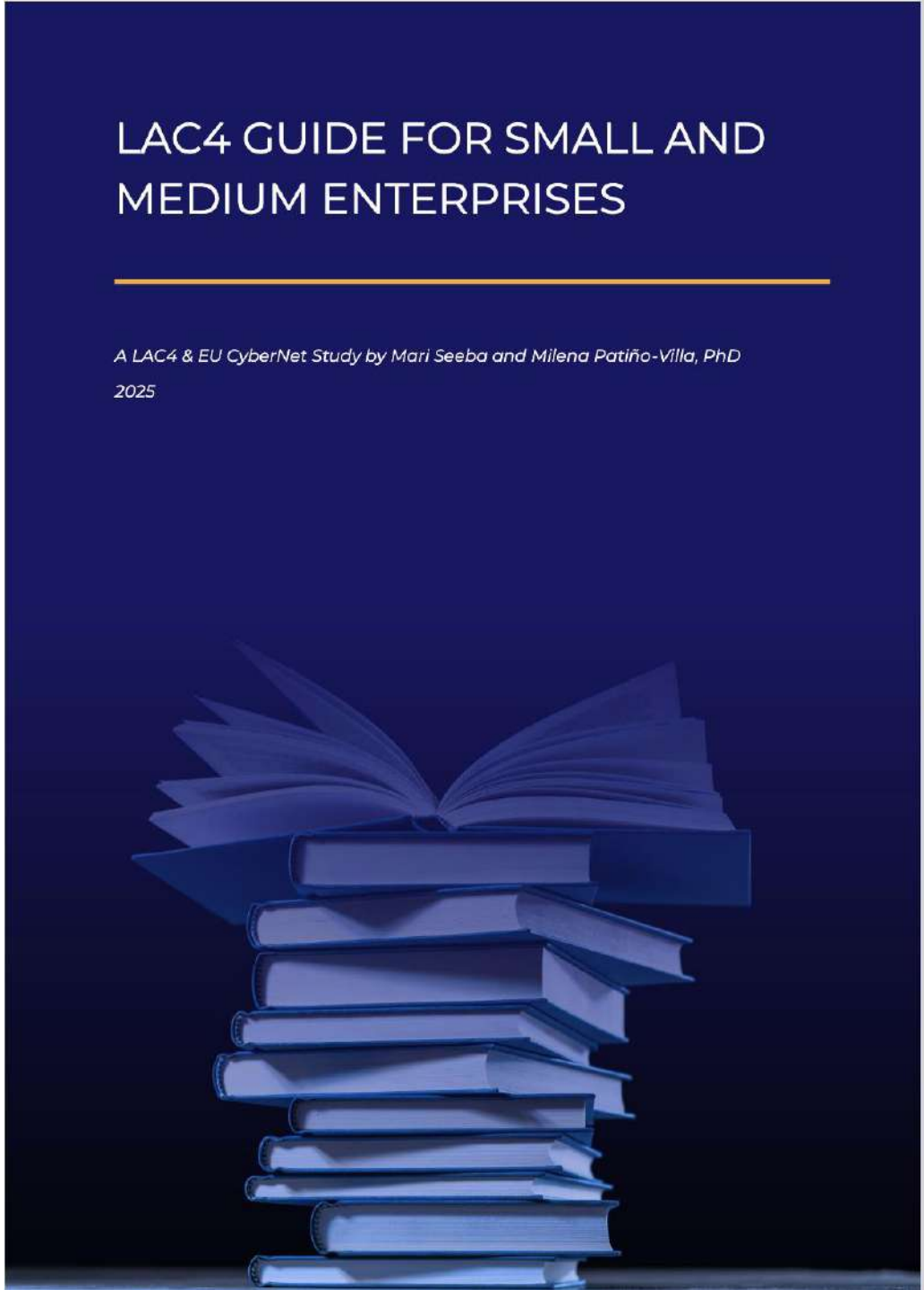
NATIONAL CYBER SECURITY CENTRE NCSC-EE

Next Milestone: Q2 2026





- Mari Seeba and Milena Patino-Villa (2025). A Practical Guide to Cybersecurity for SMEs
  - https://www.eucybernet.eu/wp-content/uploads/2025/09/guide-for-smes-lac4-2025-september-2025.pdf



We can’t measure security,
but we can evaluate, what we have done to be secure!

Thank you!

Mari.Seeba@ut.ee
Mari.Seeba@ria.ee

- AI
- GDPR
- NDA
- IoT
- Quality Management
- bitcoin
- deepfake
- risk
- classified
- CaaS

- Requirements Engineering
- NIS2
- C-I-A triangle
- OT
- OWASP
- d€
- MFA
- threat & vulnerability
- encrypted
- C(rime)aaS