Riigi Infosüsteemi Amet

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

TARK

e-RIIK

Infoturbe halduse koolitus ISKE baasil

Rünno Reinu

21.03.2018

TTÜ SecTeam

CV – Rünno Reinu

- Hetkel:
  - SecTeam OÜ infoturbe ekspert, lektor
    - info@secteam.ee
    - www.secteam.ee
  - EU
  - Certified Information Systems Security Professional (CISSP)
  - ISO27001 Certified ISMS Lead Implementer (CIS LI)
- Varemalt:
  - Eesti E-tervise Sihtasutus, infoturbejuht
  - Riigi Infosüsteemi Amet, infoturbejuht
  - Sotsiaalministeerium, andmeturbe peaspetsialist

Ajakava

- 08:45 - 09:00 Kogunemine ja hommikukohv (15 min)
- 09:00 - 10:30 Sessioon I (1 h 30 min)
- 10:30 - 10:45 Kohvipaus (15 min)
- 10:45 – 12:45 Sessioon II (2 h)
- 12:45 – 13:30 Lõuna (45 min)

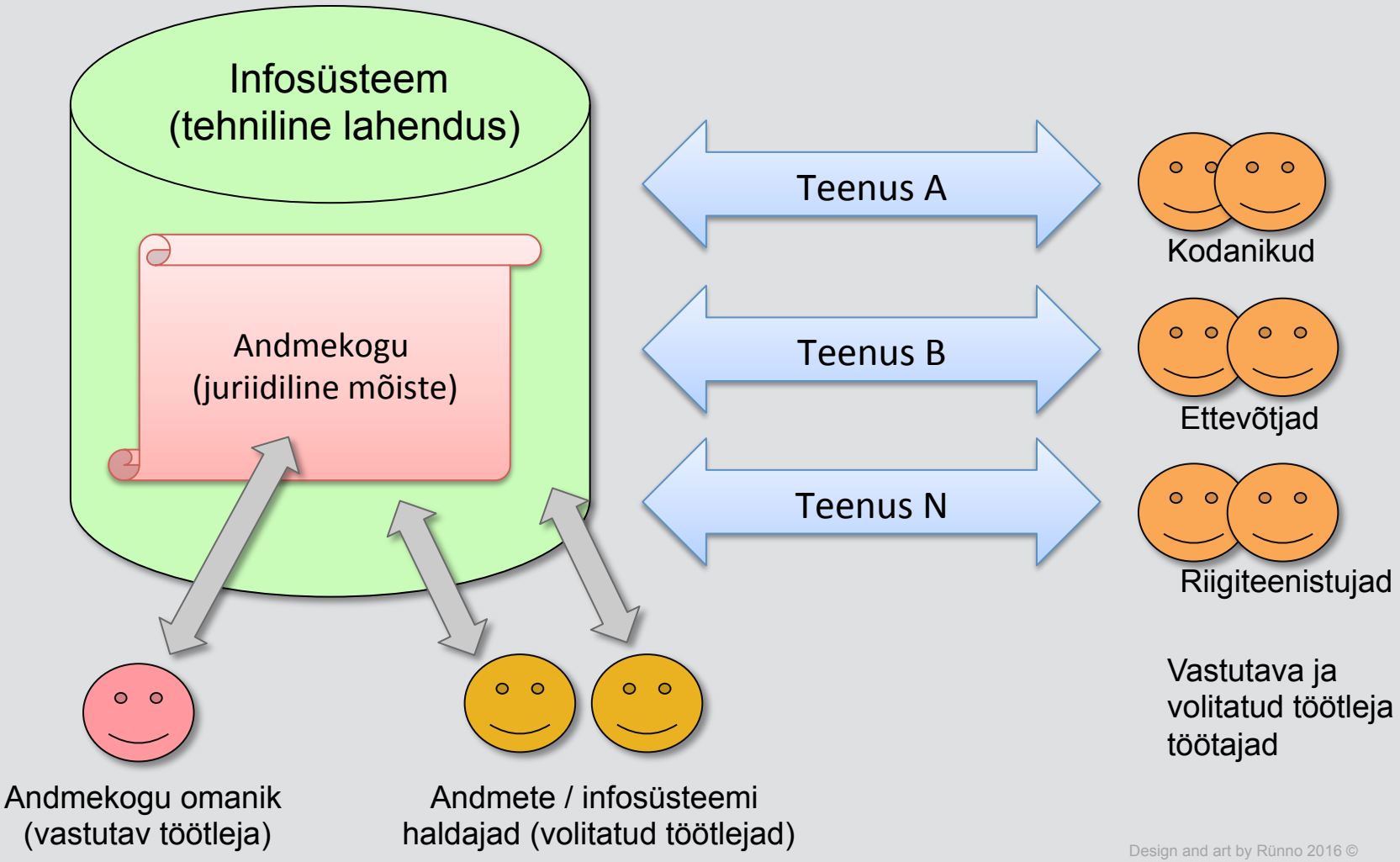
Mõisted 1/5

- Mõistete definitsioonid:
  - ISKE rakendusjuhendis v.8 lk 17-20
  - http://akit.cyber.ee/
- Andmekogu (AvTS § 43[1]) on
  - riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku
  - infosüsteemis töödeldavate
  - korrastatud andmete kogum,
  - mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks
  - Koduseks lugemiseks: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Andmekogude%20juhend.pdf

Mõisted 2/5

- Organisatsiooni sisemise töökorralduse vajadusteks peetav andmekogu - andmekogu, mida peetakse organisatsiooni õigusaktidest tulenevate või põhikirjaliste töökorralduslike ülesannete täitmisel, kui sellest ei väljastata andmeid muudeks vajadusteks. *Ka sellele kohaldub ISKE*.
- Infosüsteem - andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talituseks vajalike vahendite, ressursside ja protsessidega
- Teenus - väärtuse pakkumine klientidele võimaldades neil saavutada lõpptulemusi ilma kaasnevaid kulusid ja riske kandmata
- Vastutav töötleja (AvTS §43[4]) - (haldaja, omanik) on riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist.
- Volitatud töötleja - riigi- või kohaliku omavalitsuse asutus, avalik-õiguslik juriidiline isik või hanke- või halduslepingu alusel eraõiguslik isik, kellele vastutav töötleja on volitanud andmete töötlemise või andmekogu majutamise.

Mõisted 3/5

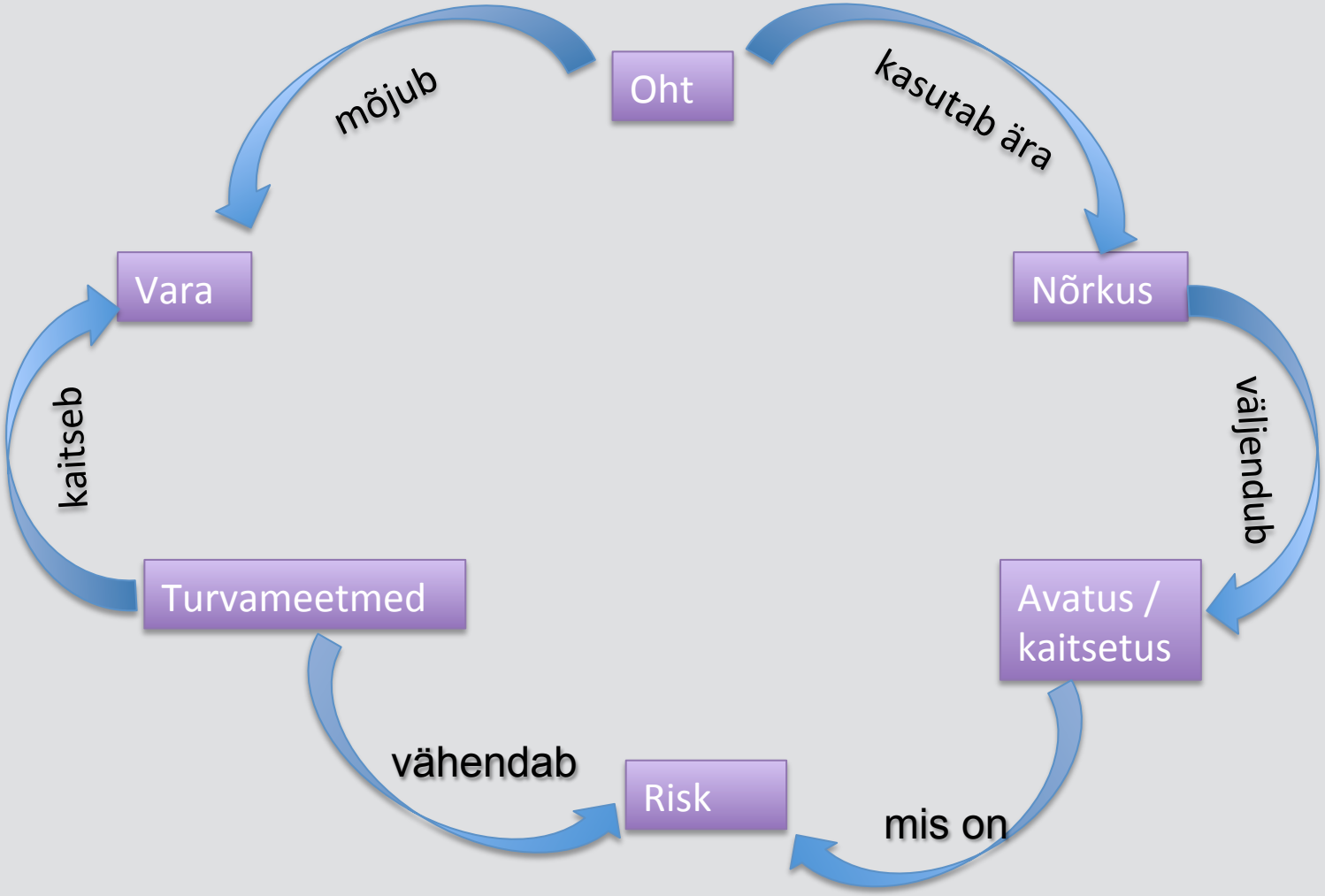


Mõisted 4/5

- Infoturve - riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele, sealhulgas andmekaitse realiseerimise vahend
- Vara (Asset) – kõik asutuse objektid, mis vajavad kaitset ja omavad väärtust. Andmed, meiliteenus, tarkvara, server, protsessid, mööbel, ruumid, inimesed, immateriaalsed varad nagu maine
- Nõrkus/haavatavus (Vulnerability) – vara, süsteemi või protsessi nõrk koht. Turvameetme puudumine või ebapiisavus
- Oht (Threat) – võimalik soovimatu sündmus, mis võib avaldada negatiivset mõju varale
- Avatus/Kaitsetus (Exposure) – vara kaitsetus ohu realiseerumise eest nõrkuse tõttu
- Risk (Risk) – tõenäosus, et oht realiseerub läbi nõrkuse ja tekib kahju
- Turvameede (Safeguard) – riski vähendamise abinõu, poliitika, protseduur, seade vms

Mõisted 5/5

Mööndustega võib mõisteid seostada järgmiselt:



Mis on ISKE?

- ISKE
  - infosüsteemide kolmeastmeline etalonturbe süsteem
  - lihtsalt **riigi infoturbe rakendamise juhend**
  - 1. versioon ilmus 2003 aastal
  - 8.00 versioon kinnitati 30.01.2017 https://www.ria.ee/public/ISKE/ISKE-versiooni-8-00-kinnitamine.pdf
- Aluseks on Saksamaa BSI infoturbe ameti etalonturbe käsiraamat, mis omakorda baseerub ISO 27000 perekonnal
- Põhineb andmete klassifitseerimisel turvaklassideks ja turbeastmeteks
- Sisaldab organisatsioonilisi (15%), füüsilisi (10%) ja infotehnilisi (75%) turvameetmeid

ISKE rakendusala

- ISKE on mõeldud andmekogude pidamisel kasutatavate infosüsteemide ja nendega seotud infovarade turvalisuse saavutamiseks ja säilitamiseks.
- ISKE on rakendatav ka muudes riigi- ja omavalitsusasutustes, äriettevõtetes ning mittetulunduslikes organisatsioonides.

ISKE-ga seotud õigusaktid

- VV määrus “Infosüsteemide turvameetmete süsteem”: https://www.riigiteataja.ee/akt/13125331?leiaKehtiv
- VV määrus “Infoturbe juhtimise süsteem”: https://www.riigiteataja.ee/akt/119032012004?leiaKehtiv
  - Asutuse juhi vastutus
  - Infoturbejuhi vastutus

Miks valida ISKE?

- Süsteemne haldus on “meie sõber”
- Detailne versus etalon riskianalüüsi metoodika:

Detailne riskianalüüs:

- Kaardista varad ja leia omanik;
- Määra iga vara väärtus (AV);
- Leia igale varale mõjuvad ohud;
- Leia iga ohu kohta kahjustatuse määr (EF) ja arvuta üksiku kahju hinnang (SLE=AV*EF);
- Analüüsi ja leia iga ohu avaldumise tõenäosus aastas (ARO);
- Arvuta aastase kahju hinnang (ALE=SLE*ARO);
- Leia iga vara igale ohule vastumeede ja arvuta ümber ARO ja ALE.
- Leia iga vastumeetme aastane kulu (ACS);
- Teosta kuluefektiivsuse analüüs iga vara iga ohu igale vastumeetmele (ALE1-ALE2-ACS).
- Vali välja kõige efektiivsemad meetmed ja juuruta need.

Etalonmetoodika (ISKE):

- Kaardista varad ja leia omanik;
- Määra omanikuga koos andmete olulisus ehk turvaklass;
- Selekteeri ISKE kataloogist välja meetmed ja juuruta need.

Muud infoturbe halduse süsteemid – ISO/IEC

- ISO/IEC 27001 ja 27002
  - ISO/IEC 27001. Infoturbe halduse süsteemid. Nõuded
  - ISO/IEC 27002. Infoturbe halduse tavakoodeks
  - https://www.evs.ee/pood
  - ISO/IEC 27000 standardipere ülevaade ptk 0.2 lk 4: https://www.evs.ee/eelvaade/evs-en-iso-iec-27000-2017-et.pdf

Muud infoturbe halduse süsteemid - CIS

- CIS Critical Security Controls
  - https://www.cisecurity.org/critical-controls.cfm
  - Fookus on IT turbel (küberruumi turbel)
  - Tasuta
  - SANS

Muud infoturbe halduse süsteemid - NIST

- NIST Cybersecurity framework
  - https://www.nist.gov/cyberframework
  - Identify –> Protect -> Detect -> Respond -> Recover
  - Võrdlustabel teemade ja teiste haldussüsteemidega
- NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations
- https://www.nist.gov/publications

Muud infoturbe halduse süsteemid

- BSI
  - https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html
- ITIL
  - Information Technology Infrastructure Library
  - IT teenuste halduse parimad praktikad
  - https://www.axelos.com/best-practice-solutions/itil
- COBIT
  - Control Objectives for Information and Related Technologies
  - Infotehnoloogia juhtimise ja halduse süsteem
  - http://www.isaca.org/COBIT/pages/default.aspx

https://www.ria.ee/ee/iske.html
https://iske.ria.ee

- ISKE rakendusjuhendi
- ISKE meetmetekataloog
- ISKE ohtudekataloog
- Seotud õigusaktid
- Auditi juhend ja tellimise näidis
- Raamdokumentide näidised

ISKE ülesehitus 1/2

- Rakendusjuhend
  - loe rahulikult mõttega läbi (ca 20 lk)
  - https://www.ria.ee/public/ISKE/ISKE_rakendusjuhend.pdf
- Ohtude kataloog (v.8.03 – 1952 tk)
  - hea ülevaade tüüpilistest ohtudest riskianalüüsiks
  - https://iske.ria.ee/8_02/ISKE_ohtude_kataloog
- Meetmete kataloog (v.8.03 – 2356 tk)
  - mahukas seletav materjal
  - ära proovi kohe algusest lõpuni läbi lugeda (ca 3750 lk)
  - Moodul = sarnaste meetmete grupp
- ISKE portaal https://iske.ria.ee
  - Ohtude ja meetmete kataloogid (html, pdf, ods)

ISKE ülesehitus 2/2

- Andmekeskuse turvanõuete kataloog
  - ISKE serveriruumi moodul versus eraldi andmekeskuse turvanõuete kataloog https://www.ria.ee/public/ISKE/AndmekeskuseTurvanouded.pdf

ISKE rakendustööriist

- Hankimisel

www.ria.ee/ee/isketooriist.html

- ISKE rakendamiseks on vaja vaadet:
  - andmekogu -> infovara -> turvaklass ->moodulid -> meetmed
  - saab edukalt hakkama tabelarvutusega

Andmete turvaomadused

- Käideldavus (K) – eelnevalt kokkulepitud vajalikul/nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus (st vajalikul/nõutaval ajahetkel ja vajaliku/nõutava aja jooksul) selleks volitatud tarbijaile (isikutele või tehnilistele vahenditele)
- Terviklus (T) – andmete õigsuse/ajakohasuse tagatus ning päritolu autentsus ning volitamatute muudatuste puudumine
- Konfidentsiaalsus (S) – andmete kättesaadavus ainult selleks volitatud tarbijatele (isikutele või tehnilistele süsteemidele) ning kättesaamatus kõigile teistele

Turva(osa)klass

- ISKE põhineb neljapallilisel skaalal ja eelnevalt nimetatud kolmel turvaeesmärgil (K, T, S):
  - rakendades kolmele turvaeesmärgile (K, T, S) neljapallilist skaalat (0, 1, 2, 3) määratletakse turvaosaklassid, mille tähised koosnevad turvaeesmärgi tähisest ja turvataseme numbrilisest väärtusest.
  - Nt konfidentsiaalsuse madalaim turvaosaklass: S0
- Turvaosaklasside komplekt moodustab turvaklassi:
  - Nt: K1T2S0

Käideldavus

- K0 – väiksem kui 90% aastas ja maksimaalne lubatud ühekordse katkestuse pikkus teenuse töo ajal üle 24 tunni (st ühekordse katkestuse pikkus tohib olla suurem kui 24 tundi)*;
- K1 – suurem või võrdne 90% ja väiksem kui 99% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töo ajal kuni 24 tundi (st ühekordse katkestuse pikkus võib olla vahemikus väiksem või võrdne 24 tunniga ja suurem kui 4 tundi)*;
- K2 – suurem või võrdne kui 99% ja väiksem kui 99,9% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töo ajal kuni 4 tundi (st ühekordse katkestuse pikkus võib olla vahemikus väiksem või võrdne 4 tunniga ja suurem kui 1 tund)*;
- K3 – käideldavus – suurem ja võrdne kui 99,9 % aastas ja maksimaalne lubatud ühekordse katkestuse pikkus teenuse töo ajal 1 tund kuni 0 sekundit (st ühekordse katkestuse pikkus võib olla väiksem või võrdne 1 tunniga)*;

Käideldavus *

- Maksimaalne lubatud katkestuste arv, maksimaalne lubatud summaarne katkestuste aeg ja muud detailsemad teenustaseme mõõdikud kirjeldatakse ja lepitakse kokku teenustaseme lepingus (SLA).
- Teenustaseme lepingus tuleb detailsemal tasemel määrata teenuse osutamise tingimused (nt päringutele vastamise aeg, planeeritud hooldustööde tegemise aeg, nõutav rikete kõrvaldamise aeg, riketest teavitamise kontaktid, varundamise tingimused jmt).
- Lepingu näidise leiab RIA veebist: https://www.ria.ee/ee/raamdokumentide-naidised.html

Terviklus

- T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontrollid pole vajalikud;
- T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse, ajakohasuse kontrollid erijuhtudel ja vastavalt vajadusele;
- T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalikud on perioodilised info õigsuse, täielikkuse ja ajakohasuse kontrollid;
- T3 – infol allikal, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

Konfidentsiaalsus 1/2

- S0 – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus kõigil huvitatutel, muutmise õigus määratletud tervikluse nõuetega);
- S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;
- S2 – salajane info: info kasutamine lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral,
- S3 – ülisalajane info: info kasutamine lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

Konfidentsiaalsus 2/2

Avaliku teabe seadus	ISKE konfidentsiaalsuse turvaosaklass
Avalik teave	S0 (avalikud andmed)
AK	S1
AK	S2 (delikaatsed isikuandmed)
AK	S3

Tagajärgede kaalukus ehk intsidendist tekkiva kahju hindamine

- R0 – turvaintsidendiga (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmisega) ei kaasne märkimisväärseid kahjusid;
- R1 – kaasnevad vähe olulised kahjud, turvaintsident põhjustab tõenäoliselt märkimisväärseid takistusi asutuse funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi;
- R2 - kaasnevad olulised kahjud, turvaintsident põhjustab tõenäoliselt olulise takistuse asutuse funktsiooni täitmisele või ohtu inimeste tervisele või keskkonnasaaste ohtu või olulisi rahalisi kaotusi;
- R3 - kaasnevad väga olulised (missioonikriitilised) kahjud, turvaintsident põhjustab tõenäoliselt asutuse funktsiooni täitmatajätmise võI märkimisväärseid häireid riigikorralduses või ohtu inimelule võI keskkonnasaastet või väga olulisi rahalisi kaotusi.

ISKE 11 sammu

1	Infovarade inventuur
2	Andmekogude kaardistamine, andmekogudele turvaklassi ja turbeastme määramine, turvaklasside RIHAsse märkimine
3	Muude infovarade turvaklassi määramine
4	Kõikide turvaklassiga infovarade vajaliku turbeastme määramine
5	Infovarade tsoneerimine (vajadusel)
6	Tüüpmoodulite spetsifitseerimine
7	Turvameetmete loetelu koostamine
8	Turvameetmete rakendamise plaani koostamine
9	Turvameetmete rakendamine
10	Tegeliku turvaolukorra kontroll
11	Konfiguratsiooni- ja muudatustehalduse sisseviimine

Kes võiks olla töögrupis?

- ISKE juurutamise ja haldamise eest vastutaja, ideaalis infoturbe eest vastutaja, nt infoturbejuht
- IT eest vastutaja
- Isik, kes tegeleb füüsilise turbe ja hoone/ruumide haldusega
- Isik, kes tegeleb asutuse töökorraldusega ja personaliga
- Andmete omanik (kes mõistab andmete väärtust ja õiguslikke raamistikke)
- Juhtkonna esindaja
- Andmekaitseametnik

Samm 1 – infovarade inventuur ja spetsifitseerimine 1/2

- Teostajad: ISKE koordinaator + IT eest vastutaja + varahaldur?
- Kasuta: olemasolevaid raamatupidamise või IT inventuuri andmeid. Tarkvara: OCS Inventory NG, Spiceworks, IPSonar, Open-AudIT, Nessus, Microsoft SCCM, nmap;
- Spetsifitseerimine: seadme nimetus, ID, tüüp, OS, rakendused, IP-d, tööviis/toetusaste, asukoht, vastutav administraator, olek (vt rakendusjuhis lk 16)
- Võrguskeem – lokatsioonid, subnetid/VLAN-id, välised IP-d, WiFi võrgud, olulisemad võrguseadmed. Tööjaamu/servereid ei tasu skeemile kanda.

Samm 1 – infovarade inventuur ja spetsifitseerimine 2/2

- Infovarade tööviisid:
  - käitavad infovarad – varad, mis otseselt on vajalikud andmekogu töo tagamiseks (nt. rakendus, andmebaas, server jmt);
  - toetavad infovarad – varad, mis on vajalikud andmekogude ja/või nendega seotud käitavate varade toimimise tagamiseks, kuid mis ise ei ole otseselt vajalikud andmete töötlemiseks ega ka andmekogust andmete kättesaadavaks tegemisega (nt. varundusserver, võrguseadmed, tulemüür jmt);
  - autonoomsed infovarad – varad, mille esmane funktsioon ei ole seotud andmete ega andmekogudega (nt. tööruumid, majad jmt).
- Toetusaste:
  - Tähtis - ilma nimetatud varata ei saa andmekogu toimida ja see vara on otseselt vajalik andmekogu toimimiseks ja/või muude vahenditega saab andmekogu toimida suhteliselt lühikest aega.
  - Vähe tähtis - andmekogu saab toimida ja/või töid/teenuseid/funktsioone saab ka täita muul viisil
- Grupeeri! Eeldab standarditud haldust

Näide– infovarade kaardistamine

1. Vt näidistabelit *ISKE_varad_ja_meetmed.xlsx*
2. Vaatleme infovarasid ja nende spetsifitseerimist (grupeerime hiljem)
3. Kui ISKE juurutamine ja ISKE auditid on andmekogu (infosüsteemi) põhised, kuidas infovarasid vastavalt jaotada

Samm 2 – andmekogude kaardistamine, turvaklassi ja turbeastme määramine, RIHA 1/2

- Teostajad: ISKE koordinaator, osakonnajuhatajad (andmete omanik), IT spetsialist
- Otsi üles andmekogud, sisemised andmekogud ja infosüsteemid:
  - Õigusaktid
  - Üksuste juhid
  - IT üksus
- Lase juhil kinnitada kaardistuse dokument koos turvaklassidega
- Vt näidiskaardistust Andmekogude_kaardistus.docx

Samm 2 – turvaklassi ja turbeastme määramine 2/2

- Teostajad: ISKE koordinaator, andmete omanik, IT spetsialist
- Protokolli turvaklassi määramine ja lase juhil kinnitada andmekogude kaardistuse dokument
- Vt turvaklassi määramise juhist rakendusjuhendis lk 9 ja Turvaklassi_määramise_protokoll.docx
- Turbeaste – kui turvaklassis esineb suurima numbrina:
  - 3, siis on turbeaste kõrge (H)
  - 2, siis on turbeaste keskmine (M)
  - 1, siis on turbeaste madal (L)
- Turvaklass ja turbeaste märgi RIHA-sse: https://www.riha.ee

Näide – turvaklassi ja turbeastme määramine

- Määrame koos ühe andmekogu (infosüsteemi) turvaklassi ja turbeastme (nt dokumendi-haldussüsteem)

Samm 3 ja 4 – muude infovarade turvaklassi ja turbeastme määramine

- Teostaja: ISKE koordinaator
- Infovarade tabelisse kanna turvaklass ja turbeaste vastavalt seotud andmekogule
- Kui infovara:
  - tööviis on käitav või toetusaste tähtis, siis jäta turvaklass/ turbeaste samaks;
  - tööviis on toetav või toetusaste vähe tähtis, siis võid turvaklassi/turbeastet alandada ühe astme võrra
- Vt näidistabelit *ISKE_varad_ja_meetmed.xlsx*

Samm 5 – infovarade tsoneerimine (vajadusel)

- Teostaja: ISKE koordinaator, IT spetsialist, juhtkonna esindaja
- Aitab optimeerida turvameetmete hulka asutuses
  - hoia H (või M) turbeastmega infovarade hulka võimalikult väiksena, sest siis on vähem meetmeid vaja rakendada
- Tsoneerida saab, kui:
  - turbeastmeks on M või H
  - esineb erinevaid turvaklasse/turbeastmeid
  - esineb võimalus füüsiliste piiride seadmiseks ehk tsoonide eraldamiseks
- Vt selgitavat pilti infovarad_ja_tsoonid.png
- Vt näidist Tsoneerimise_protokoll.docx

Samm 6 – tüüpmoodulite spetsifitseerimine

- Teostajad: ISKE koordinaator, IT spetsialist, vajadusel kaasab teisi töögrupi liikmeid
- Vaata läbi tüüpmoodulite nimekiri https://iske.ria.ee/iske_portal_static/ISKE_kataloogid_8_03.pdf (lk 47)
- Vt ISKE_varad_ja_meetmed.xlsx tüüpmoodulite lehte ja märgi ära kasutuses olevad moodulid
- Märgi need moodulid infovarade (gruppide) taha
- Kui mõni moodul on kasutuses, kuid infovara oli puudu, siis täienda infovara tabelit
- B1.0 moodul on kohustuslik

Näide– tüüpmoodulid

1. Selekteerime asutusele (nt KOV) tüüpmoodulid
2. Proovime nüüd grupeerida infovarad pidades silmas tüüpmooduleid
3. Seostame infovarad/grupid tüüpmoodulitega

Samm 7 – turvameetmete loetelu koostamine

- Teostajad: ISKE koordinaator
- Koosta igale infovarale (grupile) vastavalt tüüpmoodulitele turvameetmete nimekiri
- Kopeeri meetmed failist https://iske.ria.ee/iske_portal_static/ISKE_meetmed_8_03.ods

  Vt näidist ISKE_varad_ja_meetmed.xlsx lehelt Meetmed
- Jälgi turbeastet (L, M, H) ja H astme puhul turvaklassi (HG, HK, HT, HS)
  - tähis "**z**" – soovituslik meede (349 tk), võib olla vajalik kõrgema turvanõudluse puhul
  - tähis "**w**" – informatiivne meede (48tk), mis aitab mõista ja rakendada teisi meetmeid
  - tähis "**E**" – omane ainult Eestile (19 tk), kohustuslikud

Samm 8 – turvameetmete rakendusplaani koostamine

- Teostajad: ISKE koordinaator, IT spetsialist, (varade eest vastutajad, juhtkonna esindaja)
- Märgi meetmete taha:
  - vastutaja – kes peab rakendama või korraldama rakendamise
  - meetme olek – rakendatud, rakendamisel, ei ole rakendatud, ei rakendata
  - selgitus – väga oluline. Kus sätestatud, kuidas teostatud vms
  - rakendamise prioriteet – nt 3-palline skaala (mooduli kirjelduses toodud etapid versus L=1, M=2, H=3 versus vaba hinnang)
  - tähtaeg – millal on plaanitud meede rakendada või korduva tegevuse aeg
  - maksumus – hinnanguline meetme rakendamise kulu
- Vt ISKE_varad_ja_meetmed.xlsx
- Alusta B1.0 infoturbe halduse mooduli rakendamisest ja siis B1.x grupp
- Meedet ei pea rakendama, kui:
  - soovituslik
  - rakendamine on kulukam kui intsidendist tulenev kahju
  - meetmele on samaväärne alternatiiv
  - meedet ei ole võimalik mingi iseärasuse tõttu rakendada

Näide– rakendusplaani koostamine

- Sirvime meetmekataloogi
- Täidame mõned read rakendusplaanis

Samm 9 – turvameetmete rakendamine

- Teostajad: ISKE koordinaator, meetmete eest vastutajad
- Vaata ISKE kataloogist meetme kirjeldust ja kontrollküsimusi (terve mõistus!)
- Kui on tarvis mõne meetme kohta kommentaari, siis küsi iske@ria.ee
- Rakenda prioriteetsemad enne
- Dokumenteeri pidevalt rakendusplaanis

Samm 10 – tegeliku turvaolukorra kontroll

- Teostajad: ISKE koordinaator
- Analüüsi ohtude kataloogi abil, kas välja toodud ohud on reaalselt likvideeritud
- Analüüsi, kas on unikaalseid ohte

		Tõenäosus		
		Vähe tõenäoline	Tõenäoline	Väga tõenäoline
Mõju	Vähe kahjulik	1	2	3
	Kahjulik	2	3	4
	Väga kahjulik	3	4	5

- Vajadusel rakenda täiendavaid turvameetmeid

Samm 11 – konfiguratsiooni ja muudatuste halduse käigushoidmine

- Teostajad: ISKE koordinaator, IT spetsialist
- Muudatuste haldus - organisatsiooni ja ta IT-süsteemide, protsesside jm muudatuste ohje, suunamise ja dokumenteerimise kõigi tegevuste kogum
- Konfiguratsioonihaldus - osa muudatuste halduse tegevustest, hõlmab muudatusi IT-süsteemide konfiguratsioonides, näiteks uute programmide kasutuselevõttu, versiooniuuendusi, parameetrite muutmist jms süsteemi elutsükli kestel
- Sea sisse lihtne muudatuste halduse protsess, et muudatuste info jõuaks ISKE koordinaatorini, kes analüüsib muudatuse mõju infoturbe vaatest (ohud ja meetmed) ja ajakohastab ISKE haldussüsteemi
- Sea sisse konfiguratsiooni halduse protsess, et IT süsteemide häälestuse muudatused oleksid jälgitavad
- Mõistlik on toetuda ITIL parimatele praktikatele

Maksumus

- Ei ole üheselt arvutatav
  - Iga asutus on erineva küpsusastmega
  - Sõltub rakendatud ja rakendamisele kuuluvatest meetmetest
  - Parim ülevaade ressursivajadusest tekib peale rakendusplaani koostamist

Väline vastavusaudit

- https://www.ria.ee/ee/iske-audit.html
- Määrus “Infosüsteemide turvameetmete süsteem”:
  - H turbeaste = iga 2 aasta järel
  - M turbeaste = iga 3 aasta järel
  - L turbeaste = iga 4 aasta järel
- KOV andmekogude auditi tellib MKM arvestades § 9^1 lõigetes 4–8 sätestatud tingimusi ja nõudeid ning lähtuvalt vajadusest. Loe lisa määruse seletuskirjast: https://eelnoud.valitsus.ee/main/mount/docList/5ba911c7-12a1-4026-927e-df401f4adba9
- Audiitor peab olema sõltumatu (2 aastat) ja sertifitseeritud (CISA või ISO 27001) (http://www.eisay.ee/iske-auditite ga-tegelevate-ettevotete-loetelu)
- Uue versiooni kehtestamisest 1 aasta “armuaega”
- Hulgi on soodsam, sest ühisosa üle auditeerima ei pea
- Valimis on iga andmekogu kohta 16 moodulit
- Auditeeritud ühisosa üle auditeerima ei pea
- Järelaudit ainult kõrge riskiastmega puuduste kohta

RIA järelevalve

- Infoturbemeetmete rakendamise kontroll, suures osas seotud ISKE-ga
  - Kaardistamine ja küsitlused
  - Nõustamine ja ennetamine
  - Paikseire ja järelevalve menetlused
  - Vajadusel ettekirjutused ja sunniraha rakendamine
- Ei asenda ISKE rakendamist ega kohustulikke auditeid

Viimased soovitused

- Kui õpid keelt, ei loe sõnaraamatut otsast lõpuni läbi
- Terve mõistus!
- Järgi sammude loogilist järjekorda
- Kasuta meetmete tabeleid ja ISKE portaali (või ISKE tööriista)
- Kasuta näidisdokumente
- Ole kursis turvauudistega:
  - CERT-EE uudised: reg. üksnes asutuse meiliaadressiga
  - certnews@cert.ee
  - Subject: Subscribe
- Infoturbejuht, osale turvajuhtide kommuunis. Rohkem infot iske@ria.ee

Küsimused?

- iske@ria.ee
- info@secteam.ee
  - Rünno Reinu, infoturbe ekspert

Aitäh!