



RIIGI INFOSÜSTEEMI AMET



UNIVERSITY OF TARTU
Institute of Computer Science



Eesti
Infoturbestandard

Development of information security management standard and evaluation instrument, Estonian case

Mari Seeba

NCSC-EE leading expert of cybersecurity, UT PhD student
mari.seeba@{ria|ut}.ee

2023/04/27

Agenda

- How to choose standard?
 - Seeba, Mari, Raimundas Matulevičius, and Ilmar Toom. "Development of the Information Security Management System Standard for Public Sector Organisations in Estonia." *Business Information Systems*. 2021.
- How to evaluate the standard compliance level?
 - Seeba, Mari, Sten Mäses, and Raimundas Matulevičius. "Method for Evaluating Information Security Level in Organisations." *Research Challenges in Information Science: 16th International Conference, RCIS 2022, Barcelona, Spain, May 17–20, 2022, Proceedings*. Cham: Springer International Publishing, 2022.
- MUSE – why we need method for updating security evaluation tool?
- MASS – tool and benchmarks to evaluate security (work in progress)
 - Security level evaluation intermediate results

Motivation

- Estonia has 1.33 million inhabitants
- Digital services via data exchange layer X-tee (Estonian instance of X-Road)
 - 3000 digital services
 - 225 million request per month via X-tee
- From 2004 since now Estonian public sector organisations use security framework ISKE
 - based on previous approach of BSI IT Grundschutz
 - BSI ITG changed their approach at 2017

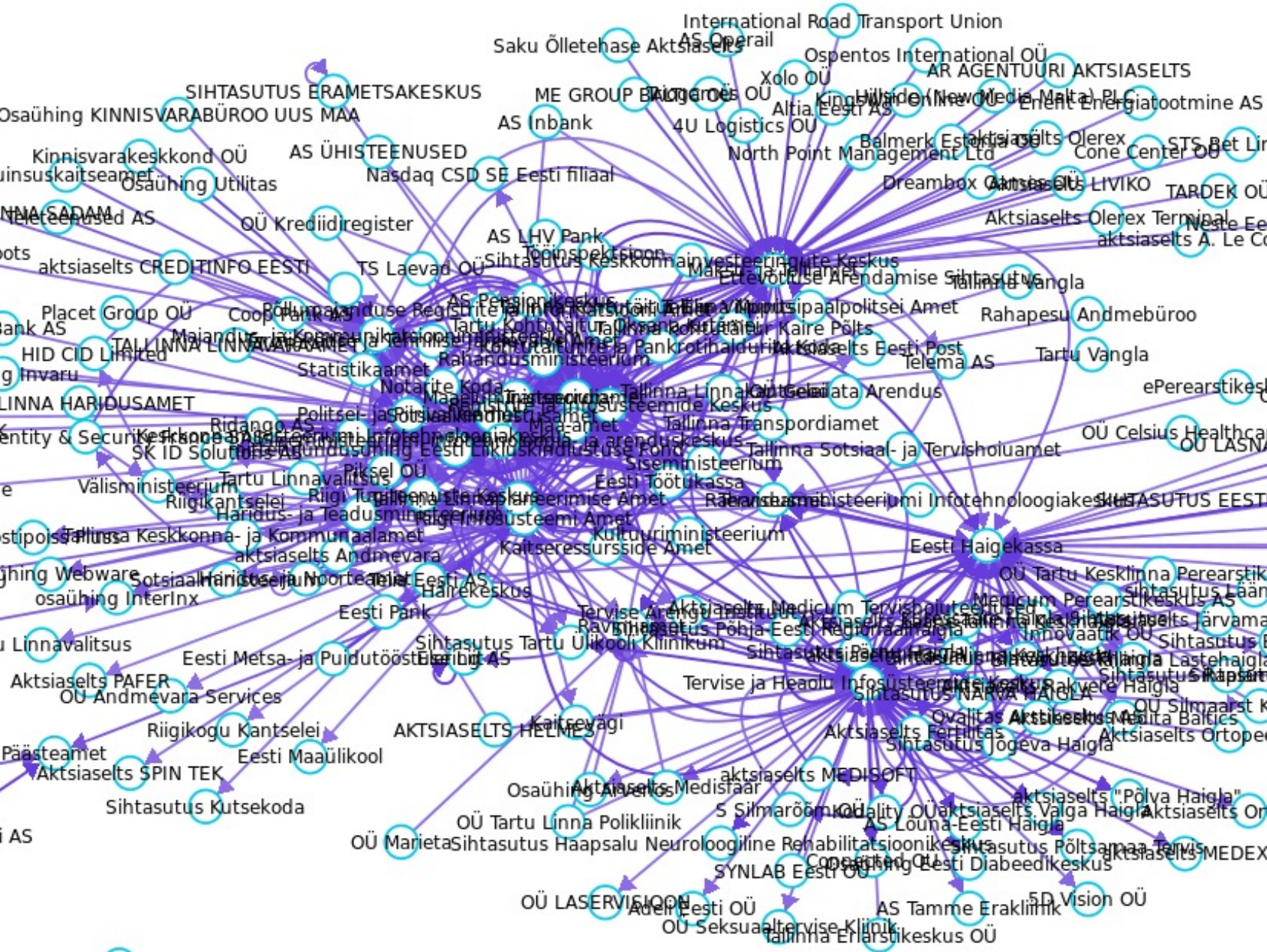


Fig. source: <https://abi.ria.ee/xtee/et/x-tee-juhend/x-tee-kasutusstatistika/x-tee-visualiseerija>

What should be the criterias or requirements of the information security management standard for public sector organisations?

- RQ1: How to find the national states requirements to the ISMS standard?
- RQ2: How to use these requirements when developing the national ISMS standard?

Requirements elicitation



Source: <https://ncsi.ega.ee/>

- NCSI database
- Cybersecurity strategies and implementation plans of EU countries
 - GR, CZ, LT, ES, BE, FI, SK, HR, FR, LV, PL, NL
- Requirements for security standard or guidelines
- Similar requirements aggregation (15 requirements)
- Requirements grouping into modules:
 - National Security module
 - Content Module
 - Assessment Module

Requirements elicitation results

National Security Module

- N1** Developer and Jurisdiction
- N2** Development financing
- N3** Licence conditions
- N4** Language
- N5** Update Cycle

Content Module

- C1** Scope
- C2** ISMS Compliance
- C3** Basic Controls
- C4** Leveled Controls
- C5** Risk Management Approach
- C6** Technology Dependence
- C7** Integrability of local needs
- C8** Controls Approach

Assessment Module

- A1** Auditability
- A2** Certification Schema





Requirements







































Req ID	Requirement	Requirement description	Country Code
National security module			
N1	Developer and jurisdiction	Standard should take into account EU and NATO regulations.	FI, GR, LT, HR
N2	Development financing	It should be possible to influence the development of the standard by national authority.	FI, GR, LT
N3	Licence conditions	Standard should be freely available to all national implementer.	FI, LT
N4	Language	Standard should be available in national language.	BE, GR, LT, LV
N5	Update cycle	Standards should be improved continuously/regularly.	BE, ES, GR, HR
Content module			
C1	Scope	Standard should be usable by public/private sector organisations information systems / processes / assets / critical infrastructure.	BE, CZ, ES, FI, GR, LT, LV, PL, SK, HR
C2	ISMS compliance	Standard should be compliant with internationally recognised standards / frameworks / best practices.	BE, CZ, ES, FI, FR, GR, LT, HR
C3	Basic controls	Standard should include basic/minimum security controls/measures.	BE, CZ, ES, FI, GR, LT, LV, PL, NL, HR
C4	Leveled controls	It should be possible to implement the standard controls/measures depending on the security level.	CZ, ES, FI, GR, LT, LV, PL, HR
C5	Risk management approach	Standard should include risk management.	BE, CZ, ES, GR, LT, LV, SK, HR
C6	Technology dependence	Standard should be technology-independent.	PL
C7	Integrability of local needs	It should be possible to adapt the standard with the national technological needs.	GR, PL
C8	Controls approach	It should be possible to change the content of the standard by national authority.	FI, GR, LT, PL
Assessment module			
A1	Auditability	Standard implementations should be auditable/assessable.	BE, CZ, ES, FI, GR, LV, PL, SK, HR, NL
A2	Certification Schema	Standard should be certifiable for being in compliance with recognized standards.	GR, PL, HR, NL

ISMS standards comparison example

Req ID	ISO27001	CIS20	BSI ITG
National security module			
N1	International Organisation (Switzerland), globally recognised	Centre for Internet Security (US based non-profit organisation), US industrial, wide adoption	Federal Office for Information Security (BSI) (Germany), German national EU jurisdiction
N2	National bodies participate in development and finance ISO. Sale of standards. [25]	Contributors: US agencies, commercial partners. Financing: donations, grants, paid programs, product sales [26]	Publicly reviewed contributions. Financing: German Gov.
N3	User based fee (also to translated versions)	Free for registered users, Creative Commons	Free download
N4	20+ languages	English, Spanish, Italian, Japanese, Lithuanian, Estonian	German, English
N5	5 year cycle	No exact rule, expectation is yearly update	Every February 1st
Content module			
C1	No limitations	No limitations	No limitations
C2	Officially compliant with ISO/IEC Management system standards, Management system standards adopted from Annex SL of ISO/IEC Directives, Consolidated ISO Supplement.	ISO 27001, NIST Framework [23]	ISO 27001
C3	Requirements mandatory, objectives with justified exclusions	User profile Implementation Group (IG) based basic requirements	Basic protection
C4	No	Three IG based levels	Standard and High level
C5	Mandatory. Guidelines: ISO/IEC 27005, ISO 31000	Guidelines: CIS RAM, ISO 27005, NIST SP 800-39, RISK IT (ISACA)	Embedded. Extension: BSI Standard 200-3: Risk Management
C6	No	No	User profile based technology modules
C7	Through risk management, local implementation	Through risk management, local implementation	Through risk management, central new technical modules development. Process modules are compliant to German regulations
C8	Control objectives (14) and controls (114). Related: ISO27000 series (50+ standards). Important: ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005	Security mode: 3 Implementation Groups. Controls (20), sub-controls (171). Related: CIS Controls TM, CIS RAM	Security mode: Basic, Standard, Core. Security catalogue: process and technical modules(5+5), Submodules (94), 1680+ requirements and measures in modules. Related: IT-Grundschutz Compendium; standards BSI 200-1, 200-2,200-3; BSI 100-4
Assessment module			
A1	External audit based on ISO 27007	Self-assessment or auditing based on ISO27001 or other standards	External audit
A2	Based on ISO 27006, ISO 27007, ISO 27008	No	Based on ISO27001 requirements and BSI methodology

Estonian Case

-  Most suitable
-  Suitable
-  Suitable with some exceptions
-  Not suitable

Req ID	Estonian Requirements	ISO27001	CIS20	BSI ITG
National security module				
N1	Standard should enable the baseline security to fulfil requirements of national and international regulations like GDPR, NIS-directive, etc. [17].			
N2	Standard should be flexible enough to add national content, measures or modules [19].			
N3	Standard should be available free of charge [19].			
N4	The standards must transfer Estonian language and culture, i.e. be in correct language, terminologically validated and compiled for Estonians [17, 18]. Correct language and consistent terminology should be used and validated [19].			
N5	Standard should be updated regularly/yearly [19, 17].			
Content module				
C1	Information security should be integrated widely in all type of organisations and their processes [17]. Standard should be extendable for all public administration and industry organisations [17]. Standard should support public sector business processes [19].			
C2	Standard should be based on an European or internationally recognised standards and practices [17, 6]. In case of a translation adoption, the standard should retain the connections with original document sets [19].			
C3	Standard should help optimising risk management by providing predefined measures for typical solutions [19].			
C4	Implementation process should enable levels of implementations - the base implementation and advanced levels based on security requirements [19].			
C5	Standard should use and adopt risk based approach for information and network security management [17].			
C6	All technologies should be given equal opportunities regardless of the platform [17].			
C7	The obligation to use Estonian based technological solutions. Therefore, the standards must enable and propagate the use of X-tee and Estonian public key infrastructure (PKI) solutions. [19]			
C8	Standard should be flexible enough to add national content, measures or modules [19].			
Assessment module				
A1	Standard should allow audit-ability [19].			
A2	-	-	-	-

- Limitations
 - Different detail and maturity level
 - Differences in requirements importance
- Conclusion
 - Reusable requirements to compare standards or guidelines
 - Each country has to do its decision by itself
 - Suggestion to ENISA to develop EU based security standard

Building blocks of security level evaluation

F4SLE- *Framework for Security Level Evaluation*

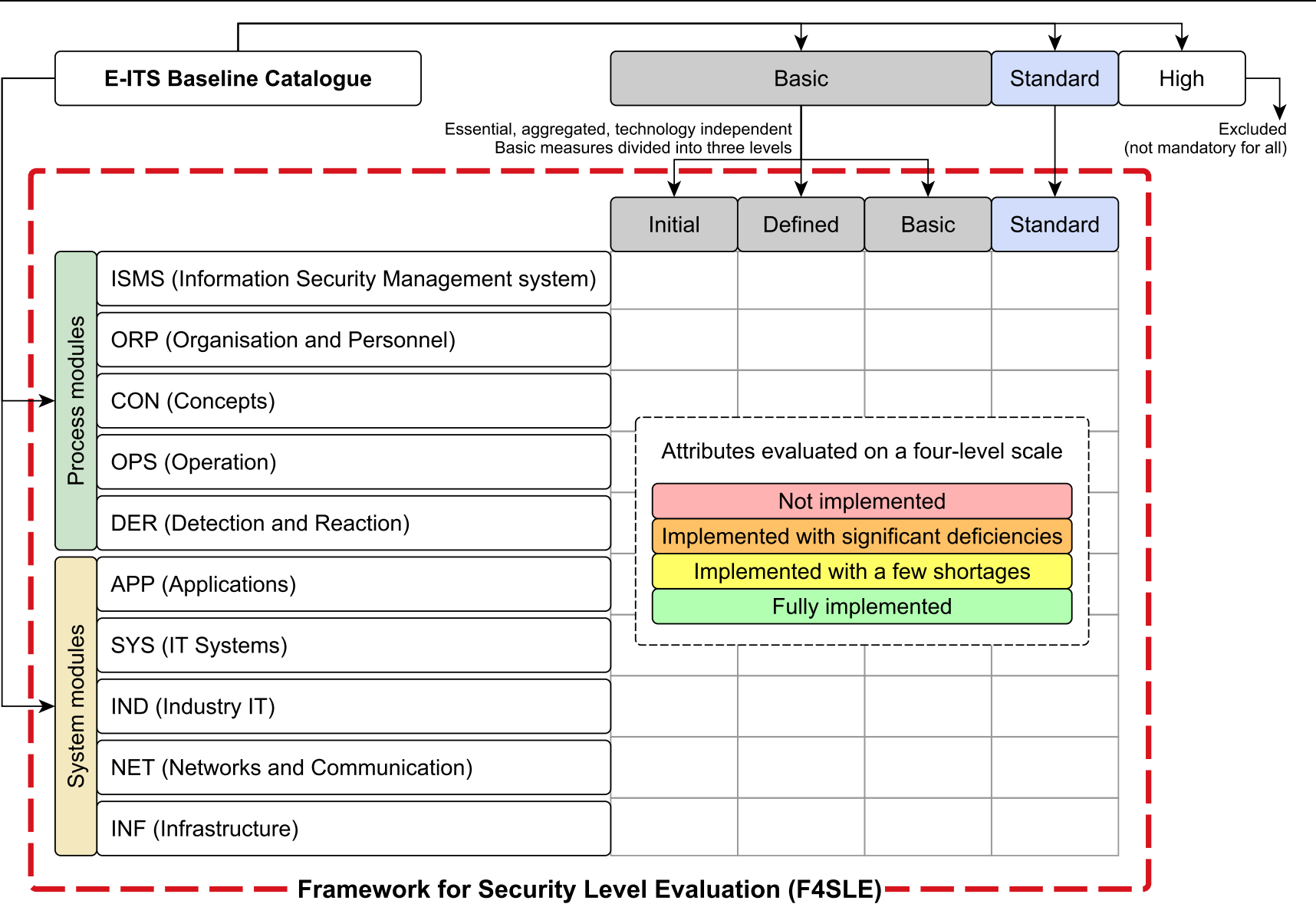
- framework and its principles
 - *Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. In: RCIS 2022. Lecture Notes in Business Information Processing, vol 446. Springer, Cham. https://doi.org/10.1007/978-3-031-05760-1_39*
- Content versions <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
 - *submitted manuscript: Seeba, M., Affia, A.-a., O., Mäses, S., Matulevičius, R. Create Your Own MUSE: a Method for Updating Security Level Evaluation Instruments*

MASS

- tool to use F4SLE
- *2023 Master thesis project of Maria Pibilota Murumaa “Designing a tool for security level evaluation framework”*
 - *CHES mini project*
- immediate results to respondents and sending the aggregated results to central server



- **INITIAL**
 - The need to deal with information security has been acknowledged and addressed
- **DEFINED**
 - Formal processes have been agreed, and the necessary information security supporting documents have been prepared
- **BASIC**
 - Practical basic activities have been implemented to manage information security
- **STANDARD**
 - There are clear organisational policies and principles. Activities are standardised, documented, regular and monitored. There is ongoing monitoring and improvement.

Method for Evaluating Information Security Level in Organisations

Mari Seeba¹, Sten Mäses² and Raimundas Matulevičius¹

¹University of Tartu, Institute of Computer Science, Tartu, Estonia
²Tallinn University of Technology, Department of Software Science, Tallinn, Estonia

TAL TECH

Research questions:
 How to evaluate the level of information security in the organisation?
 RQ1: What are the requirements of the security evaluation?
 RQ2: How to conduct the evaluation of security level?
 RQ3: How to use and interpret the results of information security evaluation?

Design science research method

Requirements for security evaluation framework

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

Req. 1: Framework should cover a wide area of security-related topics

- Procedural and technical measures.
- Comprehensive categories should still allow minor modifications or additions to the more specific topics as the technology evolves.
- Technology independent
- It should be possible to categorise any upcoming security control to an already existing category.

Req. 2: Framework should produce quantifiable and comparable

- Organisation security dynamics observation
- Evaluation should be based on evidence
- To compare different organisations between each other or against a security benchmark.

Req. 3: Framework should be quick and easy to implement and understand

- While the actual implementation of the security controls might take a long time, the evaluation should be intuitive to follow and take less than 1 hour.

Req. 4: Framework should be aligned with a security standard

- Following the standard structure helps to give the measurements a more coherent structure and avoids extra effort done to comply with the standard.

Information Security Evaluation Framework Design

Baseline standard
 We used the Estonian information security standard (E-ITS) [1] Baseline Catalogue (compliant with ISO27001)

Attributes of the Framework
 Respondent could find evidence for each attribute implementation status.

Dimensions of the framework
 Ten module groups of E-ITS:

- 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)

Example fragment of framework content

Framework with its full content is available at [2].

Baseline standard
 We used the Estonian information security standard (E-ITS) [1] Baseline Catalogue (compliant with ISO27001)

Dimensions of the framework
 Ten module groups of E-ITS:

- ISMS, ORP, CON, OPS, DER are procedural,
- INF, NET, SYS, APP, IND are system based technical modules.

Framework levels
 E-ITS measures are ordered Basic, Standard and High. Exclusion of High to include only mandatory part. E-ITS Basic divided into three levels:

- Initial Level** - organisation solves its security *ad hoc* and on a need-based
- Defined Level** - formal compliance documentation requirements
- Basic level** - processes taking place

Standard level - equals with E-ITS Standard security measures. Allows the organisation to deal with unknown risks by significantly reducing their potential impact and loss.

Information Security Evaluation Framework Design

E-ITS Baseline Catalogue

Essential, aggregated, technology independent
 Basic measures divided into three levels (not mandatory for all)

Attributes of the Framework
 Respondent could find evidence for each attribute implementation status.

Attributes evaluated on a four-level scale

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

Information Security Evaluation Framework

Attributes of the Framework
 Respondent could find evidence for each attribute implementation status.

Evaluation scale for attributes
 Four-level scale

- quantifies the dynamics of organisation security even in the case of minor changes
- forces the respondent to decide whether the situation is somewhat positive or rather negative.

Example fragment of framework content

	Initial level	Defined level	Basic level	Standard level
DER Detection and response	55. When a security incident is reported, it is responded to according to agreed rules.	57. A channel shall be established for the notification of security events and all security events shall be registered in the register of security events.	61. The critical network segments are defined and monitored.	67. Regular inspections of detection systems are carried out and automatic alarms are implemented where possible.
APP Applications	56. The obligation to audit information security incidents is recognized.	58. A fact aid guide for a security incident has been developed.	64. ...	69. ...
SYS (IT Systems)	59. ...	60. ...	65. ...	70. Attributes

Framework with its full content is available at [2].

Interpretation Use Cases

Use case 0
 The organisations used the indicated table to interpret organisation security using traffic light colours and the dominant visual colour to indicate the current security status before calculations.

Use case 1
 Then average result of the organisation by each dimension and maturity level Fig 1. Colours transferred into quantifiable form:

Use case 2
 The sum each level's average value by dimension to get the information security level of organisation by dimensions (Fig 2, blue line).

Use case 3
 The average value of information security level by dimension based on all organisations for the benchmark (Fig 2, red line).

Use case 4
 The benchmark usage as an input for state-level political and strategic decisions.

Demonstration and evaluation

Limitations

- For benchmark validation bigger reference group is needed
- Self-assessment or third party assessment or partly automated?
- Benchmark tool and falsification threat
- Updating responsibility - clear criteria
- Difficulties with interpretation - need to know the dimensions content
- Generalisation difficulties

Interpretation Use Cases

Use case 0
 The organisations used the coloured table to interpret organisation security using traffic light colours and the dominant visual colour to indicate the current security status before calculations.

Use case 1
 Then average result of the organisation by each dimension and maturity level Fig 1. Colours transferred into quantifiable form:

Use case 2
 The sum each level's average value by dimension to get the information security level of organisation by dimensions (Fig 2, blue line).

Use case 3
 The average value of information security level by dimension based on all organisations for the benchmark (Fig 2, red line).

Use case 4
 The benchmark usage as an input for state-level political and strategic decisions.

Figure 1. An organisation's security levels

Interpretation Use Cases

Use case 0
 The organisations used the coloured table to interpret organisation security using traffic light colours and the dominant visual colour to indicate the current security status before calculations.

Use case 1
 Then average result of the organisation by each dimension and maturity level Fig 1. Colours transferred into quantifiable form:

Use case 2
 The sum each level's average value by dimension to get the information security level of organisation by dimensions (Fig 2, blue line).

Use case 3
 The average value of information security level by dimension based on all organisations for the benchmark (Fig 2, red line).

Use case 4
 The benchmark usage as an input for state-level political and strategic decisions.

Figure 2. Comparison with benchmark

Interpretation Use Cases

Use case 0
 The organisations used the coloured table to interpret organisation security using traffic light colours and the dominant visual colour to indicate the current security status before calculations.

Use case 1
 Then average result of the organisation by each dimension and maturity level Fig 1. Colours transferred into quantifiable form:

Use case 2
 The sum each level's average value by dimension to get the information security level of organisation by dimensions (Fig 2, blue line).

Use case 3
 The average value of information security level by dimension based on all organisations for the benchmark (Fig 2, red line).

Use case 4
 The benchmark usage as an input for state-level political and strategic decisions.

Figure 2. Comparison with benchmark

References:

[1] RIA (Estonian Information System Authority): E-ITS. <https://eits.ria.ee/>

[2] Seeba, M., Estonian Information Security Standard (E-ITS) Based Security Level Evaluation Instrument (2021). <https://doi.org/10.23673/re-298>

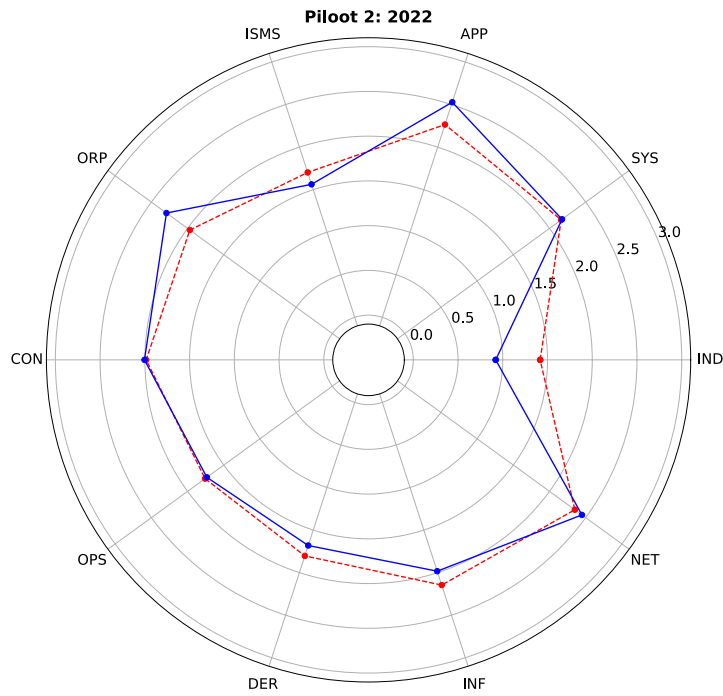
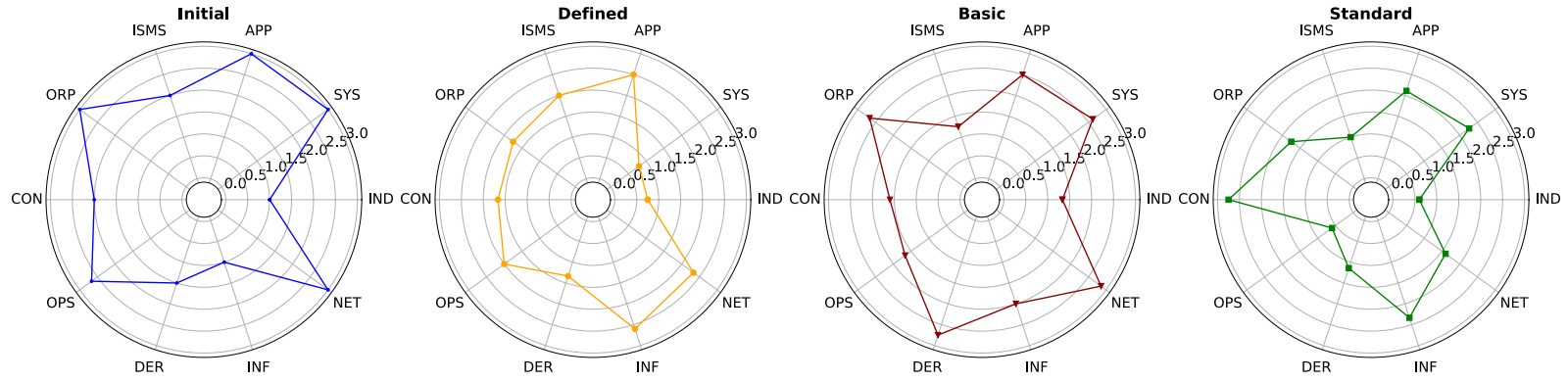
Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. In: RCIS 2022. Lecture Notes in Business Information Processing, vol 446. Springer, Cham. https://doi.org/10.1007/978-3-031-05760-1_39

Demonstration and evaluation

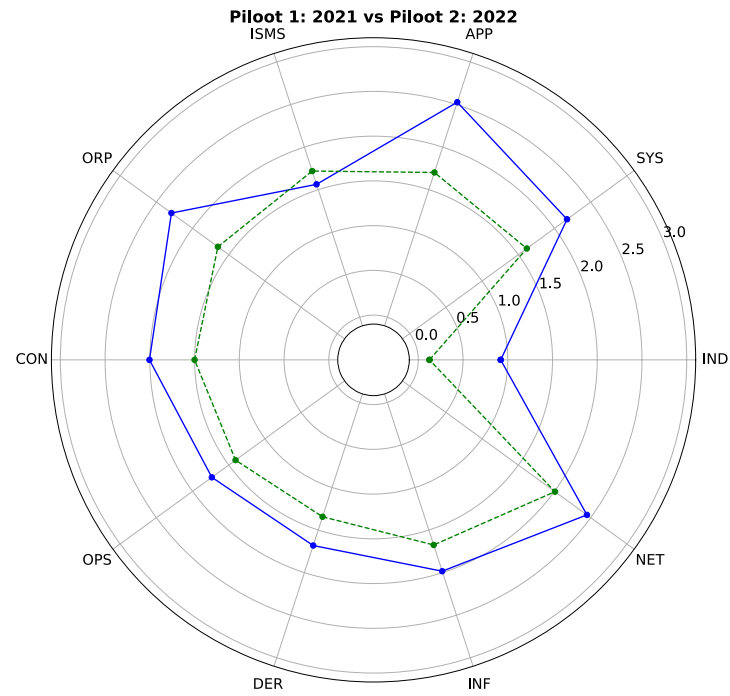
Limitations

Limitations

C22



- - - Benchmark Pilot 2: 2022
- - - Organisation security level Pilot 2: 2022



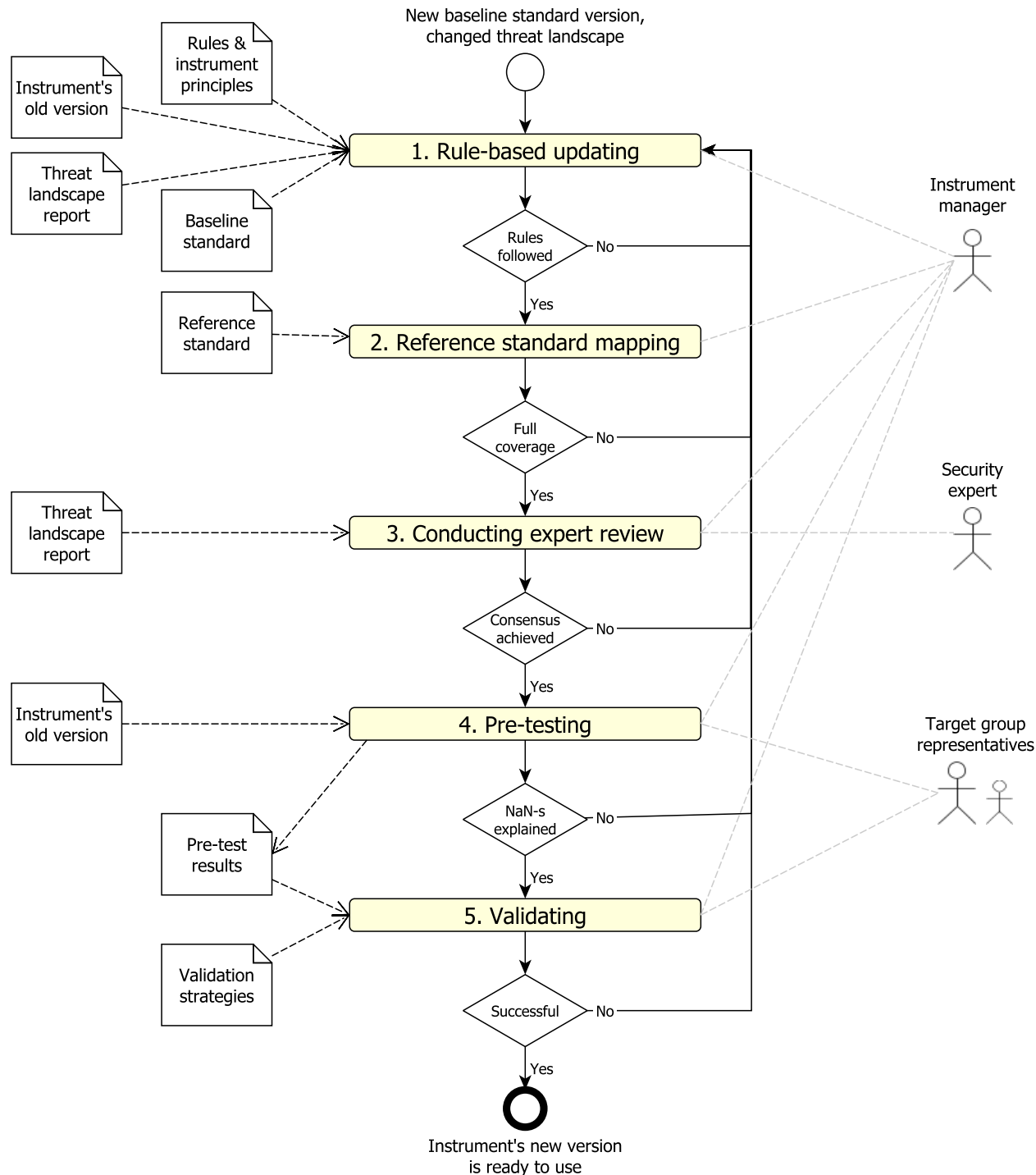
- - - Organisation security level Pilot 2: 2022
- - - Organisation security level Pilot 1: 2021

How to update security level evaluation instrument attributes in a way that

- results are comparable
- in long-term for all use cases
 - organisation level,
 - benchmark providing,
 - central view?

Method to update security evaluation instrument

MUSE



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

MS Word



MS Excel



MASS Tool

MASS – web based tool to simplify F4SLE usage

- Privacy principle – raw data does not leave from the respondent
- Only aggregated data will be sent to the server
- Immediate results to respondent
- Benchmark creation based on aggregated data

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

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



RIIGI INFOSÜSTEEMI AMET



TARTU ÜLIKOOL
arvutiteaduse instituut

0/189

APP - Rakendused

Olukorra hinnang tarkvara, rühmatarkvara, kataloogiteenuste ja tellimustarkvara haldamisele, sh nende uuendamised turvalised seadistamised, vaid vajaduspõhised juurdepääsud, logimine.

1. Rakenduste kasutuselevõtul jälgitakse rakendustele antavaid õigusi ja neid piiratakse.

① Lisainfo

Väites kirjeldatud olukorra jaoks ei ole veel midagi olulist tehtud

Väide on osaliselt vastav olukorra kirjeldusele, kuid siiski oluliste puudustega

Väide on kooskõlas sinu organisatsiooniga, kuid mõningate puudustega

Väide vastab sinu organisatsiooni kontekstis täielikult tõele

Jätan vastamata

Ei kehti

2. Rakendusi, rühmatarkvara ja kataloogiteenusid on lubatud hallata vaid selleks määratud administraatoril.

① Lisainfo

Väites kirjeldatud olukorra jaoks ei ole veel midagi olulist tehtud

Väide on osaliselt vastav olukorra kirjeldusele, kuid siiski oluliste puudustega

Väide on kooskõlas sinu organisatsiooniga, kuid mõningate puudustega

Väide vastab sinu organisatsiooni kontekstis täielikult tõele

Jätan vastamata

Ei kehti

3. Kahjurvaravastast tarkvara kasutatakse e-posti serverites rämpposti ja pahatahtliku sisu tuvastamiseks sissetulevates ja väljaminevates e-kirjades ning e-posti manustes.

① Lisainfo

Väites kirjeldatud olukorra jaoks ei ole veel midagi olulist tehtud

Väide on osaliselt vastav olukorra kirjeldusele, kuid siiski oluliste puudustega

Väide on kooskõlas sinu organisatsiooniga, kuid mõningate puudustega

Väide vastab sinu organisatsiooni kontekstis täielikult tõele

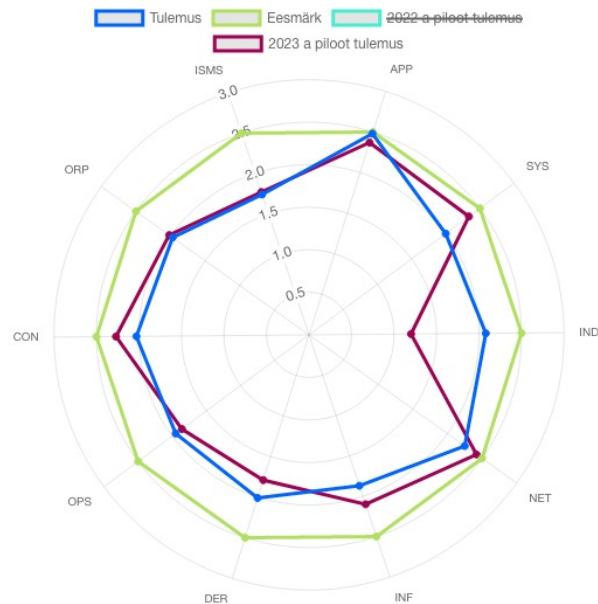
Jätan vastamata

Ei kehti

4. Kataloogiteenustele (directory service) on kehtestatud reeglid.

① Lisainfo

Tulemused võrreldes mõõtlusalusega



<0.75 ALUSTATUD

Head praktikaid pole rakendatud, riske pole teadvustatud, juhtkond pole initsiatiivi võtnud. Turvetegevused on juhuslikud ja pigem algatatud rohujuure tasandil.

>=0.75 ja <1.5 DEFINEERITUD

Protsessid ja tegevused on alustatud, kui toimuvad ad hoc. Dokumendid on koostatud, kuid osaliselt vananenud või ei vasta tegelikkusele.

>=1.5 ja <2.25 PÕHITURVE

Praktikad toimivad, on dokumenteeritud, ressursid plaanitud, rollid ja kohustused jaotatud. Tegevuste regulaarsus pole veel saavutatud.

>2.25 STANDARDTURVE

On selged üle organisatsioonilised poliitika ja printsiibid. Tegevusi seiratakse ja need on jälgitavad, tegevused on standardiseeritud ja dokumenteeritud. Toimub pidev parendamine. Erandeid seiratakse.

CON Olukorra hinnang asutuse infoturbe aluskontseptsioonidele, mida kõik muud teemavaldkonnad kasutavad, sh varundamiste, arhiveerimiste, arendustööde korraldus, isikuandmete kaitse põhimõtted ja krüptograafiaga seotud protseduurid ning teadlikkus, lisaks ka andmevahetuspartnerite andmevahetuskokkulepped.

ORP Olukorra hinnang infoturbe korralduslikule poolele, sh arvutite ja muude seadmete kasutamisega seotud reeglid, personalipoliitika, identiteedi- ja pääsuõiguste haldus ning koolitused.

ISMS Olukorra hinnang infoturbe halduse süsteemi loomisele ja korraldusele asutuses, sh juhtkonna kaasatus, vastutuste jaotus ja ressursside eraldamine, varade kaardistus.

APP Olukorra hinnang tarkvara, rühmatarkvara, kataloogiteenuste ja tellimustarkvara haldamisele, sh nende uuendamised turvalised seadistamised, vaid vajaduspõhised juurdepääsud, logimine.

SYS Olukorra hinnang riistvaralistele lahendustele nagu serverid, arvutid, tahvlid, telefonid, irdandmekandjad, virtuaalseerimislahendused ja nende haldamine (sh seadistus ja seire toimimine ning korraldus).

IND Olukorra hinnang tööpinkide juhtarvutite, sensorite, robotite, labori- ja diagnostikaseadmete, laosüsteemite jms tööstuse IT ja automaatika turvalisele haldamisele (seadistused ja seire) ning ohutusele.

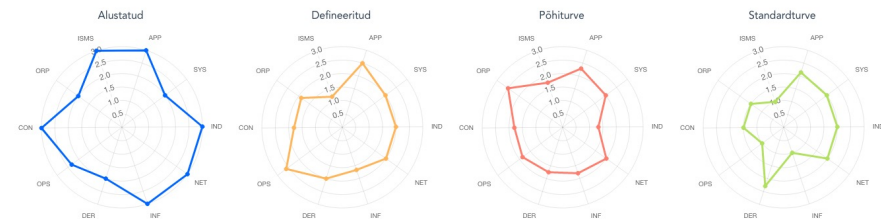
NET Olukorra hinnang võrgu, võrgukomponentide ja telefonise haldamisele, arvutivõrgu projektide ajakohasusele, regulaarsele uuendamisele ja vananenud ning ebaturvaliste lahenduste vältimisele (algsarvutid ja tootja toeta lahendused).

INF Olukorra hinnangu hoonete, ruumide, kaabelduste, mobiilsete töökohtade, sõidukite IT lahenduste, sh tarkade majade haldamisele turbe seisukohast. Arvesse võetakse hoonete tuleohutusnõuete täitmist, kaitstavate ruumide erivajadusi ja asukohta ruumiplaneeringus ning nutitaristu lülitamist asutuse ülese turvapolitiika koosseisu.

DER Olukorra hinnang turvaintsidentide haldusele, seotud tegevustele (sh IT kriminalistika), auditite läbiviimisele ja valmisolek avariidega toimetulemiseks (sh nendega seotud õppused).

OPS Olukorra hinnang asutuse IT käitamise haldamisele sõltumata konkreetsest riist- või tarkvarast ja võrgus komponendist. Siia kuulub ka pilvteenuste ja kaugtöö haldamise ja dokumenteerimisega seonduv.

Organisation result



ALUSTATUD Infoturbe tegelemise vajadus on teadvustatud ja sellega tegeletakse.

PÕHITURVE Rakendatud on praktilised tegevused infoturbe haldamiseks.

DEFINEERITUD Kokku on lepitud formaalsed protsessid ja koostatud vajalikud infoturvet toetavad dokumendid.

STANDARDTURVE On selged üle organisatsioonilised poliitika ja printsiibid. Tegevused on standardiseeritud, dokumenteeritud, regulaarselt ja jälgitavad. Toimub pidev seire ja parendamine.

What to do with the results?

- Preparing for audit
 - Input to security implementation plan, priorities
 - Management review input
 - Security dynamics monitoring
 - Understanding the standard
- Partners assessment (sh X-tee teenused)
 - Partner self-assessment / auditor tool
- Central analysis
 - Industry based benchmark
 - Input to plan supporting activities
 - Monitor the changes

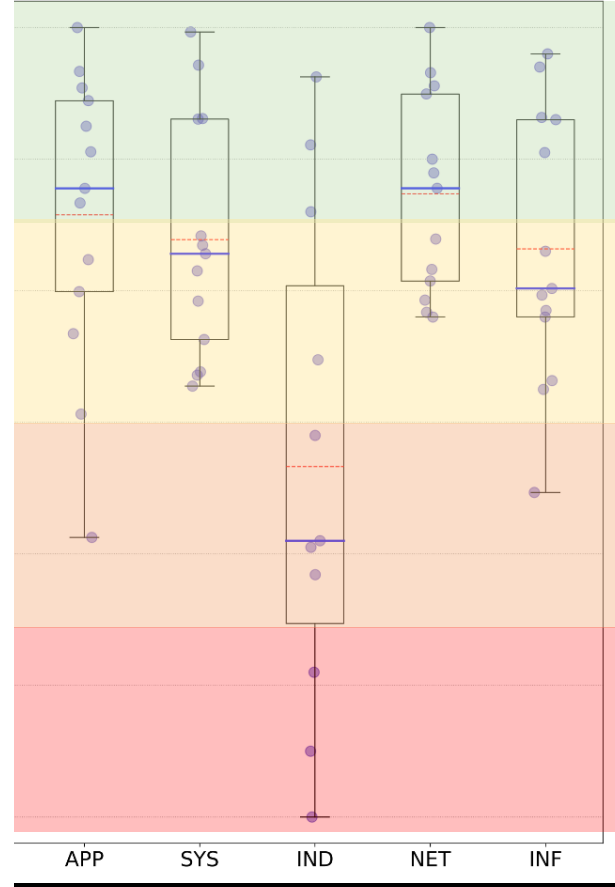
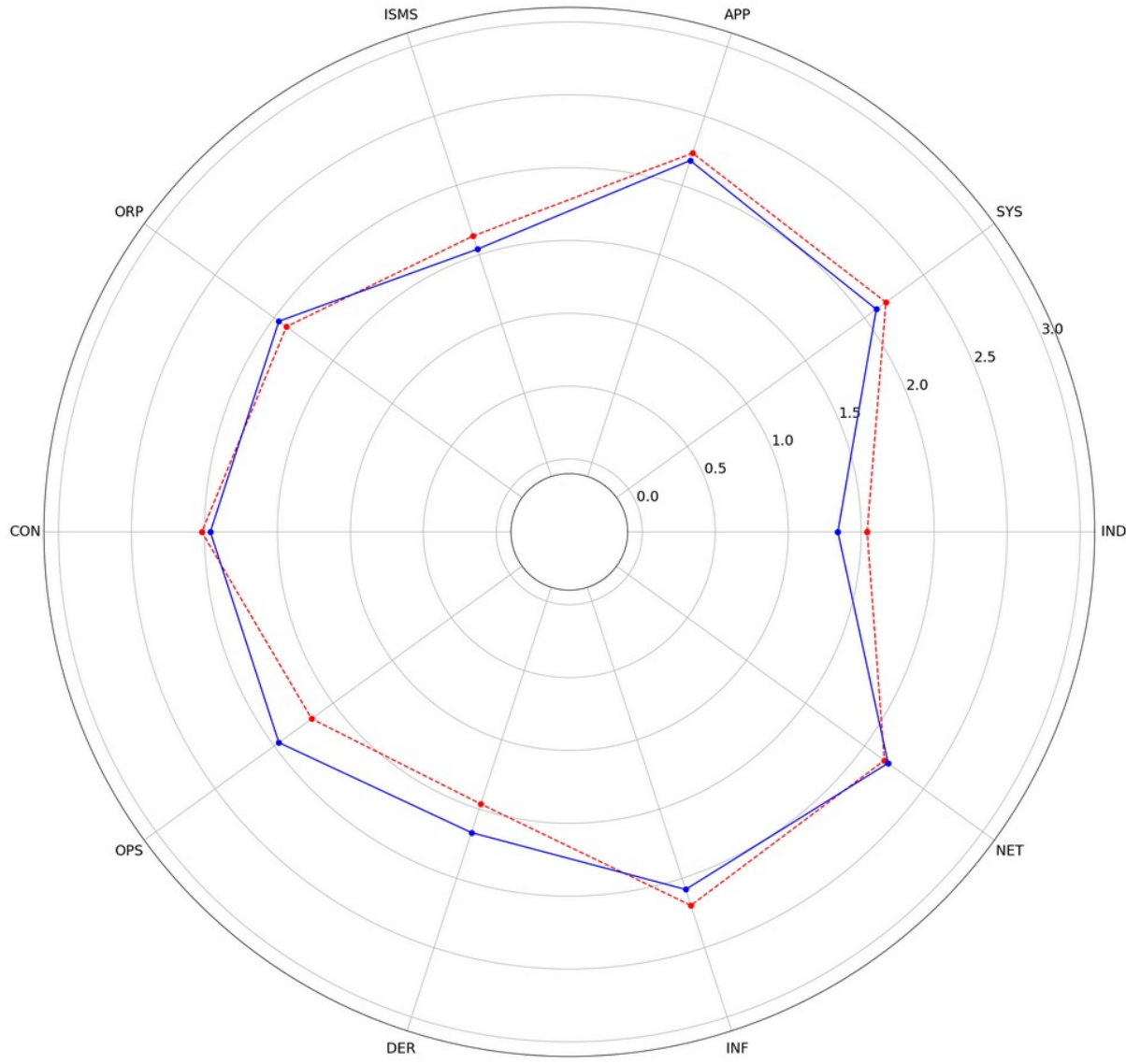
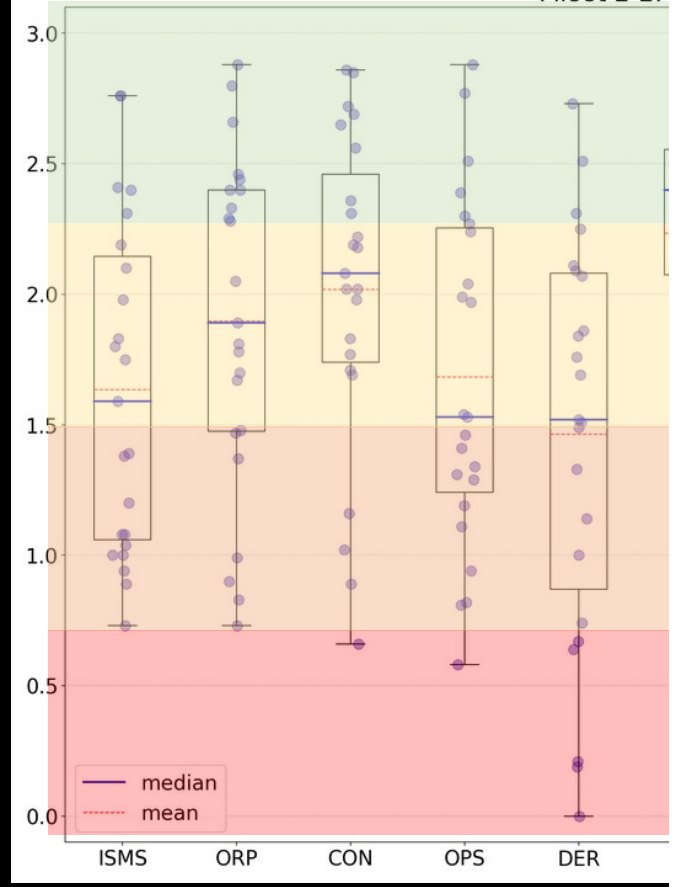
PILOOT 2/2

Benchmark comparison

2022

Pilot 2-2:

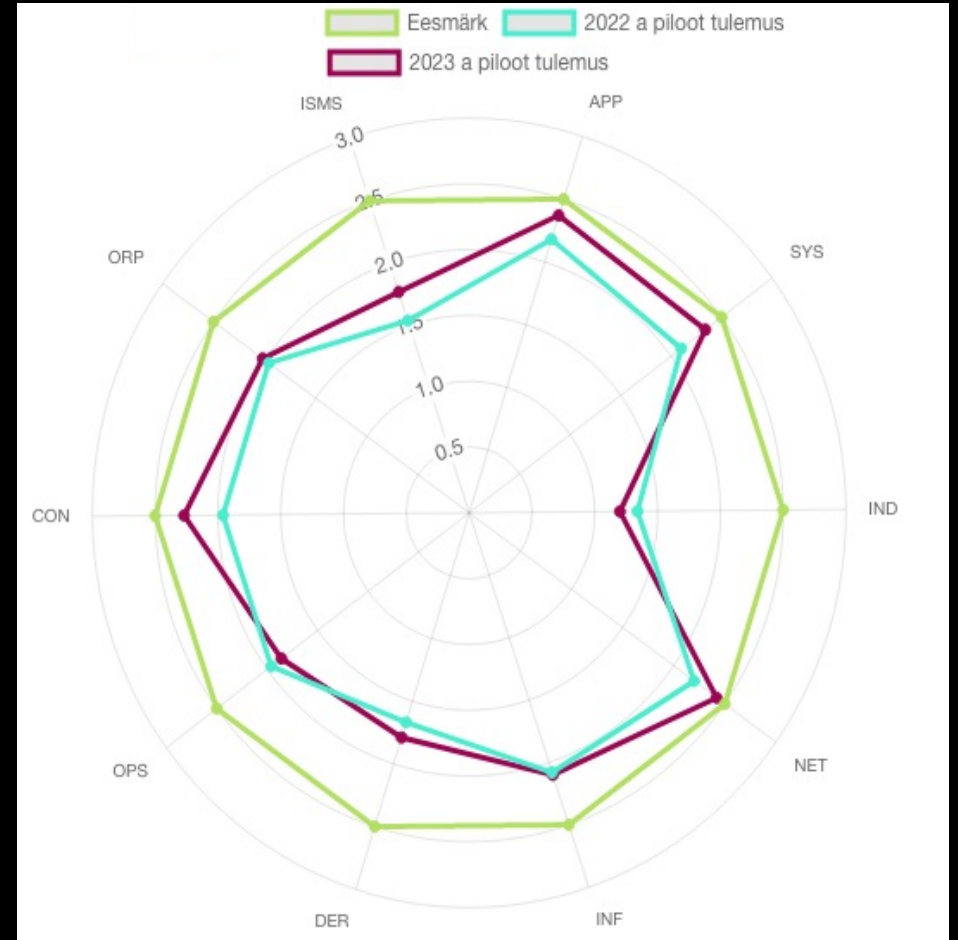
2: 2022



--- Benchmark Pilot 2-2: 2023
— Benchmark Pilot 2022

Conclusion

- Requirements of choosing standard
- Implementing requires evaluation
- Evaluation instrument needs updating
- Estonian case

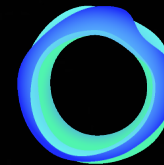




RIIGI INFOSÜSTEEMI AMET



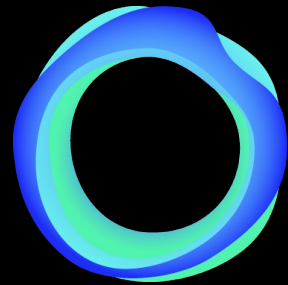
TARTU ÜLIKOOL
arvutiteaduse instituut



Eesti
Infoturbestandard

Thank you!

Mari.Seeba@{ria|ut}.ee



Eesti
Infoturbestandard