RIIGI INFOSÜSTEEMI AMET

Eesti
Infoturbestandard

Estonian Information Security Standard

Ilmar Toom

Head of Supervisory Department

Estonian Information System Authority

2022

Agenda

- History and Reasoning
- E-ITS build-up
- Implementation and supervisory
- Legal aspects
- Future challanges

Timeline

Eesti Infoturbestandard

2003 – first version of Estonian security baseline - called ISKE, based on 2003 English version of the BSI ITG

2004 – ISKE implementation legal act for public sector registries

2018 – last update of ISKE

2019 – E-ITS development based on BSI ITG 2019/2020

2020 – First version of E-ITS published in the eits.ria.ee, first implementation tool (public-private partner), trainings, pilot project, E-ITS maturity model design**

2022 – E-ITS regulation, second version, profiles, trainings

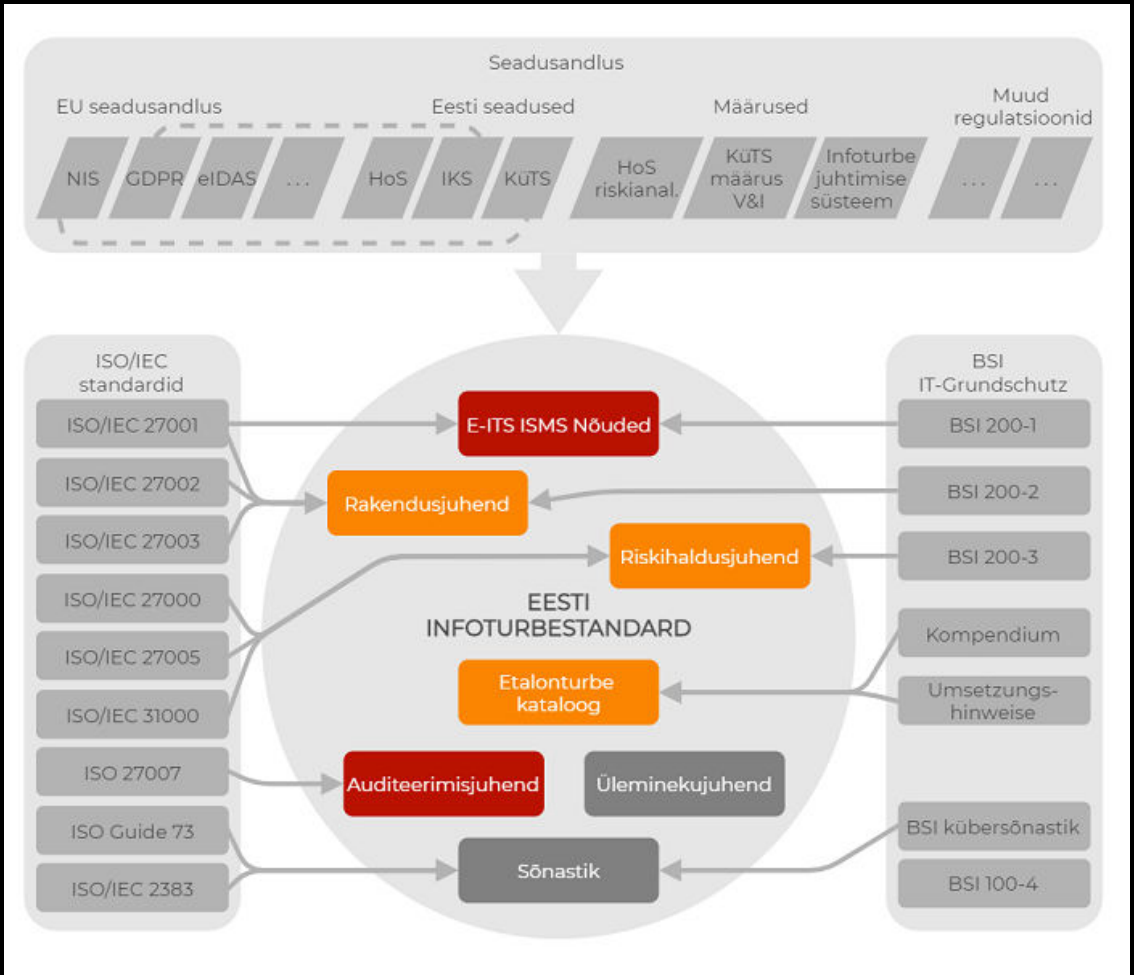
**Tool content: Seeba, M. (2021). Estonian Information security Standard (E-ITS) based security level evaluation instrument. https://datadoi.ee/handle/33/423

Target Group of E-ITS

Organisations who provide public services

- Public sector organisations
- Vital service providers*
- Other subjects of Cyber Security Act*
- Service providers for the abovementioned*

E-ITS


Seadusandlus
EU seadusandlus
Eesti seadused
Määrused
Muud regulatsioonid
NIS
GDPR
eIDAS
...
HoS
IKS
KüTS
HoS riskianal.
KüTS määrus V&I
Infoturbe juhtimise süsteem
...
...
ISO/IEC standardid
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27000
ISO/IEC 27005
ISO/IEC 31000
ISO 27007
ISO Guide 73
ISO/IEC 2383
E-ITS ISMS Nõuded
Rakendusjuhend
Riskihaldusjuhend
EESTI INFOTURBESTANDARD
Etalonturbe kataloog
Auditeerimisjuhend
Üleminekujuhend
Sõnastik
BSI IT-Grundschutz
BSI 200-1
BSI 200-2
BSI 200-3
Kompendium
Umsetzungs-hinweise
BSI kübersõnastik
BSI 100-4

Requirements for standard*

- Granularity
- EU jurisdiction
- Regular update
- Compliant with international recognised standard
- Optimised risk assesment for typical assets
- Integration with detailed risk assesment
- Business process based
- Developed in compliance with national e-Government solution – PKI (IDcard, digital signature, X-tee)

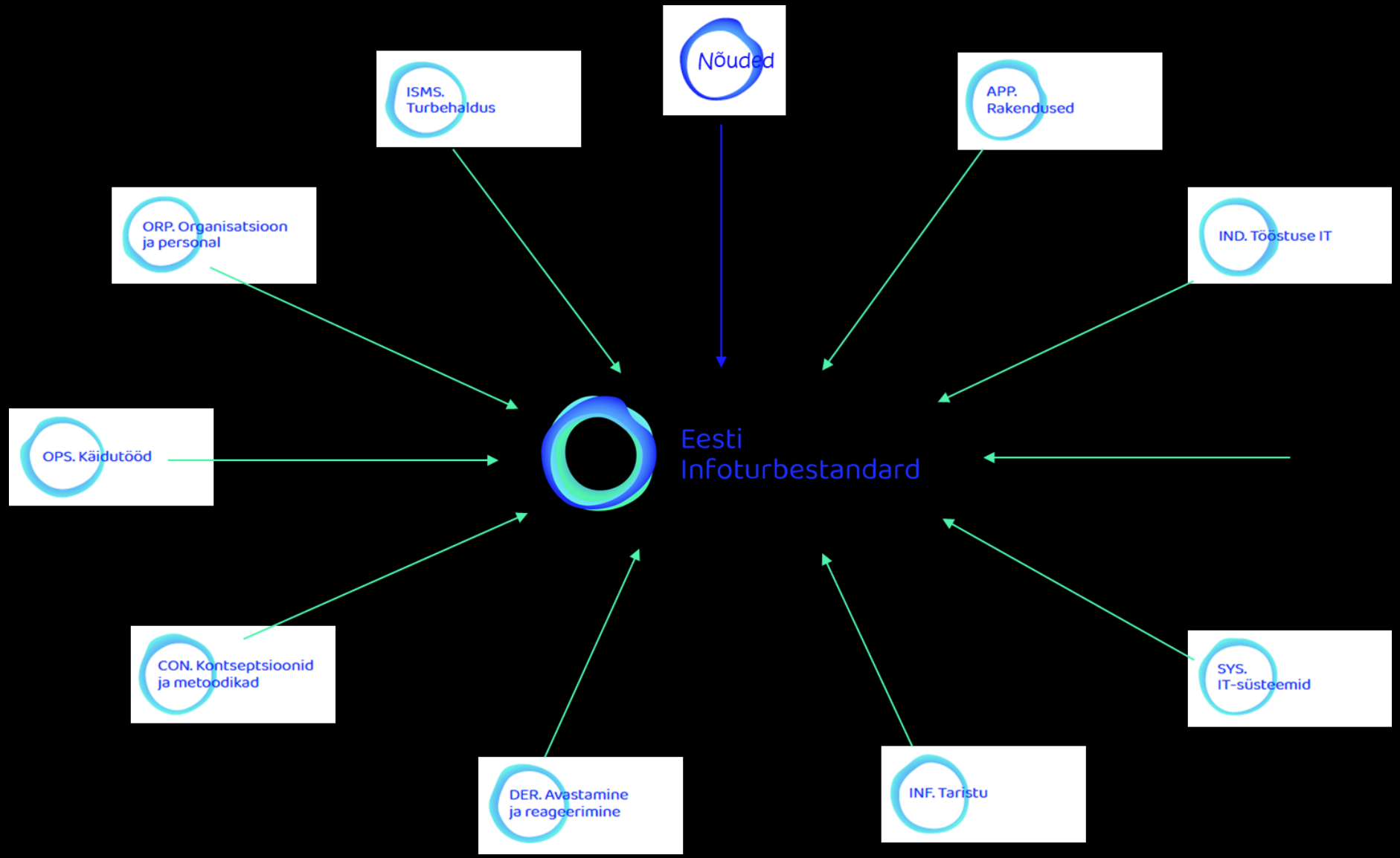
Req ID	Requirement	Requirement description
National security module		
N1	**Developer and jurisdiction**	Standard should take into account EU and NATO regulations.
N2	**Development financing**	It should be possible to influence the development of the standard by national authority.
N3	**Licence conditions**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

* Seeba, M., Matulevičius, R., & Toom, I. (2021). Development of the Information Security Management System Standard for Public Sector Organisations in Estonia. *Business Information Systems*, *1*, 355–366. https://doi.org/10.52825/bis.v1i.43

E-ITS main concepts

Eesti Infoturbestandard

- Combination of Baseline security & Risk assessment
- Protection needs – in support of security requirements
  - C-I-A – based appriach
- Maturity level approach – in support of implementation process
  - Basic, (Core), Standard
- ISO27001 compliance
- Paradigm change
  - Transition from database/registry based system to business process based system
  - Consolidated security management vs organisation based security management (security integration into processes)


Nõuded
ISMS. Turbehaldus
APP. Rakendused
ORP. Organisatsioon ja personal
IND. Tööstuse IT
OPS. Käidutööd
Eesti Infoturbestandard
CON. Kontseptsioonid ja metoodikad
SYS. IT-süsteemid
DER. Avastamine ja reageerimine
INF. Taristu

E-ITS Implementation documentation

E-ITS Quick Guide

E-ITS ISMS Requirements

E-ITS Implementation Guide

E-ITS Risk management Guide

E-ITS Glossary

Threats catalogue

Baseline Catalogue

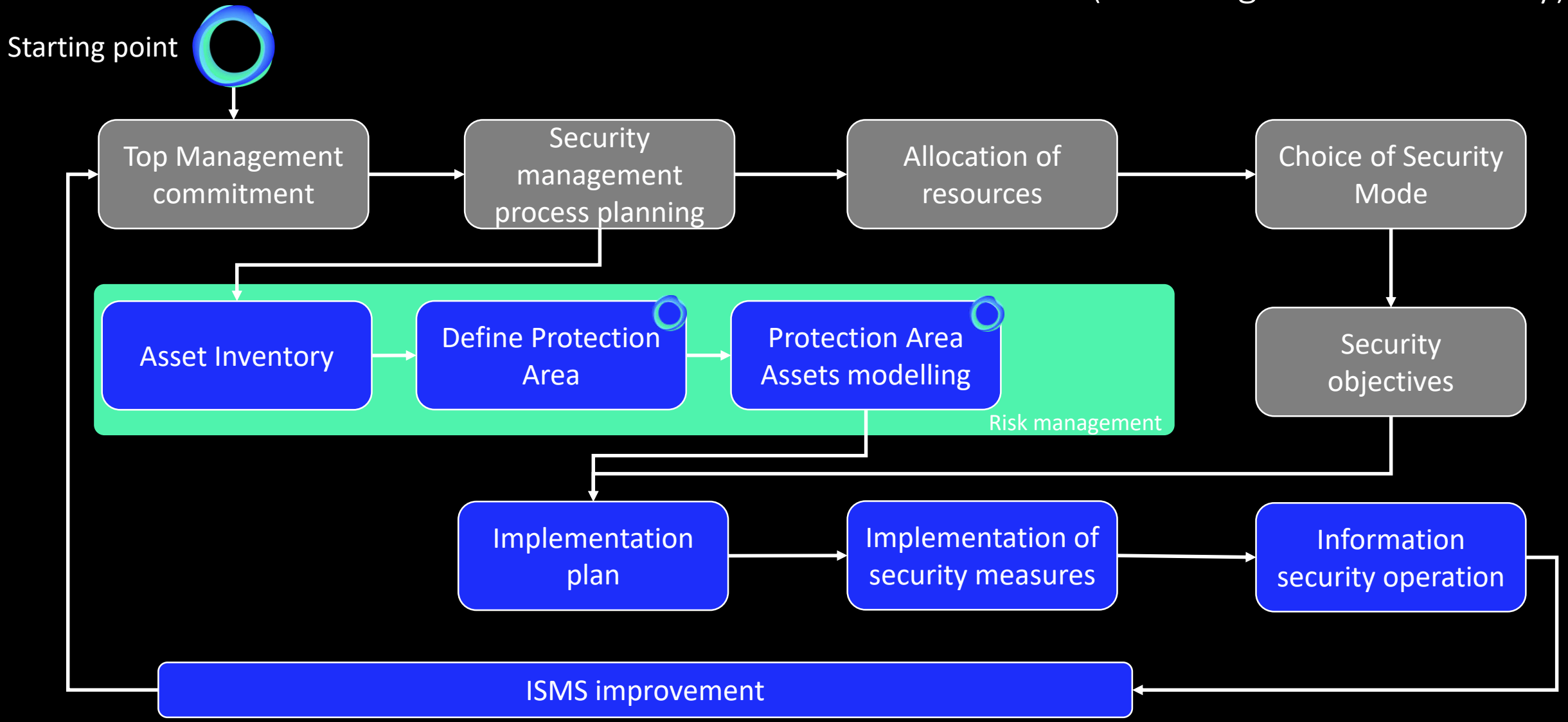
From ISKE to E-ITS Transition Guide

E-ITS Audit guide

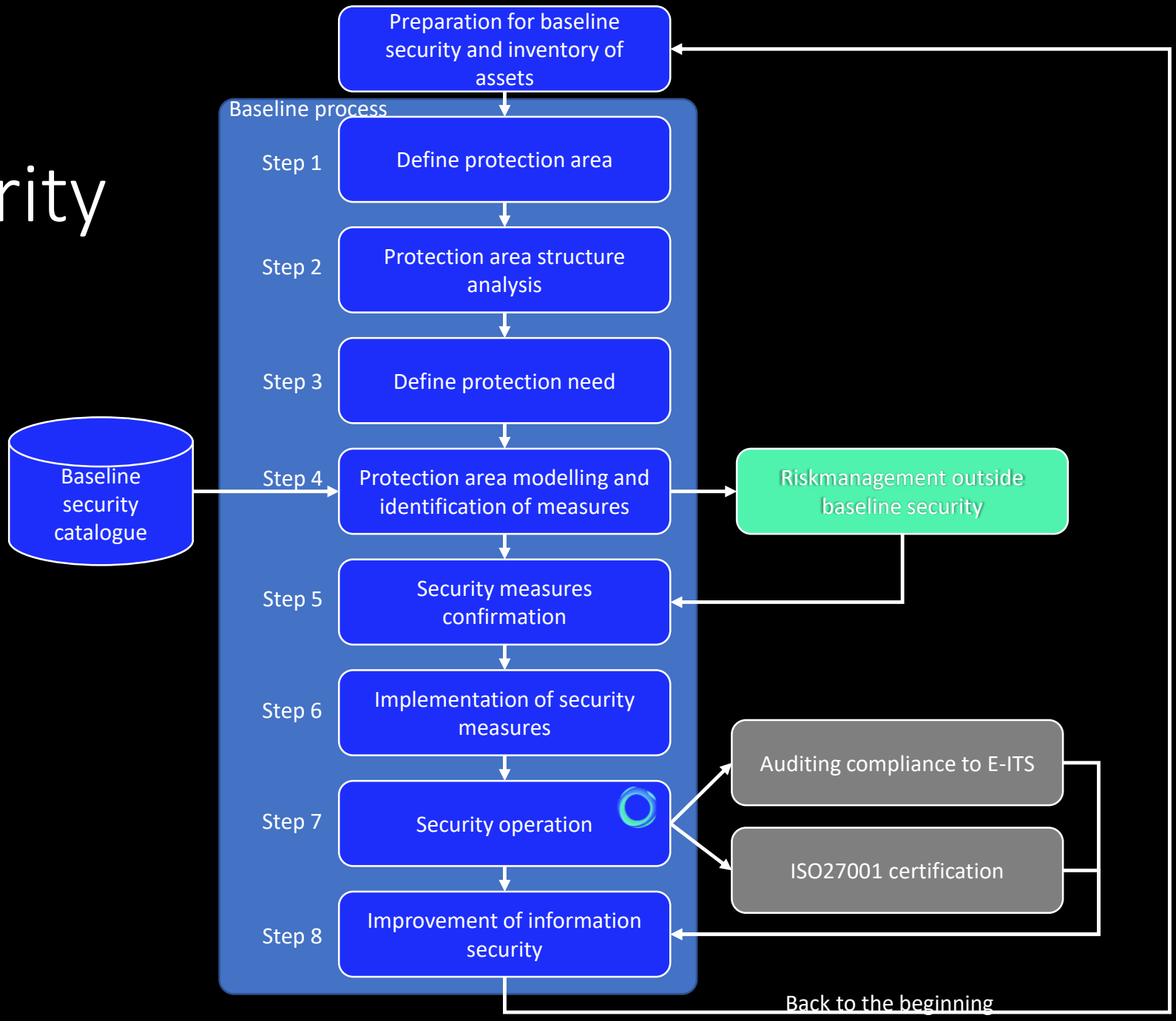
Training materials

Introductory and supplementary materials

Information security process (including baseline security)



8 steps of Baseline security



E-ITS auditing and state level supervisory

Topic	Description
Audit cycle	Three years: initial, middle and final audits (yearly)
Audit approach	• Business process based • Risk based (not required full compliance to measures) • Auditor opinion (public conclusion) • Audit report (confidential)
Audit performance	• Doc review, interviews, obverving, testing – evidence based • Only in reasonable cases permitted to be carried out remotely
Auditor	• CISA, ISO27001 LA • years of experience • Independent, not performed the consulting in the last 3 years for audit object • Required change of auditor after two audit cycle
State level supervisory	• Need based (incidents, compliant, supervisory program) • Penalties for intentional non-compliance or negligence with information security requirements

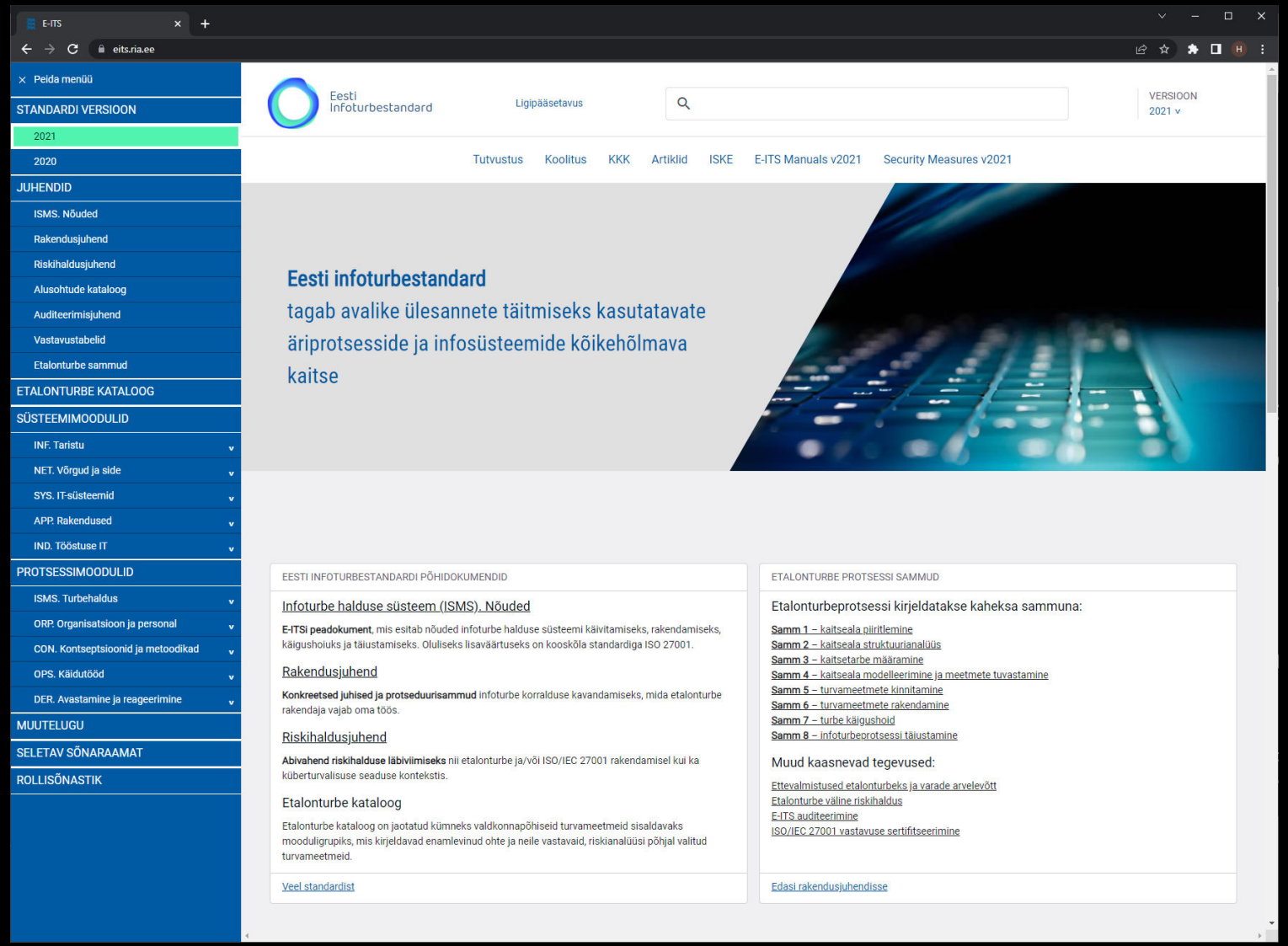
E-ITS events

- Engagement seminars – f2f meetings with implementers
  - Educational presentations
  - Practical informations
  - E-ITS development overview, news
  - Discussions
  - Introductory seminars

- Implementation trainings (outsourced)
  - To consultants
  - To implementers
  - On demand to authorities and wide audience

- Other activities
  - Pilotgroups I and II
  - Cooperation with universities (dissemination and research)
  - Engagement of private sector

eits.ria.ee


E-ITS
eits.ria.ee
Peida menüü
STANDARDI VERSIOON
2021
2020
JUHENDID
ISMS. Nõuded
Rakendusjuhend
Riskihaldusjuhend
Alusohtude kataloog
Auditeerimisjuhend
Vastavustabelid
Etalonturbe sammud
ETALONTURBE KATALOOG
SÜSTEEMIMOODULID
INF. Taristu
NET. Võrgud ja side
SYS. IT-süsteemid
APP. Rakendused
IND. Tööstuse IT
PROTSESSIMOODULID
ISMS. Turbehaldus
ORP. Organisatsioon ja personal
CON. Kontseptsioonid ja metoodikad
OPS. Käidutööd
DER. Avastamine ja reageerimine
MUUTELUGU
SELETAV SÕNARAAMAT
ROLLISÕNASTIK
Eesti Infoturbestandard
Ligipääsetavus
VERSIOON
2021
Tutvustus
Koolitus
KKK
Artiklid
ISKE
E-ITS Manuals v2021
Security Measures v2021
Eesti infoturbestandard
tagab avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kõikehõlmava kaitse
EESTI INFOTURBESTANDARDI PÕHIDOKUMENDID
Infoturbe halduse süsteem (ISMS). Nõuded
E-ITSi peadokument, mis esitab nõuded infoturbe halduse süsteemi käivitamiseks, rakendamiseks, käigushoiuks ja täiustamiseks. Oluliseks lisaväärtuseks on kooskõla standardiga ISO 27001.
Rakendusjuhend
Konkreetsed juhised ja protseduurisammud infoturbe korralduse kavandamiseks, mida etalonturbe rakendaja vajab oma töös.
Riskihaldusjuhend
Abivahend riskihalduse läbiviimiseks nii etalonturbe ja/või ISO/IEC 27001 rakendamisel kui ka küberturvalisuse seaduse kontekstis.
Etalonturbe kataloog
Etalonturbe kataloog on jaotatud kümneks valdkonnapõhiseid turvameetmeid sisaldavaks mooduligrupiks, mis kirjeldavad enamlevinud ohte ja neile vastavaid, riskianalüüsi põhjal valitud turvameetmeid.
Veel standardist
ETALONTURBE PROTSESSI SAMMUD
Etalonturbeprotsessi kirjeldatakse kaheksa sammuna:
Samm 1 – kaitseala piiritlemine
Samm 2 – kaitseala struktuurianalüüs
Samm 3 – kaitsetarbe määramine
Samm 4 – kaitseala modelleerimine ja meetmete tuvastamine
Samm 5 – turvameetmete kinnitamine
Samm 6 – turvameetmete rakendamine
Samm 7 – turbe käigushoid
Samm 8 – infoturbeprotsessi täiustamine
Muud kaasnevad tegevused:
Ettevalmistused etalonturbeks ja varade arvelevõtt
Etalonturbe väline riskihaldus
E-ITS auditeerimine
ISO/IEC 27001 vastavuse sertifitseerimine
Edasi rakendusjuhendisse

Eesti
Infoturbestandard

Estonian Information Security Standard

E-ITS is a full ecosystem of different activities which focus is information security management

Implementation support

- Coopertion with other departments
- FAQ updates
- Table top exercises
- Read Teaming
- Trainings

Regulations support

E-ITS as a mandatory part of digital society

Content development

- Yearly updates of baseline counter-measures and basic guidelines
- Updates based on users feedback, new threats and incidents

E-ITS portal management

- **eits.ria.ee** as a supporting tool
- Machine readable countermeasures
- English version of E-ITS
- All info in one place
- Branding

Early adopters

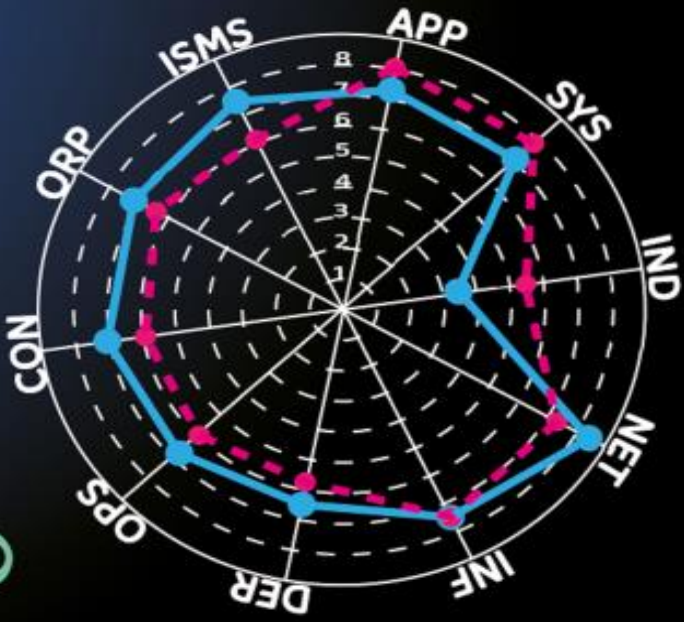
- Piloting projects
- Specific domains profiles
- Experience based consulting
- Engagement seminars

International cooperation

BSI ITG team, ENISA etc.

Information security evaluation.

Cooperatsion with universities and community



What is supervision?

Supervision is:

- a complex set of legal, technical and analytical activities and procedures,
- conducted by a mandated entity
- in order to verify the compliance with applicable requirements and,
- if necessary, force the subjects to comply with the requirements.

Whom do we supervise?

- Governmental organisations
- Local government organisations
- Vital service providers
- Telecom service providers
- Digital service providers
- Health service providers
- Trust service providers
- Members of X-road (ex-post)

Why do we supervise?

- Some people are not aware of their obligations
- Some people just say that they are not aware of their obligations
- Some people don’t know how to implement security measures
- Some people don’t implement security measures
- Incidents happen

How do we supervise?

- Indication
- Initiation of supervisory procedures
- Request for documents, explanation, evidence
- Analysis, preliminary assessment, working hypothesis
- Interviews, interrogation, examination, forensic, scans, on-site observation etc
- Negotiation, hearing subjects opinion, formulating final verdict
- Follow-up(s) if a prescription is made

Varia

- Subjects should always be given time and chance to fix the problem before sanctioning
- We do not conduct audits
- At times we offer consultative supervision and capacity building, if it seems to be more efficacious than punishing and if it does not infringe our objectivity
- One supervision project can last from a week to a year
- If the subject disagrees with us, they can go to court (has not yet happened)

RIIGI INFOSÜSTEEMI AMET

Eesti Infoturbestandard

Thank you for listening!
Questions?

Contact:

standard@ria.ee


Eesti
Infoturbestandard