



Riigi Infosüsteemi Amet

# **INFOSÜSTEEMIDE KOLMEASTMELISE ETALONTURBE SÜSTEEM ISKE**

## **Rakendusjuhend**

Version 6.00  
November 2011



## Copyright

© 2011 Riigi Infosüsteemi Amet. Kõik õigused kaitstud.

© 2011 BSI. Kõik õigused kaitstud.

Käesolev ISKE rakendusjuhend on kaitstud autoriõigustega. Dokumendi paljundamine ja allalaadimine on lubatud üksnes isiklikel ja mitteärilistel eesmärkidel. Igasugustel muudel eesmärkidel dokumendi kopeerimine, paljundamine, muutmine, tõlkimine, töötlemine, salvestamine või taasavaldamine on ilma volituseta keelatud.

---

## Sisukord

0 Muudatused ISKE rakendusjuhendi versioonis 6.00.....	4
0.1 Uuendamine ja ümbertöötamine.....	4
0.2 Muudatused moodulites.....	4
0.2.1 Lisandunud moodulid .....	4
0.2.2 Uuendatud moodulid .....	5
0.2.3 Välja jäetud moodulid.....	7
0.3 Muudatused meetmetes.....	7
0.3.1 Lisandunud meetmed.....	7
0.3.2 Uuendatud meetmed.....	8
0.3.3 Välja jäetud meetmed.....	8
0.4 Muudatused ohtudes.....	10
0.4.1 Lisandunud ohud.....	10
0.4.2 Välja jäetud ohud.....	11
1 Lühülevaade.....	13
1.1 Rakendusala.....	13
1.2 Etalonturbe olemus.....	13
1.3 Astmeline etalonturve.....	13
1.4 ISKE rakendusjuhendi struktuur.....	14
1.5 ISKE rakendamine.....	14
1.5.1 ISKE rakendamise 11 sammu.....	15
1.6 Etalonturbe täiendamine.....	17
1.7 Allikad ja lisateabi viited.....	17
2 Infovarade vajaliku turvataseme määramine.....	18
2.1 Infosüsteemide analüüs.....	18
2.1.1 Infosüsteemide inventuur.....	18
2.1.2 Infovarade spetsifitseerimine.....	18
2.1.3 Infovarade grupeerimine.....	20
2.2 Turvalisuse näitajad.....	20
2.2.1 Informatsioon ja andmed.....	20
2.2.2 Informatsiooni turvalisus ja turvaeesmärgid.....	20
2.3 Andmete turvaklassi määramine.....	21
2.4 Muude infovarade turvaklassi määramine.....	25
3 Nõutava turbeastme ja turvameetmestiku määramine .....	27
3.1 Turbeastme määramine turvaklassi järgi.....	27
3.2 Turvaklassita infovarade turbeastme määramine.....	28
3.3 Turvameetmete määramine.....	28
4 Kasutatud mõisted ja lühendid.....	29

---

## 0 Muudatused ISKE rakendusjuhendi versioonis 6.00

---

### 0.1 Uuendamine ja ümbertöötamine

ISKE rakendusjuhendi versioonis 6.00 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 H turbeastme katalooge.

Rakendusjuhendi versioonis 6.00 lisandus ISKE rakendamise 11. samm - konfiguratsiooni ja muudatuste halduse käiguhoidmine. Lisaks viidi 2011. aastal läbi kataloogide tervikluse kontroll, mille käigus ühtlustati meetmete ja moodulite nimetused dokumendi lõikes.

ISKE kataloogide versioonis 6.00 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](mailto:iske@ria.ee).

### 0.2 Muudatused moodulites

#### 0.2.1 Lisandunud moodulid

- **B 1.15 Andmete kustutamine ja hävitamine**

Kasutusest kõrvaldatud, edasi antud ning pruugituna ostetud andmekandjatel võib tihti leiduda konfidentsiaalset infot, mis poleks tohtinud seda teavet haldavast institutsioonist kunagi väljuda. Moodul B 1.15 *Andmete kustutamine ja hävitamine* kirjeldab, kuidas valida meetodeid, mille abil on võimalik andmeid ja andmekandjaid täielikult ja turvaliselt kustutada või hävitada. Salvestatud andmete väärkasutuse vältimiseks peab igal institutsioonil olema kindlaks määratud protsess, mis sätestab andmekandjate kustutamise ja hävitamise. Protsessi peavad olema kaasatud nii digitaalsed andmekandjad (nt kõvakettad) kui ka analoogandmekandjad (nt paberdokumendid).

- **B 1.16 Nõuete haldus**

Igal institutsioonil tuleb tuvastada kõik enda ja oma tööprotsesside jaoks olulised seadustest tulenevad, lepingulised ja muud ettekirjutused. Institutsioon peab tagama nende järgimise, rakendades selleks vajalikke ülevaatemeetmeid. Antud teema on mõningate uute seaduste jõustumise tõttu veelgi suurema tähelepanu alla sattunud ning seetõttu käsitletakse seda aina sagedamini märksõna all *Compliance* (vastavus). Moodul B 1.16 *Nõuete haldus* ei sisalda ühtki päris uut olulist meetet. Parema võrdluse saamiseks normidega ISO 27001 ja 27002 on kokku kogutud meetmed, mis käsitlevad *compliance*-teemavaldkonna juhtsüsteeme.

---

- **B 3.210 Klient Windows Vista all**

Lisandunud on moodul B 3.210 *Klient Windows Vista all*, mis täiendab nende moodulite ridu, mis käsitlevad Windowsi operatsioonisüsteemide turvalist käitamist. Käesolev moodul käsitleb klient-operatsioonisüsteemi Windows Vista versiooni Enterprise. Kasutajale selgitatakse turbealaseid kontseptsioone ja antakse konkreetsete konfiguratsioonide põhjal turbealaseid soovitusi.

- **B 3.304 Virtualiseerimine**

- **B 3.305 Terminaliserver**

- **B 4.8 Bluetooth**

- **B 5.17 Samba**

Moodulis B 5.17 *Samba* on peamiselt vaatluse all Samba turvaomadused. Samba on tasuta kättesaadav autentimis-, faili- ja printimisteenus, mis võimaldab omavahel koostööd teha nii Microsoft Windowsi operatsioonisüsteemidel kui ka Unixi maailmal.

- **B 5.18 DNS-server**

- **B 5.19 Interneti kasutamine**

## 0.2.2 Uuendatud moodulid

- B 1.5 Andmekaitse
- B 3.401 Kodukeskjaam (PBX)
- B 4.4 Virtuaalne privaatvõrk (VPN)
- B 5.3 Rühmatarkvara
- B 5.4 Veebiserver
- B 5.8 Kaugtöö

Ülal nimetatud moodulite sisu on ISKE-s uuendatud.

Meetmete või ohtude määratlus muutus järgnevates moodulites:

- B 1.0
- B 1.1
- B 1.2
- B 1.3
- B 1.6
- B 1.7
- B 1.8
- B 1.9

- 
- B 1.10
  - B 1.11
  - B 1.12
  - B 1.14
  - B 2.1
  - B 2.4
  - B 2.6
  - B 2.7
  - B 2.9
  - B 2.11
  - B 3.101
  - B 3.102
  - B 3.106
  - B 3.107
  - B 3.201
  - B 3.202
  - B 3.203
  - B 3.204
  - B 3.207
  - B 3.209
  - B 3.301
  - B 3.302
  - B 3.303
  - B 3.401
  - B 3.406
  - B 4.1
  - B 4.3
  - B 4.4
  - B 4.5
  - B 5.3
  - B 5.4
  - B 5.9

- 
- B 5.15
  - B 5.16

### **0.2.3 Välja jäetud moodulid**

- B 3.103 - Server Windows NT all
- B 3.205 - Klient Windows NT all
- B 3.403 - Automaatvastaja
- B 5.1 - Võrdõigusteenus (p2p)
- B 5.10 – Internet Information Server (IIS)
- B 5.11 – Apache veebiserver

## **0.3 Muudatused meetmetes**

### **0.3.1 Lisandunud meetmed**

- M 1.70 – M 1.74
- M 2.105
- M 2.431 – 2.474
- M 3.67 – 3.82
- M 4.56
- M 4.136 – M 4.150
- M 4.161 – M 4.167
- M 4.198 – M 4.199
- M 4.201 – M 4.231
- M 4.234 – M 4.252
- M 4.254 – M 4.298
- M 4.325 – M 4.369
- M 5.7 – M 5.10
- M 5.13 – M 5.21
- M 5.24 – M 5.25
- M 5.29 – M 5.35
- M 5.39
- M 5.44 – M 5.47
- M 5.51 – M 5.52
- M 5.54
- M 5.56 – M 5.64
- M 5.66 – M 5.72
- M 5.76 – M 5.81
- M 5.83 – M 5.96

- 
- M 5.98 – M 5.100
  - M 5.108 – M 5.112
  - M 5.115 – M 5.141
  - M 5.151 – M 5.164
  - M 6.110 – M 6.145

Lisaks on oluliselt muudetud, uuendatud ja täiendatud ISKE H turbeastme katalooge.

### **0.3.2      Uuendatud meetmed**

- M 2.27
- M 2.32
- M 2.122
- M 2.123
- M 2.173
- M 2.174
- M 2.176
- M 2.392
- M 4.5
- M 4.6
- M 4.10
- M 4.11
- M 4.97
- M 4.98
- M 6.26
- M 6.90

### **0.3.3      Välja jäetud meetmed**

M 2.54 – M 2.58

M 2.67 – M 2.68

M 2.91 – M 2.94

M 2.118 – M 2.121

---

M 2.267 – M 2.271

M 2.275

M 3.16

M 3.19

M 3.36 – M 3.37

M 4.8

M 4.12

M 4.38 – M 4.39

M 4.45 – M 4.46

M 4.50 – M 4.51

M 4.53 – M 4.55

M 4.58

M 4.76 – M 4.77

M 4.174 – M 4.175

M 4.178 – M 4.197

M 5.36 – M 5.37

M 5.41 – M 5.43

M 5.53

M 5.55

M 5.82

M 5.101 – M 5.107

M 6.2 – M 6.15

M 6.28

M 6.30

M 6.40

M 6.42

M 6.44

M 6.63

M 6.85 – M 6.87

M 6.89

---

## **0.4 Muudatused ohtudes**

### **0.4.1 Lisandunud ohud**

- G 1.1 – G 1.19
- G 2.1 – G 2.13
- G 2.28 – G 2.29
- G 2.32
- G 2.36 – G 2.37
- G 2.54 – G 2.55
- G 2.60
- G 2.96
- G 2.100
- G 2.148 – G 2.154
- G 3.1
- G 3.3
- G 3.7 – G 3.9
- G 3.13
- G 3.16
- G 3.28
- G 3.36 – G 3.38
- G 3.43 – G 3.45
- G 3.79
- G 3.99 – G 3.107
- G 4.10
- G 4.12
- G 4.20
- G 4.22
- G 4.32 – G 4.33
- G 4.35
- G 4.37

- 
- G 4.39
  - G 4.60
  - G 4.74 – G 4.82
  - G 5.2
  - G 5.9 – G 5.16
  - G 5.19 – G 5.21
  - G 5.23 – G 5.29
  - G 5.42 – G 5.44
  - G 5.48
  - G 5.71 – G 5.73
  - G 5.75
  - G 5.77 – G 5.78
  - G 5.85
  - G 5.87 – G 5.88
  - G 5.110 – G 5.112
  - G 5.133
  - G 5.143
  - G 5.147 – G 5.162

#### **0.4.2 Välja jäetud ohud**

- G 2.25
- G 2.30 - G 2.31
- G 2.56
- G 2.65
- G 2.94
- G 2.97
- G 3.15
- G 3.18 - G 3.20
- G 3.57 – G 3.59

- 
- G 3.62 – G 3.63
  - G 4.8
  - G 4.18 – G 4.19
  - G 4.29
  - G 5.17
  - G 5.36 – G 5.38
  - G 5.45 - G 5.47
  - G 5.74
  - G 5.76
  - G 5.108 – G 5.109
  - G 5.127

---

# 1 Lühiülevaade

---

ISKE põhineb turvet vajavate infovarade kirjeldamisel tüüpmodulite abil ning sisaldab vahendeid iga tüüpmoduli turvaklassi määramiseks ja mooduli nõutava turbeastme määramiseks selle turvaklassi järgi. Sõltuvalt tüüpmoduli 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

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

"Minimaalne" tähendab seda, et nõutava turvaseme saavutamiseks tuleb rakendada kõik konkreetse infovara tüübi ja konkreetse nõutava turvaseme kohta spetsifitseeritud kohustuslikud meetmed. Lisaks on igal turvasemel soovituslikud meetmed, mida soovitatakse rakendada, kuid mis ei ole kohustuslikud.

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

Infosüsteemid töötavad pidevalt muutuv keskkonnas, kus tekib üha uusi ohte. Seetõttu ei saa etalonmeetmestik püsida muutumatuna, vaid vajab regulaarset uuendamist. Selliste uuenduste sooritamise 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. 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 tüüpmodulite turvaspetsifikatsioonide (5 rühma, 77 tüüpi) kataloog B, vt jaotis 5 ISKE\_kataloogid\_6\_00.pdf failist,
- 4) ohtude (5 gruppi, 478 liiki) kataloog G, vt jaotis 6 ISKE\_kataloogid\_6\_00.pdf failist,
- 5) turbeastmete L ja M turvameetmete (6 rühma, 1096 liiki) kataloog M, vt jaotis 7 ISKE\_kataloogid\_6\_00.pdf failist,
- 6) turbeastme H turvameetmete (4 rühma, 222 liiki) kataloog H, vt jaotis 8 ISKE\_kataloogid\_6\_00.pdf failist.

Viidatud võrkeelsetest alusmaterjalidest võib leida muid abivahendeid: meetodilisi 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. ISKE rakendamine asutuses ei ole mitte 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.

---

## 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 tüüpmodulite kataloogi B (jaotis 5 failist ISKE\_kataloogid\_6\_00.pdf), võrdleb seda infovarade spetsifikatsioonidega ja märgib spetsifikatsioonidesse tüüpmodulite tähised vastavalt juhistele [jaotistes 3.1](#) ja [3.2](#). Kui tüüpmodulite kataloogi läbivaatusel ilmneb veel spetsifitseerimata varasid, spetsifitseerib ta nad töö selles järgus. Tüüpmodulid, 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\_6\_00.pdf) ja turbeastme H korral ka kataloogist H (jaotis 8 failist ISKE\_kataloogid\_6\_00.pdf).
8. Infoturbe spetsialist koos juhtkonna esindaja ja asutuse IT eest vastutava töötajaga koostab plaani infoturbe halduse (moodul B1.0) meetmete rakendamiseks, sejärel 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/IEC TR 13335 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 tüüpmodulite 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 [www.ria.ee/27220](http://www.ria.ee/27220)) alusel tegelikku turvaolukorda, arvestades tegelikke ohte konkreetse infosüsteemi lõikes. Kui ilmneb mingeid ohte, mida tüüpmoduli 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, tüüpmodulite, turvaklasside ja meetmete osas tuleb asutuses kasutusel olevasse töövahendisse sisestada, et oleks tagatud ajakohane ülevaade asutuse infovaradega toimuvast.

**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.**

**Rakendusjuhendis on lisaks veel “z” ja “w” turvameetmed.**

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

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

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. tüüpmodulite spetsifitseerimine;
7. turvameetmete loetelu koostamine;
8. turvameetmete rakendamise plaani koostamine;
9. turvameetmete rakendamine;
10. tegeliku turvaolukorra kontroll;
11. konfiguratsiooni- ja muudatustehalduse sisseviimine.

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 mõjutab.

---

## 1.6 Etalonturbe täiendamine

ISKE rakendusjuhend ilmub täiendatud kujul uue versioonina kord aastas, sõltuvalt allikmaterjali ([jaotis 1.7](#)) uute versioonide avaldamisest. Iga järgmine versioon võib sisaldada uusi tüüpmoduleid koos vastavate turvameetmetega ja/või uusi turvameetmeid senistele tüüpmoduleitele. 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-Kataloge 2011- 12. Ergänzungslieferung \(.pdf\)](#)

Turbehalduse korraldamisel võib mõningaid kasulikke juhiseid leida järgmistest standarditest EVS-ISO/IEC 27002. Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhised 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 tüüpmoduli 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 2003*, 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 privaativõrgu 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 kokkulepitul kujul ja kandjal, näiteks paberdokumendina, digitaalsalvestisena magnetkettal, mikrofilmil, 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 turvemetoodikate 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 volitamatu 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 volitamatu muutunud. Kõik andmed peavad alati olema seostatavad nende looja, loomisaja, konteksti jms asjaoludega ning nende seoste rikkumisel, samuti andmete endi kaotamisel 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 turvasemest 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 turvaseme, 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 on soovitatav lasta need **asutuse juhtkonnal kinnitada.**

Turvaspetsialisti seisukohalt võib turvasemete 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 hindamiskaalat. 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** – töökindlus – madal, lubatud summaarne tööseisak on üle 1 ööpäeva nädalas;

**K1** – töökindlus – lubatud summaarne seisak nädalas kuni 1 ööpäev;

**K2** – töökindlus – lubatud summaarne seisak nädalas kuni 2 tundi;

**K3** – töökindlus – lubatud summaarne seisak nädalas kuni 10 minutit;

**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 reaajas.

**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.

**Andmete turvaklass** on kolme turvaosaklassi konkreetne kombinatsioon. Nende kõikvõimalike kombinatsioonide arv on  $4 \times 4 \times 4$ , 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 etalonurvameetmete määramisel. Andmeturbe eesmärkide tagamiseks peavad olema rakendatud turvameetmed, mis vastavad infovara turvaklassile.

Turvameetmed valitakse turvaklassile vastavast etalonmeetmete kataloogist konkreetse infovara etalonurbe 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, rikest 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 avalikustamiseks 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**

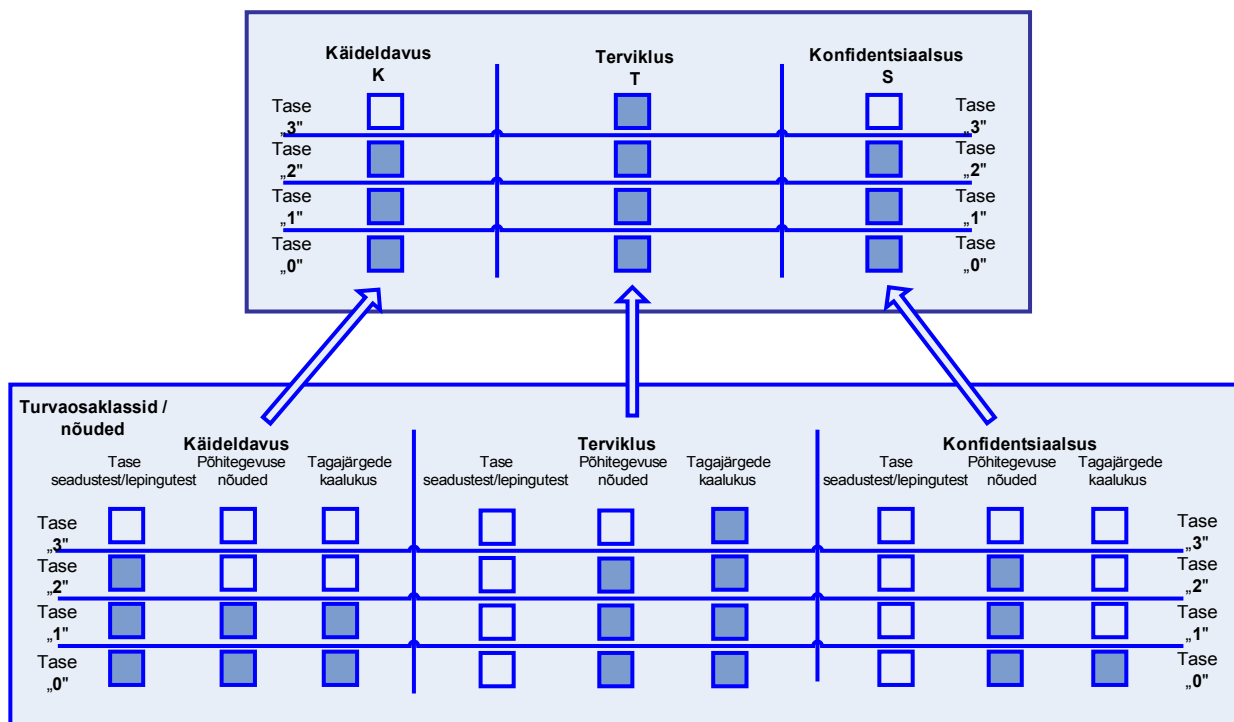
Tagajärgede kaalukus tähendab turvaintsidentist tekkivate kahjude hindamist. Kahjusid võib hinnata neljatasemelisel skaalal:

**R<sup>0</sup>** – turvaintsidentiga (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmisega) ei kaasne märkimisväärseid kahjusid;

**R<sup>1</sup>** – 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<sup>2</sup>** - 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<sup>3</sup>** - 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 inimestele 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 seotud 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 infoturbspetsialistiga.**

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 tüüpmodulite kataloogist (jaotis 6 failist ISKE\_kataloogid\_6\_00.pdf) sellele infovarale vastava tüüpmoduli 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 tüüpmodulite 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 tüüpmodulitena (jaotis 5 failist ISKE\_kataloogid\_6\_00.pdf), mis kuuluvad peamiselt tüüpmodulite rühma B1.

Kogu tüüpmodulite rühmale B1 tuleb määrata kõrgeim [jaotises 3.1](#) määratud turbeaste.

Kui tüüpmodulite 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 tüüpmodulid jaotisest 5 (ISKE\_kataloogid\_6\_00.pdf). Tüüpmodulite spetsifikatsioonides on ka loetelu rakendamisele kuuluvatest turvameetmetest.

Seejuures tuleb silmas pidada etaloniturbe 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 (jaotis 6 failist ISKE\_kataloogid\_6\_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 mõningaid infoturbes ja IT-etalonturbes kasutatavaid olulisi mõisteid.

### **Administraator**

Administraator haldab ja hooldab arvuteid ning arvutivõrke. Ta installeerib operatsioonisüsteeme ja rakendusprogramme, loob uusi kasutajatunnuseid ja jagab tööks vajalikke õigusi. Seejuures on tal tavaliselt ulatuslik või isegi piiramatult ligipääs hallatavatele arvutitele või võrkudele.

### **Andmekaitse**

Andmekaitse peab üksikisikut kaitsma selle eest, et tema isikuandmeid kasutades ei kahjustataks tema isikuõigusi. Andmekaitseks nimetatakse seepärast isikuga seotud andmete kaitset igat liiki kuritarvituste eest kolmandate isikute poolt (mitte segi ajada mõistega „andmete turvalisus“). Inglise keeles on mõistele „andmekaitse“ kaks vastet: „*data protection*“ tähistab andmekaitset kui õiguslikku terminit, mõistet „*privacy*“ kasutatakse aga ühiskondlikku eluviisi (privaatsfääri kaitse) kirjeldamiseks. Viimane termin on kasutusel peamiselt ameerika keeleruumis, kuid viimasel ajal üha enam ka ELS.

### **Andmekaitse haldus**

Andmekaitse haldusega tähistatakse protsesse, mis on vajalikud tagamaks andmekaitse õiguslike nõuete rakendamist informatsioonitöötamise planeerimisel, kasutusele võtmisel, kasutamisel ja pärast kasutuselt kõrvaldamist.

### **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.

---

## **Andmete turvalisus**

Andmete turvalisuse all mõistetakse andmete kaitsmist nende konfidentsiaalsuse, käideldavuse ja tervikluse nõudest lähtuvalt.

### **Andmevarundus (ingl. k. „backup“)**

Andmevarundus tähendab, et andmete võimaliku kaotsimineku puhuks tehakse olemasolevatest andmetest turvakoopiaid. Andmevarundus hõlmab kõiki tehnilisi ja organisatoorseid meetmeid, et kindlustada süsteemide käideldavus, terviklus ja järjekindlus (*consistency*), kaasa arvatud neis süsteemides salvestatud ja töötlemise eesmärkidel kasutatavad andmed, programmid ja toimingud.

Reeglipärane andmevarundus tähendab, et rakendatavad meetmed võimaldavad pärast käideldavuse, tervikluse või järjekindluse nõude rikkumist kahjutoonud juhtumi poolt sõltuvalt andmete tundlikkusest kas kohe või lühikese aja pärast taastada süsteemide, andmete, programmide või toimingute endise seisundi.

### **Arvutiviirus**

Arvutiviirus on sõltumatu alamprogramm, mis ennast taastotes teostab süsteemides, teistes programmides või nendega seotud keskkondades manipulatsioone, mis ei ole kasutaja poolt kontrollitavad.

### **Autentimine(ingl. k. „authentication“)**

Autentimiseks nimetatakse kommunikatsioonipartneri tõendamist, et ta on tõepoolest see, kelle ta ütleb end olevat. Seda võib teha parooli sisestamise, kiipkaardi või biomeetria abil.

### **Autentsus**

Mõistega „autentsus“ tähistatakse funktsiooni, mis tagab, et kommunikatsioonipartner on tõepoolest see, kelle ta ütleb end olevat. Autentse informatsiooni puhul on tagatud, et see pärineb nimetatud allikast. Mõistet kasutatakse mitte ainult isikute, vaid ka IT-komponentide ja rakenduste identsuse kontrollimisel.

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

### **Autoriseerimine**

Autoriseerimise puhul kontrollitakse, kas isikule, IT-komponendile või rakendusele on antud õigus teatud kindla toimingu läbiviimiseks.

### **Audit**

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

### **Biomeetria**

Biomeetria all mõistetakse isiku automatiseeritud tuvastamist tema kehaliste tunnuste põhjal. Kehalisi tunnuseid kasutatakse selleks, et kasutajat saaks eriliste omaduste abil üheselt autentida. Autentimiseks võib kasutada üht või mitut järgnevat biomeetrilist tunnust:

- iiris
- sõrmejäljed
- näo proportsioonid

- 
- hääle ja kõne iseärasused
  - käekiri
  - arvuti klaviatuuri kasutamise eripära

### **Black-Box turvatestimine**

*Black-Box* testimine tähendab, et simuleeritakse ründaja käitumist, eeldades, et ründaja ei oma üldse või omab vaid pinnapealset informatsiooni rünnatava kohta.

### **Brauser**

Sõnaga „brauser“ (sõnast „to browse“, eesti keeles „raamatus tuhnima“, „lehitsema“, „ringi uitama“) tähistatakse tarkvara, mis võimaldab pääseda interneti. Programm tõlgendab saabuvasid andmeid ja esitab need teksti ja pildina ekraanile.

### **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>

### **Business Continuity Management**

Mõistega „*Business Continuity Management*“ (BCM) tähistatakse kõiki organisatoorseid, tehnilisi ja personali puudutavaid meetmeid, mis on vajalikud asutuse või ettevõtte põhitegevuse jätkamiseks pärast hädaolukorra tekkimist või turvasüsteemi riket. BCM toetab ka tegevusprotsesside jätkuvat toimimist pikemaajaliste rikete või häirete korral.

### **„Demilitariseeritud“ tsoon**

„Demilitariseeritud“ tsoon on vahevõrk, mis asub sisevõrgu ja interneti vahel ning mis ei kuulu ei ühe ega teise võrgu juurde. Tegemist on omaette võrguga, mis ei ole aga nii tugevalt turvatud nagu sisevõrk. Lihtsate turvalüüside puhul luuakse DMZd tavaliselt paketi filtri kolmandale liidesele. Kui turvalüüs koosneb alusstruktuurist paketi filter – rakenduslüüs ehk *Application-Level-Gateway* (ALG) – paketi filter on ALG liides tavaliselt DMZ-liideseks. Juhul kui paketi filteril või ALG-l on rohkem kui kolm liidest, võib moodustada veel teisigi DMZid.

### **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 osutada 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.

### **Haavatavus (ingl. k. "vulnerability")**

Haavatavus on kaitse seisukohalt IT-süsteemi või institutsiooni oluline viga. Selle põhjused võivad olla kontseptsioonis, kasutatavates algoritmides, teostuses, konfiguratsioonis, rakenduses ja ka organisatsioonis. Haavatavus võib viia selleni, et oht võib muutuda reaalsuseks ja institutsiooni või süsteemi kahjustatakse. Haavatavuse tõttu muutub objekt (institutsioon või süsteem) ohule vastuvõtlikuks.

### **Hädaolukord**

Hädaolukord on kahju tekitav olukord, kus institutsiooni protsessid või ressursid ei toimi nii, nagu nad peaksid toimima. Vajalike protsesside ja ressursside käideldavust ei õnnestu selleks ette nähtud aja jooksul taastada. Igapäevased tööprotsessid on tugevalt pärsitud. Võimalikke teenindusleppeid (Service Level Agreements, SLA) ei suudeta täita. Tekivad suured kuni väga suured kahjud, mis mõjutavad märkimisväärselt ja vastuvõetamatult suurel määral ettevõtte aasta tulemit või ametiasutuste ülesannete täitmist. Hädaolukordade kõrvaldamiseks igapäevastest tööprotsessidest enam ei piisa. Nende kõrvaldamiseks läheb eraldi tarvis hädaolukordade likvideerimiseks mõeldud töökorraldust.

### **Infosüsteem**

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

### **Infotehnoloogia (IT)**

Infotehnoloogia (IT) hõlmab kõiki tehnilisi vahendeid, mis on vajalikud informatsiooni töötlemiseks või edastamiseks. Informatsiooni töötlemise alla kuuluvad info kogumine, arvelevõtmine, kasutamine, salvestamine, ülekandmine, programmikohane töötlemine, internetis esitamine ja informatsiooni väljastamine.

### **Infoturbe haldus**

Antud mõiste all peetakse silmas planeerimis- ja juhtimisülesandeid, mis on vajalikud läbimõeldud ja mõjusa infoturbe loomiseks ja katkematuks rakendamiseks. Samadel põhjustel, mida nimetati eelnevate mõistete „infoturbe“ ja „IT-turbe“ puhul, kasutatakse IT-etalonturbes lühemat mõistet „IT-turbe haldus“.

### **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 hädaolukorraleks valmisolek) väljatöötamisele ning planeerides ja kontrollides nende rakendamist.

### **Infoturve**

Infoturbe eesmärgiks on kaitsta informatsiooni, olgu siis tegemist paberil, arvutis või ka peas salvestatud informatsiooniga. See on turvameetmete loomise, valimise ja rakendamise protsesside kogum. IT-turbe tegeleb esmajoonel elektrooniliselt salvestatud informatsiooni ja selle töötlemise kaitsmisega. Mõiste „infoturbe“ on seetõttu laiem kui IT-turve ning see leiab järjest enam

---

kasutamist. Kuna aga kirjanduses võib ikka veel leida põhiliselt mõistet „IT-turve“, kasutatakse just seda mõistet selles, nagu ka teistes IT-etalonturbe alastes publikatsioonides.

### **Infovara**

Varad, kuhu kuuluvad andmed, andmebaasid, rakendustarkvara, süsteemitarkvara, arvutid, serverid, marsruuterid, kommutaatorid, andmekandjad, serveriruumid, majad jmt. Infovarad võib liigitada käitavateks, toetavateks ja autonoomseteks infovaradeks (vt. eraldi definitsioone).

### **Infrastruktuur**

IT-etalonturbes tähistatakse mõiste „infrastruktuur“ informatsiooni töötlemise ja Infotehnoloogia paigutamise jaoks kasutatavaid hooneid, ruume, energiavarustust, kliimaseadmeid ja kaabeldust. Siia ei kuulu IT-süsteemid ja võrguühenduselemendid.

### **Intranet**

Intranet on sisemine võrk, mis on võrgu tööshoidja täieliku kontrolli all (kindel asutus või ettevõtte). Tavaliselt on pääs intranetti teistest võrkudest (nt internet) kaitstud tulemüüriaga.

### **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**

Infotehnoloogia.

### **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>).

### **IT-turbe haldus**

IT-turbe haldus tähistab planeerimis-, juhtimis- ja kontrollülesandeid, mis on vajalikud läbimõeldud ja mõjusa infoturbe loomiseks ja katkematuks rakendamiseks. Tegemist on pideva protsessiga, mille käigus tuleb strateegiad ja kontseptsioonid nende jõudluse ja mõjususe seisukohalt korduvalt üle vaadata ja neid vajadusel täiendada.

---

## **IT-turbe põhiväärtused**

IT-etaloniturbes vaadeldakse põhiväärtusena konfidentsiaalsust, käideldavust ja terviklust. Igal kasutajal on kaitsevajaduse kindlaks määramisel loomulikult õigus põhiväärtustena käsitleda ka muid omadusi, kui see on talle vajalik. Teisteks IT-turbes kasutatavateks olulisteks üldmõisteteks on näiteks:

- autentsus (*authenticity*)
- kohustuslikkus (*liability*)
- usaldusväärsus (*trustworthy*)
- salgamise vääramine (*non-repudiation*)

## **IT-turvakontsept**

IT-turvakontsept on vajalik IT-turvastrateegia rakendamiseks. Selles on kirjas institutsiooni poolt planeeritavad sammud, et saavutada enda poolt püstitatud turvaeesmärgid. IT-turvakontsept on ettevõtte või asutuse IT-turvaprotsessi keskne dokument, millest iga konkreetne IT-turvameede peaks lähtuma.

## **IT-turvakontseptsioon**

IT-turvakontseptsiooni koostamine on IT-turbe halduse üks olulisemaid ülesandeid. Lähtuvalt IT-struktuuri analüüsi tulemustest ja kaitsevajaduste kindlaks määramisest identifitseeritakse selles vajalikud IT-turvameetmed ja pannakse need kirja IT-turvakontseptsiooni.

## **IT-struktuuri analüüs**

IT-struktuuri analüüs sisaldab nõutud informatsiooni valitud IT varade, IT-rakendamise, IT-süsteemide, võrkude, ruumide, hoonete ja ühenduste kohta selliselt, et see oleks abiks IT-etaloniturbes kirjeldatud järgnevate sammude rakendamiseks.

## **IT-turve**

IT-turve väljendab olukorda, milles on Infotehnoloogia kasutamisel tekkivad riskid – põhjustatuna kas ohtudest või haavatavast kohast - vajalike meetmete abil viidud miinimumini. IT-turve on seega seisund, milles on informatsiooni ja Infotehnoloogia konfidentsiaalsus, terviklus ja käideldavus kaitstud tänu vastavate meetmete rakendamisele. IT-turbes on kolm põhiväärtust: konfidentsiaalsus, käideldavus ja terviklus. Igal kasutajal on kaitsevajaduse kindlaks määramisel loomulikult õigus põhiväärtustena käsitleda ka muid omadusi, kui see on talle vajalik. Teisteks IT-turbes kasutatavateks olulisteks üldmõisteteks on näiteks:

- autentsus
- kohustuslikkus
- usaldusväärsus
- salgamise vääramine

## **IT varad**

IT varade all mõistetakse infrastruktuuriliste, organisatoorsete, inim- ja tehniliste komponentide kogumit, mis on vajalik teatud kasutusvaldkonna informatsioonitöötamise ülesannete täitmiseks. IT varad võib hõlmata nii ühe institutsiooni kogu infotehnoloogiat kui ka üksikuid valdkondi, mis on liigendatud vastavalt organisatoorsetele struktuuridele (nt osakonna võrk) või silmas pidades ühist IT-kasutajaskonda (nt personaliinfosüsteem).

---

## Juurdepääs

Juurdepääsu all mõistetakse informatsiooni või andmete kasutamist. Juurdepääsuõiguses määratakse kindlaks, millised isikud oma tööülesanne tõttu või millised IT-rakendused on volitatud informatsiooni, andmeid või ka IT-rakendusi kasutama või läbi viima *transaktsioone*.

## Kahjurprogramm / Kahjurtarkvara (ingl. k. Malware)

Mõisted „kahjustusfunktsioon“, „kahjurprogramm“, „kahjurtarkvara“ ja „malware“ kasutatakse tihti sünonüümidena. Sõna „malware“ on tuletatud inglisekeelsest väljendist „*Malicious software*“ ning see tähistab tarkvara, mis on loodud eesmärgiga teostada soovimatuid ja enamasti kahjulikke funktsioone. Olgu siin nimetatud arvutiviirused, ussid ja trooja hobused. Kahjurtarkvara on loodud tavaliselt üht kindlat rakendussüsteemi varianti silmas pidades, enamasti üldlevinud süsteemide ja programmide jaoks.

## Kahjustusfunktsioon

Kahjustusfunktsiooniks peetakse kasutajapoolset soovimatut funktsiooni, mis võib ettekatsematult või ka teadlikult juhitud ohustada IT-turvalisust.

## Kaitsevajadus

Kaitsevajadus kirjeldab, milline kaitse on piisav ja sobilik tegevusprotsessidele, nende käigus töödeldavale informatsioonile ning kasutatavale infotehnoloogiale.

## Kaitsevajaduse määratlemine

Antud mõiste tähendab, et iga konkreetne institutsioon omab sobilikke kriteeriume, mille alusel määratleda, millist kaitsevajaduste kategooriat IT-komponentidele rakendada.

## Kasutajatunnus (sageli ka kasutajakonto)

Kasutajatunnus on nimi, millega kasutaja end IT-süsteemis identifitseerib. See võib olla kasutaja tegelik nimi, pseudonüüm, lühend või kombinatsioon tähtedest ja/või numbritest.

## Keylogger

Mõistega „*keylogger*“ tähistatakse klaviatuurile tehtud iga klahvivajutuse salvestamist riist- või tarkvara poolt, et neid siis võimalikult tähelepanematult ründajale edastada, kes võib saadud informatsioonist välja filtreerida temale olulised andmed, nt sissepääsuparoolid või krediitkaardi numbrid.

## Klient

Kliendiks nimetatakse tark- või riistvara, mis võimaldab kasutada serveri teatud teenuseid. Tihti kasutatakse mõistet „klient“ töökoha arvuti kohta, millel on võrgus juurdepääs serveri andmetele ja programmidele.

## Kohustuslikkus (ingl. k. Liability)

Kohustuslikkuse all mõistetakse kokkuvõetuna kahte IT-turvaeesmärki: autentsust ja salgamise vääramist. Informatsiooni valdkonda ülekantuna tähendab see, et informatsiooni allikas on tõestanud oma identsuse ja teate saamist ei saa vaidlustada.

## Konfidentsiaalsus

Konfidentsiaalsuse all mõistetakse informatsiooni kaitsmist selle volitamatu kasutamise eest. Konfidentsiaalsed andmed ja informatsioon peaksid olema lubatud viisil kättesaadavad vaid neile, kel on õigus neid kasutada.

---

## **Krüpteerimine**

Krüpteerimine muudab krüpteerimata teksti sõltuvalt lisainformatsioonist, mida nimetatakse „võtmeks“, salajaseks (krüpteeritud) tekstiks, mida ei saa võtit mitteomavad isikud lahti krüpteerida. Vastupidist muutmist, salajase teksti tagasimuutmist krüpteerimata tekstiks, nimetatakse lahti krüpteerimiseks.

## **Kumulatsiooni efekt**

Kumulatsiooni efekti all mõistetakse olukorda, kui mitmete (nt väiksemate) kahjude kuhjumise tagajärjel võib IT-süsteemis tekkida suurem kogukahju ning sellest tulenevalt võib IT-süsteemi kaitsevajadus kasvada. Kumulatsiooni efekti vallapäästjaks võib olla ka asjaolu, et ühes IT-süsteemis kasutatakse mitmed IT-rakendusi või töödeldakse suuremat hulka tundlikku informatsiooni, nii et kahjude kuhjumise tõttu võib olla kogukahju suurem.

## **Käideldavus**

Teenuste, IT-süsteemi funktsioonide, IT-rakenduste või IT-võrkude või ka informatsiooni käideldavus on tagatud, kui neid saab kasutada ettenähtud viisil.

## **Käitavad infovarad**

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

## **Ligipääs**

Ligipääsuga tähistatakse IT-süsteemide, süsteemi komponentide ja võrkude kasutamist. Pääsuõigused võimaldavad isikul seega kasutada kindlaid ressursse, nagu näiteks IT-süsteemid või süsteemi komponendid ja võrgud.

## **Maksimumprintsiiip**

Maksimumprintsiiibi kohaselt määrab tugevaimat mõju avaldanud kahju või kahjude summa tegevusprotsessi, rakenduse või IT-süsteemi kaitsevajaduse.

## **Meetmete kataloog**

IT-etalonturbe kataloogides soovitatakse igas moodulis sobivat meetet, 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 soovitude struktureerimiseks. Moodulid on ühe tasandi (nt IT-süsteemid, võrgud) üksused. Neis kirjeldatakse osalt tehnilisi komponente (nt kaabeldus), osalt organisatoorseid meetmeid (nt hädaolukorras 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.

---

## **Nuhkvara (ingl. k. „Spyware“)**

Nuhkvaraks nimetakse programme, mis koguvad kasutaja arvutist salaja informatsiooni ning edastavad selle infost huvitatud osapooltele. Nuhkvara peetakse tihti vaid ebameeldivaks?!, kuid ei tohiks unustada, et nuhkvara kaudu saab välja uurida ka konfidentsiaalset informatsiooni nagu nt paroolid.

## **Oht (ingl. k. "applied threat")**

Ohuks nimetakse olukorda või sündmust, mis avaldab mõju konkreetse objekti haavatavale kohale.

## **Ohukataloog**

Ohukataloogid on IT-etaloniturbekataloogide üheks osaks, sisaldades infotehnoloogiale kahju toovate võimalike ohtude kirjeldusi. Ohud on kataloogis liigendatud järgnevalt: vääraratu jõud, organisatoorsed puudused, inimvead, tehnilised rikked ja ründed.

## **Omanik**

vt. andmete omanik.

## **Paik (ingl. k. Patch)**

Paik (ingl. k. „patch“, eesti „paik ehk hädaparandus programmis“) on väike programm, mis kõrvaldab kasutusprogrammide või operatsioonisüsteemide tarkvaravead, nt turvaaukud.

## **Paketifilter**

Paketifiltri all mõistetakse spetsiaalse tarkvaraga IT-süsteeme, mis filtreerivad kindlate reeglite alusel võrgust väljaminevaid ja sissetulevaid saadetisi. Paketifiltri ülesandeks on andmepakettide edasisaatmine või tühistamine UDP/IP- ja TCP/IP-kihi *päise andmetes* sisalduvate andmete põhjal (nt IP-aadress ja porti number). Vastavad otsused teeb paketifilter vastavalt kasutaja poolt ette antud filtreerimisreeglitele. Paljudel juhtudel pakuvad paketifiltrid ka „*Network Address Translation*“ (NAT) võimalust, mille puhul asendatakse IP-pakettide saatja aadressid paketifiltri IP-aadressiga. Niimoodi varjatakse kaitstava võrgu struktuuri.

## **Penetratsiooni test**

Penetratsiooni test on eesmärgipärane, tavaliselt simuleeritud rünnak IT-süsteemile, et kontrollida olemasolevate turvameetmete olemasolu.

## **Proksi (ingl. k. Proxy)**

Proksi on võrkudes teatud liiki asendajaks. Ta võtab teateid vastu ja edastab need võrgu teise kohta. Proksi abil on võimalik filtreerida andmevoogu ja edastada vajalikke andmeid.

## **Rakenduslüüs (ingl. k. Application-Level-Gateway)**

Kasutaja tasandil võtavad tulemüüri funktsioonid enda kanda niinimetatud *Application-Level-Gateway'd* (ALG-d) ehk rakendustaseme lüüsid. Kaudselt täidavad ALGd ka ISO/OSI mudeli 1.-3. kihi funktsioone. ALGsid nimetakse ka tihti turvaproksideks. Proksid katkestavad otsese andmevoogu allika ja selle sihtkoha vahel. Kliendi ja serveri vahelises kommunikatsioonis, mis toimub üle proksi, võtab proksi vastu kliendi päringud ja saadab need edasi serverile. Proksi toimib analoogselt ka siis, kui ühenduse loomine toimub vastupidises järjekorras, st serverilt kliendi suunas.

---

Kõik ühendused kahe arvuti vahel kulgevad sellisel juhul otseselt proksi kaudu. Selline kommunikatsioonivorm võimaldab proksil näiteks filtreerida teatud protokollikäske.

## **RIA**

Riigi Infosüsteemide Arenduskeskus.

## **RIHA**

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

## **Risk**

Risk on tihti ettenägelikkusel põhinev prognoos. Negatiivses mõttes on risk seotud võimaliku kahju tekkimisega. Positiivses mõttes võib risk olla seotud aga ka võimaliku kasusaamisega (võimalus). See, mida mõista kahju või kasu all, sõltub väärtushinnangutest. Riski defineeritakse tihti ka kui kombinatsiooni tõenäosusest, milles võiks kahju tekkida. Erinevalt „ohust“ sisaldab mõiste „risk“ ka hinnangut selle kohta, millise konkreetse kahju võib iga vastav juhtum endaga kaasa tuua.

## **Riskianalüüs (ingl. k. Risk Assessment / Analysis)**

Riskianalüüsiga püütakse määratleda, millised kahjutoivad sündmused võivad aset leida ja milline on nende toimumise tõenäosus ning millised negatiivsed tagajärjed võivad nendega kaasneda.

## **Rootkit**

*Rootkit* on kahjurprogramm, mis sisaldab süsteemprogrammide manipuleeritavaid versioone. *Unix*'i keskkonnas on nendeks tavaliselt programmid *login*, *ps*, *who*, *netstat* jm. Manipuleeritavad süsteemprogrammid võimaldavad ründajal varjata, et ta on edukalt omandanud administraatori õigused sisselogimisel, nii et ta võib seda juurdepääsuteed ka hiljem uuesti kasutada.

## **Rünne**

Rünne on tahtlikult tekitatud oht, täpsemalt soovimatu või volitamata tegutsemine kasusaamise eesmärgil või selleks, et kolmandat osapoolt kahjustada. Ründajad võivad tegutseda ka kellegi tellimusel, kes soovivad ründest kasu saada.

## **Salgamise vääramine (ingl. k. non-repudiation)**

Informatsiooni ja andmete saatmise puhul on oluline tagada, et nende saatmist ja vastuvõtmist ei saaks eitada. Eristatakse

- päritolu salgamist: teate saatjal ei tohi olla hiljem võimalik vaidlustada asjaolu, et antud teade on tema saadetud;
- sisu salgamist: teate saajal ei tohi olla hiljem võimalik saadetud teate kättesaamist vaidlustada.

## **Server**

Serveriks nimetatakse tark- või riistvara, mis pakub teistele (klientidele) kindlaid teenuseid. Tavaliselt nimetatakse nii arvutit, mis teeb oma riist- ja tarkvararessursid teistele arvutitele võrgu kaudu kättesaadavaks. Näiteks aplikaatsiooni-, andme-, interneti- või e-posti-server. Tihti tekitavad segadust x-serverid, kuna selle serveri protsess toimib töökoha arvutis, seega kliendi jaoks server-klient-võrgus.

---

## **Sissepääs**

Sissepääs tähendab sisenemist piiritletud alale, nagu näiteks ruumidesse või mingi hoone kaitstud piirkonda. Sisepääsuõigused lubavad seega isikutel astuda kindlasse piirkonda, nagu näiteks territooriumile, hoonesse või selle kindlatesse ruumidesse.

## **Tagauks (ingl. k. backdoor)**

Tagausteks nimetatakse kahjurprogramme, mille ülesandeks on hoida - selleks luba omamata - lahti ligipääs IT-süsteemile, võimaldades tungida märkamatuult süsteemi. Sealjuures on sissetungijal võimalikult paljudele andmetele juurdepääs, mis aitab tal peita ründejälgi.

## **Terviklus**

Terviklus tähistab andmete korrektsuse ja süsteemide laitmatu funktsioonivõime tagamist. Kui mõistet „terviklus“ kasutatakse andmete kohta, väljendab see, et andmed on täielikud ja muutusteta. Infotehnoloogias on sel mõistel tavaliselt aga laiem tähendus ning seda kasutatakse informatsiooni kohta. Mõistet „informatsioon“ kasutatakse seejuures andmete kohta, millele saab olenevalt seosest omistada kindlad atribuudid nagu näiteks autor või koostamisae. Informatsiooni tervikluse kadu võib seega tähendada, et viimatinimetatuid on lubamatult muudetud st autori andmeid on võltsitud või koostamisajaga on manipuleeritud.

## **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 tegemiseks (nt. varundusserver, võrguseadmed, tulemüür vmt).

## **Trooja hobune**

Trooja hobune, sageli ka troojalaseks nimetatud, on varjatud, mittedokumenteeritud funktsiooni või mõjuga programm. Trooja hobune levib mitte ise, vaid peibutab kasutajat käivitama näiliselt kasutoovat programmi.

## **Tugev autentimine**

Tugeva autentimise all mõistetakse kombinatsiooni kahest autentimistehnikast, nagu parool pluss transaktsiooni numbrid (ühekordsed paroolid) või pluss kiipkaart. Seepärast nimetatakse seda sageli ka kahefaktoriliseks autentimiseks.

## **Turbeaste**

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

## **Tulemüür**

Tulemüür (tähistatakse ka mõistega „turvalüüs“) on tark- ja riistvara tehnilistest komponentidest koosnev süsteem IP-võrkude turvaliseks ühendamiseks (vt Turvalüüs)

## **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.

## **Turvakontseptsioon**

Turvakontseptsioonis määratakse kindlaks ja süstematiseeritakse kontseptsioonilised turvanõuded ning kirjeldatakse nende rakendamiseks vajalikke meetmeid.

## **Turvalüüs**

Turvalüüs (nimetatakse tihti ka tulemüüriks) on tark- ja riistvaratehnilistest komponentidest koosnev süsteem, mis tagab IP-võrkude turvalise ühendamise. Selleks piiratakse kommunikatsiooni tehnilisi võimalusi vastavalt kehtivale infoturbe poliitikale.

Võrguühenduse turvalisus tähendab seejuures eranditult üksnes volitatud süsteemi juurdepääsu või soovitud andmevooge erinevate võrkude vahel ning kõikide edastatavate andmete kontrollitavust.

## **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 turvaseme 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 organisatoorse kui ka inim-, tehniliste- või infrastruktuure puudutavate turvameetmete abil. Sünonüümideks kasutatakse ka mõisteid „turvaabinõu“ või „kaitsemeede“. Kasutatakse ka ingliskeelseid mõisteid *"safeguard"*, *"security measure"* või *"measure"*. Inglisekeelses keeleruumis kasutatakse *"safeguard"* kõrval tihti ka mõistet *"control"*.

## **Turvapoliitika (ingl. k. Security Policy)**

Turvapoliitikas formuleeritakse kaitseesmärgid ja üldised turvameetmed ettevõtte või asutuse poolt ametlikult etteantud nõuetest lähtuvalt. Üksikasjalikud turvameetmed sisalduvad mahukamas turvakontseptsioonis.

## **Tüüp tarkvara**

Tüüp tarkvara all mõistetakse tarkvara (programmid, programmi moodulid, abiprogrammid jne) ja selle juurde kuuluvat dokumentatsiooni, mis on loodud turu üldisi vajadusi silmas pidades ja mitte ühe kindla tellija soovil. Iseloomulikuks asjaoluks on, et see on kasutaja poolt ise installeeritav ning kasutajaspetsiifiliseks kohandamiseks on vajalikud vaid väikesed kulutused.

## **Varad**

Kõik, mis omab organisatsiooni jaoks väärtust. Varana võib käsitleda andmeid, tarkvara, arvutitöökohti, arvutivõrku, servereid, inimesi, ruume, immateriaalseid varasid (nt. maineväärtus) jmt.

---

## **Võrguplaan**

Võrguplaan on graafiline ülevaade võrgu komponentidest ja nende ühendustest.

### **Uss**

Usside (arvuti-, interneti-, meiliuss) puhul on tegemist kahjurvaraga, mis sarnaselt viirusega iseend taastoodab ja kasutab iseseisvaks levimiseks võrke.

### **VLAN**

Virtuaalseid kohtvõrke (VLANe) kasutatakse võrkude loogiliseks struktureerimiseks. Seejuures moodustatakse füüsilise võrgu sisse loogiline võrgustruktuur, et ühendada funktsionaalselt kokkukuuluvad töökohad ja serverid ühte virtuaalsesse võrku.

### **VPN**

Virtuaalne privaatvõrk (VPN) on võrk, mida füüsiliselt rakendatakse teise võrgu (tihti internet) sees, kuid mis on loogiliselt sellest võrgust lahutatud. VPNides saab krüpteerimismeetmete abil kaitsta andmete terviklust ja konfidentsiaalsust, samuti saab kindlalt autentida kommunikatsioonipartnerit, seda ka juhul, kui mitmed võrgud või arvutid on rendiliinide või avalike võrkude kaudu üksteisega ühendatud. Mõistet „VPN“ kasutatakse tihti tähistamaks krüpteeritud ühendusi, transpordikanali kindlustamiseks võib siiski kasutada ka teisi meetodeid, näiteks kasutatud ülekanalprotokolli spetsiaalseid funktsioone.

### **Väärtus (ingl. k. asset)**

Väärtused on kõik see, mis on institutsioonile oluline (varad, teadmine, esemed, tervis).

### **WLAN**

Mõistega „WLAN“ (traadita kohtvõrk) tähistatakse traadita võrke, mis põhinevad *Institute of Electrical and Electronics Engineers* (IEEE) IEEE 802.11 ga tähistatud standardite gruppidel.