Riigi Infosüsteemi Amet

INFOSÜSTEEMIDE KOLMEASTMELISE ETALONTURBE SÜSTEEM

ISKE

Rakendusjuhend

Versioon 7.00
Märts 2014

Sisukord

0 Muudatused ISKE rakendusjuhendi versioonis 7.00

0.1 Uuendamine ja ümbertöötamine

ISKE rakendusjuhendi versioonis 7.00 on katalooge ja turvaspetsifikatsioone uuendatud ja täiendatud vastavalt BSI etalonsüsteemi (detsember 2009 ja september 2011) saksakeelsete versioonide põhjal vastavalt BSI alussüsteemis tehtud muudatustele ja täiendustele. Lisaks on käesolevas rakendusjuhendi versioonis oluliselt muudetud, uuendatud ja täiendatud ISKE ID kaardi meetmete katalooge.

Rakendusjuhendi versioonis 7.00 lisandus ISKE rakendamise 11. sammu vastutuse tabel. . Lisaks viidi läbi kataloogide tervikluse kontroll, mille käigus ühtlustati meetmete ja moodulite nimetused dokumendi lõikes.

ISKE kataloogide versioonis 7.00 on tõlgitud originaaljuhendist kõigi moodulite kirjeldused ning kõik olulisemad meetmed ja nende selgitused. Lisaks tõlkimisele on meetmeid vastavalt Eesti oludele kohandatud.

Kui peaks leiduma veel meetmeid ISKE turbeastmetes „L" ja „M", millel puudub käesolevas ISKE rakendusjuhendis piisav selgitus, siis neid meetmeid ei ole kohustus rakendada.

Kõik parandusettepanekud ja info ebatäpsuste kohta palume saata iske@ria.ee.

0.2 Muudatused moodulites

0.2.1 Lisandunud moodulid

- B 3.109 – Windows Server 2008
- B 3.211 – Mac OS X-ga töötav klientsüsteem
- B 3.212 – Widows 7-ga töötav klientsüsteem
- B 5.20 – Open LDAP
- B 5.21 – Veebirakendused
- B 5.22 – Logimine
- B 5.E2 – ID-kaart/PKI

0.2.2 Uuendatud moodulid

- B 2.1 - Hooned
- B 2.3 - Bürooruum/lokaalne töökoht
- B 5.5 – Lotus Notes/Domino

- B 5.12 - Microsoft Exchange / Outlook

Ülal nimetatud moodulite sisu on ISKE-s uuendatud.

0.2.3 Välja jäetud moodulid

- B 3.105 - Server Novell Netware 4.x all
- B 3.106 - Server Windows 2000 all
- B 3.207 - Klient Windows 2000 all

0.3 Muudatused meetmetes

0.3.1 Lisandunud meetmed

- M 1.75 – M 1. 80
- M 2.475 – M 2.515
- M 3. 83 – M 3. 90
- M 4.370 – M 4.435
- M 5.165 – M 5.173
- M 6.146 – M 6.151
- M 2.E12 - M 2.E21
- M 3.E2
- M 4.E1 – M 4.E6
- M 5.E1 – M 5.E2

0.3.2 Uuendatud meetmed

- M 1.3
- M 1.7
- M 2.35
- M 2.65
- M 2.206- M 2.207
- M 2. 232
- M 2.324 – M 2.327
- M 2.364

- M 2.367 – M 2.368
- M 2.440 – M 2.442
- M 3.28
- M 4.56
- M 4.116
- M 4.128
- M 4.132
- M 4.146 – M 4.147
- M 4.243 – M 4.244
- M 4.247 – M 4.249
- M 4.280
- M 4.284
- M 4.337
- M 4.339 – M 4.340
- M 4.344
- M 5.90
- M 5.100
- M 5.123
- M 6.21
- M 6.76
- M 6.78
- M 6.99

0.3.3 Välja jäetud meetmed

- M 1.42
- M 2.102
- M 2.199
- M 2.205
- M 2.227 – M 2.228

- M 2.233
- M 3.24 - M 3.26
- M 4.89
- M 4.136 – M 4.137
- M 4.139 – M 4.145
- M 4.150
- M 4.164
- M 4.167
- M 4.361
- M 5.84 – M 5.86
- M 5.99
- M 6.137
- M 6.22
- M 6.55
- M 6.77

0.4 Muudatused ohtudes

0.4.1 Lisandunud ohud

- G 2.14 – G 2.22
- G 2.24
- G 2.26 – G 2.27
- G 2.38 – G 2.39
- G 2.41
- G 2.44 - G 2.51
- G 2.53
- G 2.57

- G 2.59
- G 2.61 – G 2.63
- G 2.66 – G 2.93
- G 2.95
- G 2.98 – G 2.99
- G 2.101 – G 2.147
- G 2.155 – G 2.174
- G 3.2
- G 3.4 – G 3.6
- G 3.10 – G 3.12
- G 3.14
- G 3.17
- G 3.21 – G 3.24
- G 3.27
- G 3.29 – G 3.35
- G 3.40 – G 3.42
- G 3.46
- G 3.48 - G 3.56
- G 3.60 – G 3.61
- G 3.64 – G 3.78
- G 3.80 – G 3.98
- G 3.108 – G 3.116
- G 4.1 – G 4.7

- G 4.9

0.4.2 Uuendatud ohud

- G 2.40
- G 4.38
- G 4.54
- G 4.57
- G 5.50
- G 5.135
- G 5.137

0.4.3 Välja jäetud ohud

- G 2.33 – G 2.34
- G 2.42 – G 2.43
- G 3.25 – G 3. 26
- G 3.47
- G 5.55 – G 5.56
- G 5.58 – G 5.59

1 Lühiülevaade

ISKE põhineb turvet vajavate infovarade kirjeldamisel tüüpmoodulite abil ning sisaldab vahendeid iga tüüpmooduli turvaklassi määramiseks ja mooduli nõutava turbeastme määramiseks selle turvaklassi järgi. Sõltuvalt tüüpmooduli nõutavast turbeastmest määratakse mooduli turvaspetsifikatsiooni kaudu etalonkataloogidest turvameetmed ja kontrollitakse mooduli turvalisust ohtude etalonkataloogi abil.

1.1 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 ja mittetulunduslikes organisatsioonides.

ISKE ei ole mõeldud riigisaladust käitlevate infosüsteemide turbeks.

1.2 Etalonturbe olemus

Etalonturve on tüpiseeritud minimaalne turvameetmestik, mida tuleb rakendada infovaradele ettenähtud turvataseme saavutamiseks ja säilitamiseks. Käesolevad meetmed on koostatud tüüpiliste infovarade turvaanalüüsi ja nende turbe pikaajalise praktika põhjal.

"Rakendamine" tähendab seda, et nõutava turvataseme saavutamiseks tuleb rakendada kõik konkreetse infovara tüübi ja konkreetse nõutava turvataseme kohta spetsifitseeritud kohustuslikud meetmed. Turvameedet ei pea rakendama juhul kui konkreetse turvameetme rakendamine ei vähenda riske ja/või turvameetme rakendamine on kulukas võrreldes turvameetme rakendamisest tulenevate riskide vähendamisega. Samuti ei pea igat turvameedet rakendama, kui riskid on kaetud teiste meetmete rakendamisega. Riigiasutustes tuleb konkreetsete turvameetme mitte rakendamine aktsepteerida infoturbe juhi või infoturbe eest vastutava isiku poolt. Seejuures tuleb asutuse juhti teavitada turvameetmete mitterakendamisest tulenevatest riskidest. Lisaks on igal turvatasemel soovituslikud meetmed, mida soovitatakse rakendada, kuid mis ei ole kohustuslikud:

"z" tähistab soovituslikke meetmeid, mis võivad osutuda vajalikeks eelkõige kõrgema turvanõudluse puhul.

"w" tähistab meetmeid, mille eesmärgiks on aidata mõista ja rakendada teisi turvameetmeid

Ühtlasi tähendab selline rakendamise metoodika optimaalsust, sest kasvõi ühest kohustuslikust meetmest loobumine võib tähendada seda, et nõutavat turvataset ei saavutata. Muude meetmete põhjendamatu lisamine toob kaasa lisakulud, infovarade käideldavuse languse ja tööprotsesside aeglustumise.

Infosüsteemid töötavad pidevalt muutuvas keskkonnas, kus tekib üha uusi ohte. Seetõttu ei saa etalonmeetmestik püsida muutumatuna, vaid vajab regulaarset uuendamist. Selliste uuenduste sooritamine sagedamini kui kord aastas ei ole reaalne. Kuni rakendusjuhendi järgmise versiooni ilmumiseni tuleb asutuste infoturbe eest vastutajail hoolikalt jälgida teavet uute ohtude kohta ja vajaduse korral rakendada lisaks etalonmeetmetele muid abinõusid nende ohtude tõrjeks. Lisaks

jäävad alati ohud, mida ei käsitle käesolev juhend, selle tulevased versioonid ega ka enamik teisi turvastandardeid, kuid millega tuleb igapäevaselt arvestada.

1.3 Astmeline etalonturve

Infosüsteemide turvanõuete analüüsimisel ilmneb tavaliselt, et asutuses on kasutusel turvanõuete taseme poolest üksteisest erinevaid süsteeme ja teenuseid. On selge, et neile on otstarbekas rakendada vastavalt erineva tugevusega turvameetmestikke.

ISKE pakub kolme turbeastet: madalat (L), keskmist (M) ja kõrget (H). Meetmestik on ehitatud kihilisena, nii et keskmine aste saadakse teatud meetmete lisamise teel madala astme omadele ja kõrge aste saadakse teatud meetmete lisamisel keskmise astme omadele.

1.4 ISKE rakendusjuhendi struktuur

ISKE rakendusjuhendi põhikomponendid on infovarade spetsifitseerimise ja turvaanalüüsi juhised ning järgmised etaloninstrumendid:

1) turvaklasside määramise 4-tasemeline skaala, vt jaotis 2.3,
2) tabel nõutava turbeastme (L/M/H) määramiseks turvaklassi järgi, vt jaotis 3.1
3) infovarade tüüpmoodulite turvaspetsifikatsioonide (5 rühma, 77 tüüpi) kataloog B, vt jaotis 5 ISKE_kataloogid_7_00.pdf failist,
4) ohtude (5 gruppi, 478 liiki) kataloog G, vt jaotis 7 ISKE_ohtude_kataloog_7_00.pdf failist,
5) turbeastmete L ja M turvameetmete (6 rühma, 1096 liiki) kataloog M, vt jaotis 7 ISKE_kataloogid_7_00.pdf failist,
6) turbeastme H turvameetmete (4 rühma, 222 liiki) kataloog H, vt jaotis 8 ISKE_kataloogid_7_00.pdf failist.

Viidatud võõrkeelsetest alusmaterjalidest võib leida muid abivahendeid: metoodilisi juhiseid, turvameetmete rakendamise põhjalikke juhendeid, dokumenteerimisvorme jm.

ISKE rakendusjuhendi lahutamatuks osaks on ISKE kataloogid, mis on märgitud kui Lisa 1.

1.5 ISKE rakendamine

ISKE rakendamine asutuses ei ole ühekordne projekt. Tegemist on pideva protsessiga, kuna muutuvad nii IT keskkond, turvaohud ja –meetmed kui ka ISKE rakendusjuhend ise. Asutuse IT keskkonna või süsteemide muudatuste puhul tuleb uuesti kontrollida, millised moodulid, ohud ja turvameetmed lisandusid ning vajadusel rakendada vajalikke turvameetmeid; soovitatav on arvestada ISKE nõudmisi juba enne selliste muudatuste tegemist. Sama tuleks teha pärast ISKE rakendusjuhendi uuendamist.

Tihti tekib küsimus, millistest vahenditest peaks ISKE rakendamist finantseerima. Käesolevas jaotises toodud üheteistkümnest rakendamise tööst esimesed kaheksa on seotud pigem süsteemide analüüsi ja ISKE rakendamise kavandamisega ning ei nõua eriti suuri rahalisi ressursse. Seega saab need igal juhul ära teha ning nendest tuleks alustada.

ISKE täielikul esmakordsel rakendamisel võivad siiski olla vajalikud suhteliselt suuremad ressursid kui seda on vaja hilisema rakendatuse kontrollimiseks ja uutest rakendusjuhendi versioonidest tingitud muudatuste elluviimiseks. Seepärast tuleks ISKE esmakordne täielik rakendamine ette planeerida ning taotleda vajadusel vastavate ressursside eraldamist eelarvesse.

Edasine asutuse IT keskkonna vastavus ISKE metoodikale tuleks tagada hoolduse ja arenduse raamides, planeerides näiteks vastavad vahendid vajadusel igasse algatatavasse projekti.

ISKE rakendamise paremaks korraldamiseks asutuses oleks soovitav määrata ISKE rakendamise eest vastutav isik – ISKE koordinaator/infoturbe eest vastutav isik/infoturbejuht vms. ISKE rakendamine asutuses ei ole ainult IT osakonna sisene „projekt“, vaid pigem kogu asutust läbiv programm või tegevuste kogum. ISKE koordinaator ei pea olema infoturbe eest vastutav isik (aga võib seda olla) ega ei pea ka tingimata olema isik IT osakonnast. ISKE koordinaatori roll on pigem projektijuhi tüüpi, kes koordineerib ja korraldab ISKE rakendamist, kutsub kokku koosolekuid, jälgib ja kontrollib rakendamisplaani täitmist jne. On soovitav, et ISKE koordinaatoril oleks hea side asutuse juhtkonna ning erinevate osakondadega. Lisaks tuleb arvestada ka infoturbe juhimise süsteemi määruse nõuetega. Vaata ka https://www.riigiteataja.ee/akt/119032012004

1.5.1 ISKE rakendamise 11 sammu

1. Asutuse IT eest vastutav töötaja koostöös ISKE koordinaatoriga ja asutuse juhtkonnaga viib läbi infovarade inventuuri ja spetsifitseerimise vastavalt juhistele jaotises 2.1.

2.ISKE koordinaator koostöös põhitegevuse poole esindajatega viib läbi andmekogude kaardistamise. Iga andmekogu omanik (ehk peakasutaja) (vt. jaotis 4 „omaniku“ definitsioon) määrab koostöös ISKE koordinaatori ja infoturbe juhi/spetsialistiga andmekogule turvaklassi vastavalt jaotises 2.3 antud juhistele ning märgib turvaklassid infovarade spetsifikatsioonidesse. Lisaks tuleb edastada turvaklass RIHAsse https://riha.eesti.ee/ kaudu.

3. IT eest vastutav töötaja koos infoturbe spetsialistiga määrab muude infovarade turvaklassi vastavalt juhistele jaotises 2.4 ning märgib turvaklassid infovarade spetsifikatsioonidesse.

4. Infoturbe spetsialist määrab jaotises 3.1 oleva tabeli abil kõikide turvaklassiga infovarade vajaliku turbeastme ja märgib turbeastmed infovarade spetsifikatsioonidesse.

5. Kui kõrgeimaks vajalikuks turbeastmeks osutus M või H, otsustab juhtkonna esindaja koos IT eest vastutava töötaja ja infoturbe spetsialistiga, kas rakendada kogu asutuses ühte turbeastet või jaotada asutus eri turbeastmetega tsoonideks. Viimasel juhul kavandavad nad tsoonid ja selliste tsoonide loomiseks vajalikud muudatused. Kui turvaastmete määramisel ei ilmnenud vajadust turbeastet L ületavaks turbeks, rakendatakse aste L kogu asutuse ulatuses.

6. Infoturbe spetsialist vaatab läbi tüüpmoodulite kataloogi B (jaotis 5 failist ISKE_kataloogid_7_00.pdf), võrdleb seda infovarade spetsifikatsioonidega ja märgib spetsifikatsioonidesse tüüpmoodulite tähised vastavalt juhistele jaotistes 3.1 ja 3.2. Kui tüüpmoodulite kataloogi läbivaatusel ilmneb veel spetsifitseerimata varasid, spetsifitseerib ta nad töö selles järgus. Tüüpmoodulid, millele vastavaid varasid asutuses ei ole, jäetakse arvestamata; see nõue ei puuduta organisatsioonilisi varasid, mis kuuluvad moodulirühma B1.

7. Infoturbe spetsialist koostab kõrgeimast määratud turbeastmest lähtudes turbehalduse meetmete loetelu, leides need meetmed mooduli B1.0 turvaspetsifikatsiooni põhjal turvameetmete kataloogist M (jaotis 7 failist ISKE_kataloogid_7_00.pdf) ja turbeastme H korral ka kataloogist H (jaotis 8 failist ISKE_kataloogid_7_00.pdf).

8. Infoturbe spetsialist koos juhtkonna esindaja ja asutuse IT eest vastutava töötajaga koostab plaani infoturbe halduse (moodul B1.0) meetmete rakendamiseks, seejärel määrab muude infovarade turbe rakendamise prioriteedid ja turbe rakendamise plaani, arvestades ka meetmete rakendamise maksumuse ning ajalise kestvuse prognoose. Infoturbe halduse kavandamisel võib lisaks

etalonmeetmete juhistele abivahendina kasutada ka standardites EVS-ISO/ 27000, 27001 ja EVS-ISO/IEC 27002 antud juhiseid. Plaani koostades on eelnevalt vajalik omada ülevaadet, missugused turvameetmed on juba rakendatud ja millised ei ole rakendatud.

9. Infoturbe spetsialist korraldab plaani täitmise, koostades turvameetmete loetelud tüüpmoodulite turvaspetsifikatsioonide ja turvameetmete kataloogide põhjal, juhindudes turbehalduse meetmetest ja kaasates töösse asjakohaseid töötajaid ja informeerides regulaarselt juhtkonda.

10. Pärast iga infovara turvameetmete evitamist kontrollib infoturbespetsialist ohtude kataloogi G (ohtude kataloog on kättesaadav veebilehelt https://www.ria.ee/iske-dokumendid/) alusel tegelikku turvaolukorda, arvestades tegelikke ohte konkreetse infosüsteemi lõikes. Kui ilmneb mingeid ohte, mida tüüpmooduli turvaspetsifikatsioon ei arvesta, kontrollib ta rakendatud turvameetmete piisavust tegelikes tingimustes ning rakendab vajaduse korral täiendavaid turvameetmeid.

11. Konfiguratsiooni ja muudatuste halduse käigushoidmine, st kõik muudatused infovarade, tüüpmoodulite, turvaklasside ja meetmete osas tuleb asutuses kasutusel olevasse töövahendisse sisestada, et oleks tagatud ajakohane ülevaade asutuse infovaradega toimuvast.

Järgnevalt on esitatud ISKE rakendamise 11 sammu loeteluna.

1. infovarade inventuur;
2. andmekogude kaardistamine, andmekogudele turvaklassi ja turbeastme määramine, märgib andmekogude turvaklassid RIHAsse;
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.

ISKE rakendamise 11 sammu RAC tabel

ISKE rakendamise 11 sammu

Tegevus	Vastutajad			
	IT töötaja	ISKE koordinaator*	Äripoole esindaja	Juhtkond
1. Infovarade inventuur	R	R	R	-
2. Andmekogude kaardistamine, andmekogudele turvaklassi ja turbetaseme määramine, andmekogude turvaklassi määramine RIHAsse;	-	R	R	-
3. Muudele infovaradele turvaklassi määramine	R	R	-	R
4. kõikide turvaklassiga infovarade vajaliku turbetaseme määramine	-	R	-	R
5. Infovarade tsoneerimine (vajadusel)	R	R	-	R
6. Tüüpmoodulite spetsifitseerimine	-	R	-	-
7. Turvameetmete loetelu koostamine	R	R	-	R
8. Turvameetmete rakendusplaani koostamine	R	R	-	R
9. Turvameetmete rakendamine	R	R	R	R
10. Tegeliku turvaolukorra kontroll	R	R	R	R
11. Konfiguratsiooni ja muudatustehalduse toimimine	R	R	R	-

* ISKE koordinaator -roll, mille täitja ülesandeks on ISKE ja/või infoturbe ja/või andmekaitse juurutamise koordineerimine ja juhtimine asutuses.

R – vastutab/osaleb

Kui asutuses tehakse muudatusi andmekogude osas (luuakse uus andmekogu, andmekogu andmete koosseis muutub vmt) ja/või nendega seotud infovarade lõikes, siis alustatakse kogu rakendamise protsessiga algusest peale või sellest etapist alates, mida muudatus mõjutas.

1.6 Etalonturbe täiendamine

ISKE rakendusjuhend ilmub täiendatud kujul uue versioonina kord aastas, sõltuvalt allikmaterjali (jaotis1.7) uute versioonide avaldamisest. Iga järgmine versioon võib sisaldada uusi tüüpmooduleid koos vastavate turvameetmetega ja/või uusi turvameetmeid senistele tüüpmoodulitele. ISKE rakendusjuhendi uue versiooni ilmumisel vaatab infoturbe spetsialist läbi täiendused moodulite loetelus ja moodulite turvaspetsifikatsioonides ning korraldab uutele moodulitele vastavate infovarade turbe ja võimalikud senistele moodulitele vastavate varade turvameetmete täiendused ühe aasta jooksul peale uue juhendi ametlikku kinnitamist majandus- ja kommunikatsiooniministri poolt. Aasta peale uue rakendusjuhendi avalikustamist lisatakse täiendused/muudatused auditeerimisele kuuluvate objektide nimekirja

1.7 Allikad ja lisateabeviited

ISKE põhineb Saksamaa Infoturbeameti (*Bundesamt für Sicherheit in der Informationstechnik, BSI*) poolt publitseeritaval IT etalonturbe käsiraamatul (*IT Grundschutzhandbuch'il*). BSI süsteem on väga ulatuslikult ja detailselt dokumenteeritud ning seda täiendatakse regulaarselt kord aastas.

Nende moodulite kirjelduste, ohtude ja turvameetmete puhul, kus täpsustavad märksõnad ja lisaseletused puuduvad või osutuvad ebapiisavaks, on soovitatav hankida lisateavet BSI käsiraamatust.

BSI koduleheküljelt on saadaval järgmised materjalid.

1. Inglisekeelne juhend *IT Baseline Protection Manual* (november 2005 aasta versioon):

IT-Grundschutz Catalogues 2005 (.pdf)

2. Saksakeelne juhend *IT-Grundschutzhandbuch* (september 2011 aasta versioon):

IT-Grundschutz-Kataloge2014-13 (.pdf)

Turbehalduse korraldamisel võib mõningaid kasulikke juhiseid leida järgmistest standarditest

EVS-ISO/IEC 27002. Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhis

EVS-ISO/IEC 27001. Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded.

2 Infovarade vajaliku turvataseme määramine

2.1 Infosüsteemide analüüs

See on ettevalmistav töö, mis loob lähteandmed infosüsteemide turvaanalüüsiks ja selle dokumenteerimiseks. Töö sooritatakse kolmes etapis. Kõik koostatavad spetsifikatsioonid peavad sisaldama turvaklassi, turbeastme ja tüüpmooduli tähise lahtreid, mis täidetakse hiljem.

Inventuuri ja spetsifitseerimise detailsus sõltub asutuse vajadustest. Üldine põhimõte on, et detailsuse aste peaks võimaldama ISKE rakendamist ning ei tohiks tekitada asutusele asjatut aja- ja töökulu. Võimalusi detailsuse astme määramiseks:

- Spetsifitseerida sellise detailsusega, nagu seda on vaja ISKE rakendamiseks – moodulite määramiseks, ISKE rakendamise tööde planeerimiseks ja täitjate kaasamiseks jne. Näiteks, kui asutuses on kasutusel *Windows Server 2008*, peab see olema spetsifikatsioonis kirjas, et rakendada moodulit B3.108, planeerida selle meetmed, määrata täitjad ning kontrollida täitmist.
- Spetsifitseerida sellise detailsusega, nagu on vaja IT keskkonna haldamiseks ja/või süsteemide konfiguratsioonihalduseks. Näiteks, asutustes tuleb niikuinii omada ülevaadet IT keskkonnast (seadmed, litsentsid, süsteemid jne). Selline ülevaade, mida on vajadusel täiendatud, võib olla ISKE rakendamiseks piisav.

2.1.1 Infosüsteemide inventuur

Kuna enamik arvutisüsteeme on tänapäeval ühendatud koht- ja sisevõrkudega, alustatakse seda etappi asutuse arvutivõrkude dokumenteerimisest. Arvutivõrkude dokumenteerimist võiks alustada võrguskeemi koostamisest (nt. võrkude topoloogia skeem). Võrguskeem on komponentide graafiline esitus, mis näitab kuidas erinevad komponendid on üksteisega ühendatud. Võrguskeem peaks infoturbe seisukohast sisaldama minimaalselt järgmisi komponente:

- IT süsteemid s.t. serverid, töökoha arvutid, võrguseadmed (nt. marsruuterid, kommutaatorid, traadita võrgu seadmed), võrguprinterid jne;
- Komponentide vahelisi võrguühendusi s.t. kohtvõrgu ühendusi (nt. Ethernet tehnoloogial baseeruvaid), WLANi ühendusi jne;
- Kohtvõrgu ühendusi laivõrguga s.t. interneti ühendusi, ühendusi teiste lokatsioonidega, sissehelistamisel baseeruvaid ühendusi jmt.

Inventuuri vastavaust tuleb kontrollida vähemalt korra aastas. Soovituslik on kõik infosüsteemides toimunud muudatused, mis omavad tähtsust ISKE rakendamise osas, koheselt inventuuri kajastavasse töövahendisse sisse märkida.

2.1.2 Infovarade spetsifitseerimine

Iga võrguskeemil või töövahendis kajastatud komponendi kohta peaks olema saadaval minimaalne informatsioon, mida võib säilitada eraldi tabelis, kataloogis või tööriistas/haldusvahendis. Minimaalselt peaks iga komponendi kohta olema saadaval järgmine informatsioon:

- Unikaalne nimetus (nt. seadme täielik nimi või id number);
- Tüüp (nt. x rakenduse andmebaasi server, tööjaam, sidesüsteem vmt);
- ja funktsioon;
- Kasutatav platvorm (s.t. riistvara ja operatsiooni süsteem);
- Tööviis (s.t. käitav, toetav või autonoomne);
- Kasutatav rakendus ja andmebaas;
- Asukoht (nt. hoone ja ruumi number);
- Vastutav administraator ja kasutajad (üksus/ametikoht/roll/...);
- Olek (kasutuses, testimisel, plaanitud)
- Kasutatavad kommunikatsiooni liidesed (internet, Bluetooth, WLAN adapter);
- Võrguühenduse tüüp ja võrguaadress.

Lisaks seadmetele tuleb spetsifitseerida üldkasutatavad infrastruktuuri osad (nt arhiivi- ja laoruumid, koosolekuruumid, serveriruumid, seadmekapid, toitekilbid, toiteliinid jne).

Virtuaalsed IT süsteemid, virtuaalkohtvõrgu ühendused (VLANid) ja virtuaalse privaatvõrgu ühendused (VPNid) jmt. tuleks samuti esitada võrguskeemidel ja seda juhul kui virtuaalsed lahendused erinevad oluliselt füüsilistest lahendustes. Eelneva esitamiseks võib olla mõistlik joonistada kaks eraldi skeemi.

Lähtudes eelnevast võib infovarad liigitada kas käitavateks, toetavateks ja autonoomseteks varadeks. Järgnevalt on defineeritud nimetatud varade tüübid:

Käitavad infovarad – varad, mis otseselt on vajalikud andmekogu töö 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 vmt).

Autonoomsed infovarad–varad, mille esmane funktsioon ei ole seotud andmete ega andmekogudega (nt. tööruumid, majad).

Eelneval viisil eri tüüpi varadeks jagamine võib eri asutustes erineda ja siinkohal ei saa ette anda ka ainuõigeid lahendusi. Olulisem siinkohal on hinnata varade toetusastet. Selleks antakse vajalikud juhised käesoleva rakendusjuhendi punktis 2.4.

2.1.3 Infovarade grupeerimine

Pärast inventuuri läbiviimist selgub tihti, et infovarade ühikuid on niivõrd suurel hulgal, et nende haldamine on väga keeruline. Lisaks on hiljem keeruline pidada arvestatust konkreetsele infovarale rakendatud turvameetme(te) üle. Seetõttu on mõistlik sarnased infovarad grupeerida. Sarnaste infovarade grupeerimisel ühte gruppi võib arvestada järgmiste tunnustega:

- Infovarad on sama tüüpi;
- Infovarad on konfigureeritud ja konfigureeritakse ühetaoliselt;
- Infovarad on ühendatud võrku ühetaoliselt (IT süsteemid samasse kommutaatorisse);
- Infovaradel on samad administratiivsed ja infrastruktuursed nõuded;
- Infovaradel on samad kaitse nõuded;

Infovarade grupeerimisel tuleks lisaks eelnevale arvestada, et turvameetmete rakendamise protsessis oleks jätkuvalt võimalik pidada arvestust turvameetmete rakendatuse üle.

Lihtsaks näiteks infovarade grupeerimisel on asutuse tööjaamad. Ühte gruppi võib grupeerida asutuse tööjaamad, mille operatsioonisüsteemiks on Windows Vista ning mis on keskselt ja ühetaoliselt hallatud.

2.2 Turvalisuse näitajad

2.2.1 Informatsioon ja andmed

Informatsioon ehk **teave** on igasugune teadmine, mis puudutab objekte - näiteks fakte, sündmusi, asju, protsesse või ideid ja millel on teatavas kontekstis eritähendus.

Andmed on informatsiooni taastõlgendatav esitus, mis sobib edastuseks, tõlgenduseks või töötluseks. Informatsioonil iseenesest puudub vorm, see tekib alles esituse ehk andmete kaudu. Andmed on informatsiooni esitus mingil eelnevalt kokkulepitud kujul ja kandjal, näiteks paberdokumendina, digitaalsalvestisena magnetkettal, mikrofilmina, fotona jne.

2.2.2 Informatsiooni turvalisus ja turvaeesmärgid

Igasugusel andmetena talletataval või edastataval informatsioonil on enamasti väärtus tarbija (inimese või tehnilise süsteemi) jaoks. Seetõttu on vajalik andmeturve, mis peab tagama andmete väärtuse säilimise, st andmete turvalisuse. Traditsiooniliselt on andmete turvalisuseks peetud eelkõige nende konfidentsiaalsust ehk salastatust. Tänapäevalgi kiputakse tihti samastama andmeturvet salastusega, kuigi andmeturbe ulatus on tunduvalt laienenud. Andmete turvalisus kui üldeesmärk on mitmemõõtmeline ja koosneb osaeesmärkidest.

Mitmesuguste turbemetoodikate aluseks võivad olla erinevad turvamudelid, mis hõlmavad 3-6 osaeesmärki. Levinuim on turvamudel, mis põhineb kolmel osaeesmärgil, andmete kolme omaduse ja nimelt käideldavuse, tervikluse ja konfidentsiaalsuse tagamisel. Sellisel mudelil põhineb ka ISKE.

Andmete käideldavus on 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). Käideldavus on esmane nõue iga infosüsteemi kõigile andmetele ja muudele infovaradele; käideldavuse kadumisel on kogu infosüsteem tarbetu.

Andmete terviklus on andmete õigsuse/täielikkuse/ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.

Asutuse normaalse töö üks eeldusi on, et iga andmekogumi (dokumendi, faili, säiliku, registri kirje jne) kohta saab teha kindlaks, kes ja millal on selle loonud, ning olla kindel selles, et see andmekogum ei ole pärast loomist stiihiliste tegurite toimel või kellegi tegevuse tulemusena volitamatult muutunud. Kõik andmed peavad alati olema seostatavad nende looja, loomisaja, konteksti jms asjaoludega ning nende seoste rikkumisel, samuti andmete endi kaotsiminekul või muutumisel on tööd negatiivselt mõjutavad tagajärjed.

Andmete konfidentsiaalsus on andmete kättesaadavus ainult selleks volitatud tarbijaile (isikutele või tehnilistele süsteemidele) ning kättesaamatus kõigile ülejäänutele.

Avalike andmete turbe korral peavad olema tagatud käideldavus ja terviklus**.**

Üheski praktilises süsteemis ei ole olemas täielikku turvet**,** st täielikku käideldavust, täielikku terviklust ja täielikku konfidentsiaalsust. Millistele infoturbe aspektidele tuleb konkreetsete andmete korral tähelepanu pöörata, oleneb konkreetsest infosüsteemist ja selle otstarbest, st käideldavate andmete väärtusest. Enamasti tuleb arvesse võtta turvalisuse kõiki kolme komponenti, kuid erinevate kaaludega. Organisatsioonis nõutav infoturbe tase sõltub organisatsiooni ülesannetest, õigusaktidest ja eeskirjadest, organisatsiooni tegevuse sisemisest korraldusest, infosüsteemide ja ka teenuseandjate ja koostöö- või lepingupartnerite tagatud või nõutud turvatasemest jms. Niisiis tähendab andmete turvalisus, et on saavutatud **kolm eesmärki: teabe käideldavus (K), teabe terviklus (T), teabe konfidentsiaalsus (S)**.

2.3 Andmete turvaklassi määramine

Infosüsteemi ja selles olevate andmete turbe rajamine tähendab turvameetmestiku valimist vastavalt turvavajaduste alusel kehtestatud turvanõuetele. Mida suuremad on nõuded konkreetsete andmete turbele, st andmete käideldavusele, terviklusele ja konfidentsiaalsusele, seda tugevam turvameetmestik tuleb rakendada.

Asutuse infosüsteemi turvanõuded sõltuvad paljudest asjaoludest. Neid ja andmete väärtust teab kõige paremini andmete omanik, kes seetõttu kõige paremini oskab neist tuletada konkreetsetele andmetele sobiva turvataseme, täpsemalt - konkreetsetele andmetele sobiva käideldavustaseme, terviklustaseme ja konfidentsiaalsus taseme.

Andmete vajaliku turbetaseme peab määrama andmete omanik. Infoturbe spetsialist ei saa määrata andmete vajalikku turbetaset, kuna ta ei tarvitse teada andmete turbevajaduse tausta ja põhitegevuse poolelt andmetele esitatavaid nõudeid. IT või infoturbe spetsialist võib olla nõuandja rollis. Pärast andmete turbetaseme ja turvaosaklasside määramist omaniku poolt tuleb turvaklassid **asutuse juhtkonnal kinnitada**.

Turvaspetsialisti seisukohalt võib turvatasemete kombinatsioone, st turvaklasse vaadelda kui teatud turvameetmestike sümboleid, mis on sõltumatud turvavajaduste põhjustest. Asutuste töötajate seisukohalt võib turvaklasse vaadelda kui teatud turvanõuete komplekside sümboleid. Näiteks ei

olene konfidentsiaalsust tagavad turvameetmed sellest, kas kaitstavad andmed on ärisaladus või delikaatsed isikuandmed, vaid üksnes sellest, mil määral neid on vaja kaitsta.

Vajalike turbetasemete määramiseks on mõistlik kasutada hindamisskaalat. ISKE põhineb neljapallilisel skaalal ja eelnevalt nimetatud (jaotis2.2) kolmel turvaeesmärgil. Rakendades kolmele turvaeesmärgile neljapallilist skaalat määratletakse alljärgnevad **turvaosaklassid**, mille tähised koosnevad turvaeesmärgi tähisest ja turvataseme väärtusest.

Käideldavus:

K0 – Käideldavus – väiksem kui 80% aastas ja maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal üle 24 tunni (st ühekordse katkestuse pikkus tohib olla suurem kui 24 tundi)*;

K1 – käideldavus –käideldavus – suurem või võrdne 80% ja väiksem kui 99% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal kuni 24 tundi (st ühekordse katkestuse pikkus võib olla vahemikus väiksem või võrdne 24 tunniga ja suurem kui 4 tundi)*;

K2 – käideldavus – suurem või võrdne kui 99% ja väiksem kui 99,9% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö 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 töö ajal 1 tund kuni 0 sekundit (st ühekordse katkestuse pikkus võib olla väiksem või võrdne 1 tunniga) *;

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:

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.

* Maksimaalne lubatud katkestuste arv, maksimaalne lubatud summaarne katkestuste aeg ja muud detailsemad teenustaseme mõõdikud kirjeldatakse ja lepitakse kokku asutuse teenustaseme lepetes (SLA-des). SLA näidise leiab RIA veebist https://www.ria.ee/raamdokumentide-naidised/ --> SLA näidis.

*Juhul, kui teenustaseme kokkulepet ei ole sõlmitud, kehtivad järgmised käideldavuse nõuded:

Andmete turvaklass on kolme turvaosaklassi konkreetne kombinatsioon. Nende kõikvõimalike kombinatsioonide arv on 4x4x4, seega on erinevaid turvaklasse 64.

Andmete turvaklassi tähis moodustatakse osaklasside tähistest nende järjestuses K-T-S.
Üks konkreetne andmete turvaklass on näiteks **K2T3S1**. Selline tähis on aluseks andmetele ja muudele infovaradele kohustuslike etalonturvameetmete määramisel. Andmeturbe eesmärkide tagamiseks peavad olema rakendatud turvameetmed, mis vastavad infovara turvaklassile.

Turvameetmed valitakse turvaklassile vastavast etalonmeetmete kataloogist konkreetse infovara etalonturbe spetsifikatsioonide alusel.

Andmete turvaklassi määramiseks teostab andmete omanik infosüsteemides käideldavate andmete turvaanalüüsi, määrates selleks kõigi andmeliikide turvaosaklassid ülaltoodud kriteeriumide alusel. Ühe andmekogu eri andmeliikidel võib olla erinev turvaklass.

Andmete turvaklass ei ole piisav asendamaks andmekogust pakutavate teenuste teenustaseme lepinguid või kokkuleppeid. Teenustaseme lepingus tuleks detailsemal tasemel määrata teenuse osutamise tingimused (nt. päringutele vastamise aeg, planeeritud hooldustööde tegemise aeg, nõutav rikete kõrvaldamise aeg, riketest teavitamise kontaktid, varundamise tingimused jmt.).

Turvaosaklasside määramisel tuleb arvestada järgmist tüüpi nõuetega (vt joonis 1):
Seadustest ja lepingutest tulenevad nõuded

Seadustest tulenevad nõuded nt. teabe konfidentsiaalsusele. Kui teave on seadusandluses tunnistatud avalikustamisele kuuluvaks teabeks (nt. lähtuvalt Avaliku teabe seadusest), siis tuleks määrata konfidentsiaalsuse turvaosaklassiks S0. Kui teave on seaduse alusel tunnistatud vastava tasemega juurdepääsupiiranguga teabeks, siis tuleks sellele vastavalt nõuetele määrata konfidentsiaalsuse turvaosaklass S1, S2 või S3. Delikaatsete isikuandmete töötlemisel tuleks määrata teabe konfidentsiaalsuse turvaosaklassiks vähemalt S2.

Lepingutest tuleb lähtuda juhul kui nendest tulenevad kohustused andmete käideldavusele, terviklusele ja/või konfidentsiaalsusele. Kui näiteks riigiasutus tarbib teise riigiasutuse poolt pakutavaid teenuseid ja nende vahel on sõlmitud leping, mis määrab eraldi nõuded andmete käideldavusele, terviklusele ja konfidentsiaalsusele, siis tuleb turvaosaklasside määramisel arvestada nimetatud nõuete ja kohustustega.

Põhitegevuse (või äritegevuse) protsessidest tulenevad nõuded

Põhitegevusest võivad tuleneda konkreetsed nõuded pakutavatele IT teenustele ning need määravad ka nõuded andmete käideldavuse, terviklusele ja konfidentsiaalsusele. Kui asutuse teenindusbürood peavad teenindama kodanikke nt. vahemikus E-R 09.00-18.00, siis nendel aegadel peavad toimima IT süsteemid ja peab olema tagatud andmete käideldavus.

Tagajärgede kaalukuse hindamine

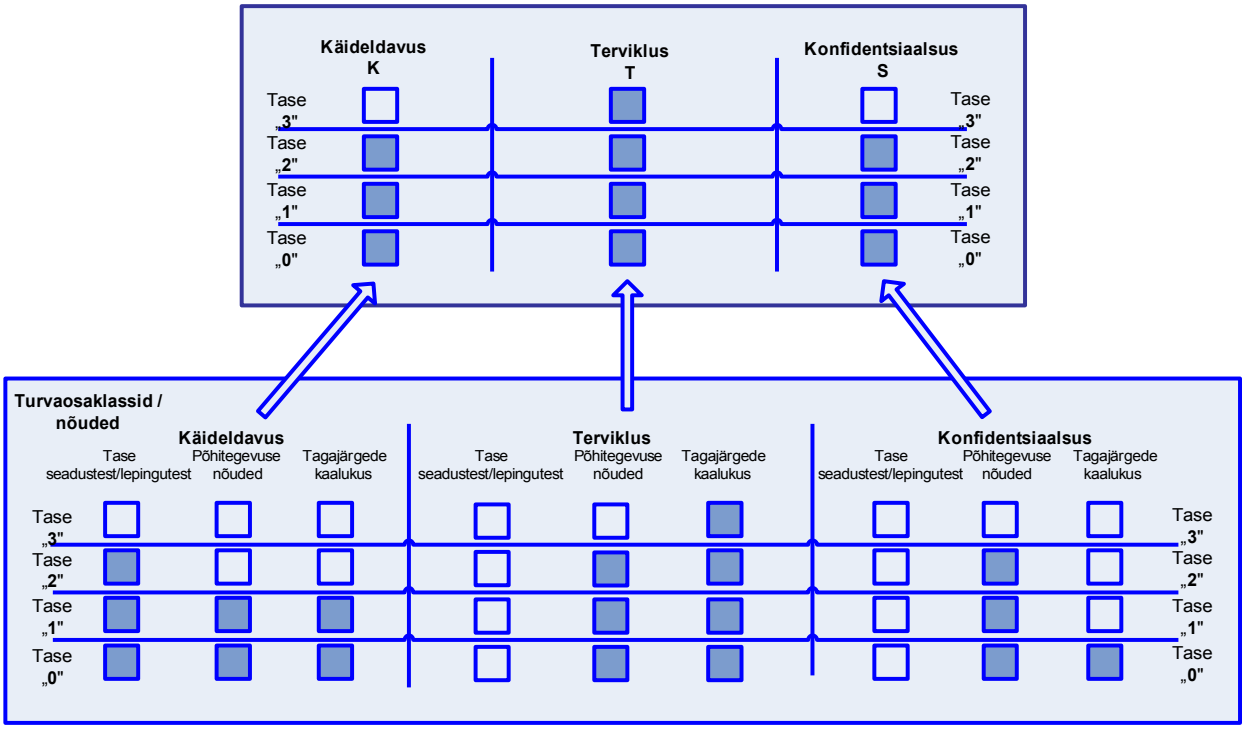
Tagajärgede kaalukus tähendab turvaintsidendist tekkivate kahjude hindamist. Kahjusid võib hinnata neljatasemelisel skaalal:

$_{R}$0 – turvaintsidendiga (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmisega) ei kaasne märkimisväärseid kahjusid;

$_{R}$1 – kaasnevad vähe olulised kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt märkimisväärseid takistusi asutuse funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi;

$_R$**2** - kaasnevad olulised kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt olulise takistuse asutuse funktsiooni täitmisele või ohtu inimeste tervisele või keskkonnasaaste ohtu või olulisi rahalisi kaotusi;

$_R$**3** - kaasnevad väga olulised (missioonikriitilised) kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt asutuse funktsiooni täitmatajätmise või märkimisväärseid häireid riigikorralduses või ohtu inimelule või keskkonnasaastet või väga olulisi rahalisi kaotusi.



Joonis 1. *Turvaosaklassid ja turvaosaklasside määramise nõuded*

Kui eelnevalt nimetatud nõuded määravad erinevad tasemed, siis tuleb turvaosaklassi määramisel lähtuda kõrgeimast tasemest.

Näiteks, tervikluse turvaosaklassi korral seadustes/lepingutest ei tulene nõudeid, põhitegevuse nõuded määravad taseme „2" ja tagajärgede kaalukus määrab taseme „3", siis lähtudes eelnevast määratakse turvaosaklassiks T3.

Turvaanalüüsi süstemaatiliseks sooritamiseks ja dokumenteerimiseks kasutatakse infosüsteemide spetsifikatsioone, mis koostati infosüsteemide analüüsi tulemusena (jaotis2.1). Andmete turvaklassid märgitakse spetsifikatsioonidesse vastavate andmeliikide või süsteemi rakenduste nimetuste juurde. Turvaanalüüsi käigus vaadatakse läbi kõik spetsifitseeritud infosüsteemid. Andmete turvaanalüüsi sooritab andmete omanik.

2.4 Muude infovarade turvaklassi määramine

Kui andmete turvaklassid on määratud, määratakse muude infovarade turvaklassid, alustades kõige kõrgemate turvaklassidega andmeid käitlevatest infosüsteemidest.

Järgmisena vaadatakse kõiki süsteemiga seotud infovarasid (sh tugi- jm toetavad süsteemid s.t. toetavate ja autonoomsete varad) ja hinnates nende tähtsust kõrgeima turvaklassiga andmekogude seisukohalt, alljärgnevas tabelis oleval skaalal.

Vara roll	Kriteerium
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.

Kui vara osutub kõrge turvaklassiga andmekogu jaoks tähtsaks, tuleb talle määrata samasugune turvaklass, muul juhul võib klass olla ühe taseme võrra madalam. Turvaosaklassi võib alandada ainult juhul, kui see ei ohusta kogu süsteemi turvalisust ega ole seatud turvalisuse klassiga vastuolus.

Näiteid vara turvaklassi määramistest: Kui andmekogu turbeaste on H ja H turbeaste tuleneb käideldavusest, siis on enamikel juhtudel mõistlik määrata kõrged käideldavuse nõuded ka kõigile andmekogu käideldavust tagavatele varadele s.t. rakendus, andmebaas, operatsioonisüsteem, server, võrguseadmed, tulemüür, serveriruum, kaablid ja töökohad, mis vajavad kõrget käideldavust andmete käitlemise mõttes. Turbeastet on mõistlik alandada näiteks järgmiste toetavate varade jaoks - kontoriruumid, koosoleku saalid ja need tööjaamad, mille kasutajad ei pea pääsema andmekogule ligi H käideldavuse tasemel. Jälgima peab ka seda, et kui andmekogu konfidentsiaalsust on vaja tagada S2 tasemel, siis tööjaama turvaklass, kus andmeid töödeldakse, peab olema sama. Lisaks, kui süsteemi arhitektuur seda lubab, võib andmekogu teenustele määrata ka eraldi turvaklassid.

Kui aga H turbeaste tuleneb andmete konfidentsiaalsuses, siis ei pea tingimata H turbeastet määrama nt. kaabeldusele ja seda juhul kui kaablis on andmed krüpteeritud kujul.

Muudest infosüsteemidest sõltumatute infosüsteemide puhul vaadeldakse kõigepealt andmete turvaklassi. Kui see on suhteliselt madal, hinnatakse kogu süsteemi tähtsust; selleks võib samuti kasutada ülaltoodud tabelit. Kui süsteem tervikuna osutub hetkel käideldavatest andmetest olulisemaks (näiteks maksumust arvestades), antakse talle vastavalt kõrgem turvaklass. Infosüsteemile määratud turvaklass määratakse ka temaga otseselt seotud infovaradele.

Hetkel mitte kasutusel olevate infovarade puhul (veel käiku andmata toite- või sideliinid, testimisel olev tarkvara jms) tuleb hindamisel arvestada nende tulevast otstarvet.

Ülalloetletud infovarade turvaklassid määrab asutuse infotehnoloogia eest vastutav spetsialist koos infoturbespetsialistiga.

Töö selles järgus tuleb hoolikalt jälgida süsteemidevahelisi seoseid, hoolitsedes selle eest, et oluliste infosüsteemidega seotud muude süsteemide liiga nõrk turve ei ohustaks oluliste süsteemide turvalisust.

Kui asutuse struktuur, ruumid, tehniline taristu ja tingimused võimaldavad kulude kokkuhoiuks kasutada tsoneerimist erinevate ISKE klasside osas, siis võib seda kasutada.

Muude infovarade toetusastme määramisel tuleb arvestada ohte ja riske, mis võivad tuleneda vara turbeastme alandamisest ning kas asutus on valmis neid riske aktsepteerima.

3 Nõutava turbeastme ja turvameetmestiku määramine

3.1 Turbeastme määramine turvaklassi järgi

Turvaklassi järgi määratakse kõigi eelnevalt spetsifitseeritud (jaotis2.1) ja turvaanalüüsi tulemusena turvaklassi saanud infovarade nõutav turbeaste.

Turvaklasse ehk kolme turvaosaklassi erinevaid kombinatsioone on kokku 64.
Alljärgnev tabel seab nende 64 kombinatsiooniga vastavusse kolm etalonturbe astet:

- **madal turbeaste (L),**
- **keskmine turbeaste (M),**
- **kõrge turbeaste (H).**

		K0	K1	K2	K3
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

Iga infovara turvaklassi osaklasside järgi leitakse sellest tabelist vastava vara jaoks nõutav etalonturbeaste ja märgitakse see infovarade spetsifikatsiooni (jaotis2.1) vastavasse lahtrisse.

Seejärel leitakse tüüpmoodulite kataloogist (jaotis 6 failist ISKE_kataloogid_7_00.pdf) sellele infovarale vastava tüüpmooduli tähis ja märgitakse see infovarade spetsifikatsiooni (jaotis2.1) vastavasse lahtrisse.

Kui kõikide spetsifitseeritud varade turbeastmed on määratud, sõltub edasine tegevus saadud turbeastmete arvust:

kui kõikidel varadel on ühesugune turbeaste, võib määrata turvameetmed tüüpmoodulite turvaspetsifikatsioonide ja turvameetmete kataloogi abil;

kui turbeastmeid on kaks või kolm, tuleb analüüsida võimalust asutuse infoturbe otstarbekaks tsoneerimiseks, vt punkti 2.4.

Tsoneerimise otstarbekas korraldamine võib nõuda muudatusi süsteemide funktsioonides ja paigutuses, ruumide funktsioonides jne. Enne lõplikke turvaotsustusi tuleb muudatused kavandada, kinnitada ja plaanida. Optimaalse tsoneerimise huvides võib olla vajalik tõsta mõnede infovarade eelnevalt leitud turbeastet, mõnedel varadel võib seda aga funktsioonide ümberpaigutamise tulemusena langetada.

3.2 Turvaklassita infovarade turbeastme määramine

Jaotises 3.1 on juhised turvaklassiga infovarade, st spetsifitseeritud infovarade nõutava turbeastme määramiseks. Spetsifitseerimisele kuulusid aga ainult andmed, materiaalsed infovarad ja tarkvara. Kaitset vajavad aga ka töökorraldusprotsessid ja muud organisatsioonilised ressursid, ka infoturbe haldus ise sõltub nõutavast turbetasemest.

Kõik sellised spetsifitseerimata varad on kirjeldatud vastavate tüüpmoodulitena (jaotis 5 failist ISKE_kataloogid_7_00.pdf), mis kuuluvad peamiselt tüüpmoodulite rühma B1.

Kogu tüüpmoodulite rühmale B1 tuleb määrata kõrgeim jaotises 3.1 määratud turbeaste.

Kui tüüpmoodulite läbivaatusel ilmneb, et spetsifitseerimata on jäänud veel mingeid infovarasid, tuleb uurida nende seoseid juba liigitatud infovaradega ja määrata selle põhjal turbeaste.

3.3 Turvameetmete määramine

Kui kõigi infovarade nõutav turbeaste on määratud, tuleb leida igale infovarale vastavad tüüpmoodulid jaotisest 5 (ISKE_kataloogid_7_00.pdf). Tüüpmoodulite spetsifikatsioonides on ka loetelu rakendamisele kuuluvatest turvameetmetest.

Seejuures tuleb silmas pidada etalonturbe kihilisust. See tähendab, et astme M rakendamiseks tuleb rakendada astme L ja astme M turvameetmed ning astme H rakendamiseks tuleb rakendada astme L, astme M ja astme H turvameetmed.

Kõrgeima kihi meetmed jagunevad

kohustuslikeks (kataloogi H alamkataloogi HG meetmed) ja
tingimuslikeks (kataloogi H alamkataloogide HK, HT, HS meetmed).

Tingimuslike meetmete rakendamine sõltub moodulirühma kõrgeima tasemega turvaosaklassi(de)st:

K3 korral tuleb rakendada kõik alumises tabelis loetletud HK-meetmed

T3 korral tuleb rakendada kõik alumises tabelis loetletud HT-meetmed

S3 korral tuleb rakendada kõik alumises tabelis loetletud HS-meetmed

Turvameetmete määramist tuleb alustada moodulirühmaga B1 ja mooduliga B1.0, mis määrab infoturbe halduse meetmed.

Seejärel tuleb määrata turvameetmed kõrgeima turbeastmega infovaradele ning saavutada nende kiire kihthaaval rakendamine.

Edasine varade käsitlemise järjestus pole eriti oluline ja võib sõltuda konkreetsetest tingimustest.

Kui kõik turvameetmed on määratud, tuleb kontrollida kõigi moodulispetsifikatsiooni ohtude veeru ja kataloogi G (failist ISKE_ohtude_kataloog_7_00.pdf) andmetega võrreldes tegelikku ohusituatsiooni võimalike kataloogis puuduvate ohtude avastamiseks. Kui selliseid uusi ohte ilmneb, tuleb uurida, kas määratud etalonmeetmed on nende tõrjeks piisavad või tuleb rakendada veel mingeid lisameetmeid.

4 Kasutatud mõisted ja lühendid

Käesolevas seletussõnastikus selgitatakse neid mõisteid ja termineid, mida ei leia akit.cyber.ee sõnastikust ega ISO/IEC 27000 „Turbemeetodid, infoturbe halduse süsteemid , ülevaade ja sõnavara.

Andmekogu

Andmekogu 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.

Andmete omanik (sageli nimetatakse ka „peakasutaja“)

Isik, kes vastutab andmete eest terve elutsükli jooksul (s.t. vastutab muuhulgas andmete loomise, klassifitseerimise, kasutamise, ligipääsude reguleerimise ja administreerimise eest). See, et isik on käesoleva juhendi mõistes andmete „omanik“, ei tähenda, et isikul on tegelikud omandiõigused nende varade suhtes. Andmete omanik delegeerib üldjuhul andmete ja süsteemide, milles andmed paiknevad, tehnilise administreerimise IT osakonnale. IT osakond tavaliselt haldab ja administreerib infovarasid andmete omaniku eest ja vastavalt andmete omaniku poolt esitatud nõuetele. IT osakond võib omakorda delegeerida mõningaid haldamise ja administreerimise aspekte edasi, näiteks välisele teenusepakkujale. Osapool, kellele niimoodi funktsioone delegeeriti, vastutab oma ülesannete täitmise eest, kuid ei muutu käesoleva juhendi mõistes andmete omanikuks.

Andmete turvaanalüüs

Turvaklassi määramiseks sooritatav andmete tähtsuse hindamine ning andmete turvalisuse puudumisest tulenev kahjude hindamine.

Audit

Audit on süstemaatiline kontroll etteantud turvaeeskirja sobivuse ja selle järgimise üle. Audit peab olema sõltumatu ja neutraalne.

BSI (*Bundesamt für Sicherheit in der Informationstechnik*, Saksamaa Infoturbeamet)

Asutus, mis arendab ja haldab ISKE aluseks olevat etalonturbe käsiraamatut *IT-Grundschutzhandbuch*, vt http://www.bsi.bund.de/index.htm

Digitaalne allkiri

Digitaalne allkiri on kontrollinformatsioon, mis lisatakse sõnumile või failile, ja mida iseloomustavad järgmised omadused:

- digitaalne allkiri võimaldab selle looja üheselt kindlaks määrata;

- digitaalne allkiri võimaldab kontrollida, kas fail, millele on lisatud digitaalne allkiri, on identne failiga, mis tõepoolest allkirjastati.

Etalonmeetmed

Tüüpsed katalogiseeritud ja valimismetoodikaga varustatud turvameetmed, mille hulgast tehtav valik sõltub turvaklassist ja andmeid töötleva infosüsteemi koostisest.

Etalonturbe astmelisus

ISKE metoodikas on välja toodud kolm astet: "L" – madal, "M" – keskmine, "H" – kõrge.

"Z" tähistab soovituslikke meetmeid, mis võivad osutuda vajalikeks eelkõige kõrgema turvanõudluse puhul.

"W" tähistab meetmeid, mille eesmärgiks on aidata mõista ja rakendada teisi turvameetmeid

Etalonturve

Turvameetmestik, mille rakendamine on vajalik andmete turvalisuse saavutamiseks ja säilitamiseks.

Infosüsteem

Andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talituseks vajalike vahendite, ressursside ja protsessidega.

Infoturbe juht

Ettevõtte või asutuse IT-turvaosakonna pädev isik, kes on vastutav kõigi IT-turvaküsimuste eest, osaledes IT-turvaprotsessis ja IT-turvahaldusmeeskonna töös, aidates kaasa IT-turvaeeskirja, IT-turvakontseptsiooni ja teiste dokumentide (nt hädaolukorraks valmisolek) väljatöötamisele ning planeerides ja kontrollides nende rakendamist.

ISKE

Infosüsteemide kolmeastmelise etalonturbe süsteem.

ISKE koordinaator

Roll, mille täitja ülesandeks on kogu ISKE juurutamise koordineerimine ja juhtimine asutuses.

ISKE rakendamise kord

ISKE rakendusjuhendi jaotistes 1...3 esitatud protseduurid ja meetodid ISKE rakendamiseks.

IT-etalonturbe analüüs

IT-etalonturbe analüüsi hulka kuulub modelleerimine koos vajalike turvameetmete väljaselgitamisega ja põhiturvakontroll, mille käigus võrreldakse ettevõttes või asutuses hetkel kasutuses olevat turvameetmete rakendamist sellega, milline see peaks olema.

IT-etalonturve

Mõiste „IT-etalonturve“ tähistab infoturbe haldussüsteemi ülesehitamise metoodikat, samuti IT varade kindlustamist standardturvameetmetega. Lisaks tähistatakse selle mõistega ka seisukorda, mille korral on normaalse kaitsevajadusega IT-süsteemidele vajalik rakendada standardturvameetmeid.

IT-Grundschutzhandbuch

ISKE aluseks olev BSI poolt publitseeritav etalonturbe käsiraamat (http://www.bsi.de/gshb/index.htm).

Käitavad infovarad

Varad, mis otseselt on vajalikud andmekogu töö tagamiseks (nt. rakendus, andmebaas, server jmt.);

Meetmete kataloog

IT-etalonturbe kataloogides soovitatakse igas moodulis sobivat meedet, mis on kataloogideks kokkuvõetuna liigendatud infrastruktuuriks, organisatsiooniks, personaliks, riistvaraks/tarkvaraks, kommunikatsiooniks ja valmisolekuks hädaolukorras.

Modelleerimine

Vastavalt IT-etalonturbele mõistetakse modelleerimise all ettevõtte või asutuse IT varade kaardistamist lähtudes IT-etalonturbe kataloogides sisalduvatest moodulitest. Vastavalt IT-etalonturbe kataloogi ptk 2.2 sisaldab iga moodul viidet, millisel puhul seda rakendada ja milliseid eeldusi tuleks seejuures silmas pidada.

Moodul

Mõistet kasutatakse IT-etalonturbe kataloogis sisalduvate soovituste struktureerimiseks. Moodulid on ühe tasandi (nt IT-süsteemid, võrgud) üksused. Neis kirjeldatakse osalt tehnilisi komponente (nt kaabeldus), osalt organisatoorseid meetmeid (nt hädaolukorraks valmisoleku kontseptsioon) ja erilisi rakendusvorme (nt kodune töökoht). Igas moodulis kirjeldatakse kindlat IT-komponenti ja nimetatakse ohud, samuti antakse soovitusi organisatoorsete ja tehniliste turvameetmete rakendamiseks.

RIA

Riigi Infosüsteemi Amet

RIHA

Riigi infosüsteemide haldussüsteem, vt https://riha.eesti.ee

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 vmt).

Turbeaste

Infoturbe näitaja, mis määratakse turvaklassi põhjal vastavalt ISKE rakendusjuhendis antud juhistele. ISKEs on kolm turbeastet L – madal, M – keskmine ja H – kõrge.

Turvaintsident

Sündmus ja/või sündmused, millega kaasneb andmete ja/või muude infovarade käideldavuse, tervikluse ja/või konfidentsiaalsuse kadu ja/või tekib oluline oht andmete käideldavuse, tervikluse ja/või konfidentsiaalsuse kao tekkeks.

Turvaklass

Andmete tähtsusest tulenev andmete nõutav turvalisuse tase, väljendatuna neljaastmelisel skaalal ning kolmekomponendilisena, st kolme turvaosaklassi ühendina. Andmete turvaklassi tähis moodustatakse turvaosaklasside tähistest nende järjestuses K-T-S, nt K2T3S1.

Turvaosaklass

Andmete tähtsusest tulenev infoturbe eesmärgi saavutamise nõutav tase väljendatuna neljaastmelisel skaalal. Kolmest infoturbe eesmärgist tuleneb kolm turvaosaklassi. Turvaosaklassi tähis koosneb turvaeesmärgi tähisest (nt K, T, S) ja turvataseme väärtusest (nt 0,1,2,3), nt K2.

Turvameede

Organisatsioonilised toimingud ja vahendid, tehnilised protsessid ja tehniliste vahendite rakendamine andmete ja infosüsteemide andmete turvalisuse saavutamiseks ja säilitamiseks Turvameetmeks (lühidalt meetmeks) nimetatakse kõiki tegevusi, mille eesmärgiks on turvariskide vähendamine ja nende ennetamine. Seda saab teha nii organisatoorsete kui ka inim-, tehniliste- või infrastruktuure puudutavate turvameetmete abil. Sünonüümidena kasutatakse ka mõisteid „turvaabinõu“ või „kaitsemeede“. Kasutatakse ka inglisekeelseid mõisteid *"safeguard"*, *"security measure"* või *"measure"*. Ingliskeelses keeleruumis kasutatakse *"safeguard"* kõrval tihti ka mõistet *"control"*.