UNIVERSITY OF TARTU
Institute of Computer Science

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Toward NIS2 Compliance for Multiple Stakeholders with Security Level Evaluation Framework

DOI: 10.7250/csimq.2025-45.07

Mari Seeba
Tarmo Oja
Sten Mäses
Maria Pibilota Murumaa
Raimundas Matulevičius

Idea

- **NIS2 Directive mandate:** common high security level across EU
- Multiple stakeholders request organizations to report their security status
- **Goal:** Optimize security evaluation to reduce administrative burden of organizations

Core principle:

"Collect data once and use it many times."

F4SLE: Framework for Security Level Evaluation

An instrument based on Estonian Information Security Standard (E-ITS), providing quatifiable and comparable results

10 security dimensions

ISMS APP
ORP SYS
CON NET
OPS IND
DER INF

4 maturity Levels

Initial – awareness
Basic – practical
Defined – documented
Standard – resilience

Method for updating the instrument (MUSE)

To ensure long-term data comparability to avoid security measures drift

Only aggregated data is collected centrally.

- *Seeba, M., Mäses, S., Matulevičius, R. (2022)*
- *Seeba,M., Affia, A.-a.,O., Mäses, S., Matulevičius, R. (2024)*

User Stories of Stakeholders

F4SLE operationalized **10 User Stories** of 6 key Stakeholder groups, providing one dataset can serve multiple needs.

Stakeholder	Primary Goal
Member State	Factual proof of achieving a high common level of cybersecurity in all sectors
Supervisory Authority	Planning supervisory tasks and optimize the workflow
Entity (Organization)	An overview of cybersecurity and improve vulnerable areas
Security Consultant	Improve the entity's security level by finding and focusing on vulnerable areas
ENISA	Collect data to evaluate the EU security level and report the result to the EU Parliament
Service Provider & Supplier	to share evaluation results with partners and assess compliance with partner requirements

- *Seeba, M., Valgre, M., Matulevičius, R. 2025.*

Results

Empirical testing

Usability evaluation in the perspective of efficiency, effectiveness and satisfactory of F4SLE (excluding UI)

284 Organizations

Estonia and EU 225
Central America 59

2 Security consultants

Finding vulnerable areas
Compliance with standards

Member State

(Estonian ministry)
Aggregated data by sectors

Conceptual testing

Supervisory Authority

Allows to prioritize task and optimize resources

ENISA

Admits the need for standardised instrument

Service Provider & Supplier

Organisations corfirm the need

Conclusion

- A unified framework can reduce burden of organizations
- External motivation is needed for organisations
- **Future work:** automated security checks to recude self-assessment bias and increase reliability

UNIVERSITY OF TARTU
Institute of Computer Science

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

References

Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. RCIS 2022 DOI: 10.1007/978-3-031-05760-1_39

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 DOI: 10.1016/j.csi.2023.103776

Seeba, M., Valgre, M., Matulevičius, R. 2025. Evaluating Organization Security: User Stories of European Union NIS2 Directive CAiSE 2025 DOI: 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.
Complex Systems Informatics and Modeling Quarterly DOI: 10.7250/csimq.2025-45.07

Mari Seeba (2026) A multi-stakeholder framework for comparable and repeatable security level evaluation in organizations. Dissretationes Informaticae Universitatis Tartuensis 84 https://hdl.handle.net/10062/121927

Thank you!

mari.seeba@ut.ee