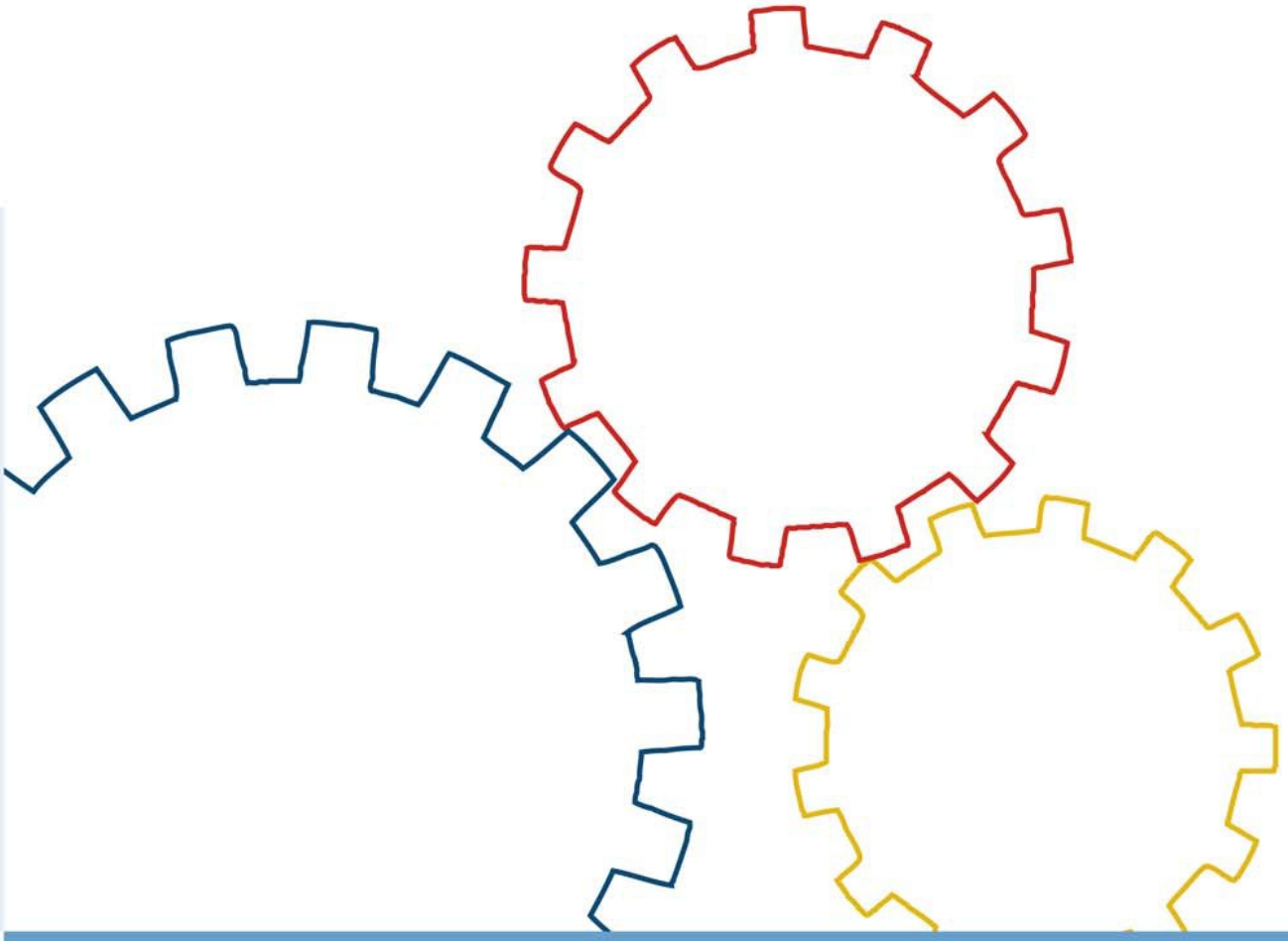
Bundesamt
für Sicherheit in der
Informationstechnik

# Standard BSI 100-1

Infoturbehalduse süsteemid (ISMS)



www.bsi.bund.de/gshb

Versioon 1.5

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189, 53175 Bonn

# Sisukord

# 1 Sissejuhatus

## 1.1 Versioonide ajalugu

| Seis | Versioon | Muudatused |
|---|---|---|
| Detsember 2005 | 1.0 | BSI |
| Mai 2008 | 1.5 | Keskendub rohkem infoturbele võrreldes varasema IT-turbega, mistõttu on mõisteid kohandatud.<br>Kohandatud ISO standardite täiendustega. |

## 1.2 Eesmärk

Ettevõtete ja ametiasutuste andmed on väärtus, mida tuleb sobivalt kaitsta. Tänapäeval koostatakse, salvestatakse, transporditakse ja töödeldakse andmeid kui mitte täielikult, siis vähemasti osaliselt kindlasti IT-süsteemidega. Majanduse ja juhtimise valdkonnas on muutunud arusaam, et IT-kooslusi tuleb muu hulgas ka kaitsta, juba iseenesestmõistetavaks. Siiski ei tohiks unustada, et adekvaatseid kaitsemeetmeid tuleb võtta ka kõikide teiste valdkondade ja tööprotsesside puhul. Turvaintsidendid, nt andmete soovimatu avalikustamine või nende manipuleerimine, võivad ühtmoodi rängalt tabada nii ettevõtteid kui ka ametiasutusi, sest need segavad igapäevaste tööülesannete täitmist ja toovad endaga kaasa suuri kulusid.

Praktika on näidanud, et kõige tõhusam viis, kuidas infoturvet jätkusuutlikult parendada, pole mitte investeering turbetehnoloogiasse, vaid turbevaldkonna halduse optimeerimine. Meetmed, mida võetakse infoturbe parendamiseks, ei mõju positiivselt mitte üksnes turbevaldkonnale, vaid suurendavad ka paljude teiste tööprotsesside tulemuslikkust ja kasumlikkust. Infoturbesse tehtavad investeeringud on paljudel juhtudel aidanud kokku hoida kulusid. Infoturbega tegelemise positiivsed lisamõjud, mis tekivad infoturbehalduse paremast integreerimisest olemasolevate struktuuridega, on tööde parem kvaliteet, klientide usalduse suurenemine, IT-koosluse ja tööprotsesside optimeerimine ning sünergiaefektide ärakasutamine.

Sobiva turbeastme saavutamine oleneb esmajoones alati süstemaatilisest käsitlusviisist ning kõikvõimalikud tehnilised lahendused on alles teisel kohal. Seda teesi selgitavad järgmised tähelepanekud.

- Juhtkond vastutab selle eest, et organisatsioon täidaks seadustest ja lepingutest tulenevaid kohustusi ning et kõik olulised tööprotsessid toimiksid tõrgeteta.
- Infoturbe valdkond puutub kokku organisatsiooni kõikvõimalike tegevusaladega ja keskendub ennekõike organisatsiooni peamistele tööprotsessidele. Seetõttu on infoturbe integreerimine organisatsiooni kõikide struktuuride ja protsessidega juhtkonna vastutusel.
- Lisaks vastutab juhtkond ka ressursside sihipärase kasutamise eest.

Seega kannab juhtkond infoturbe rakendamise eest suurt vastutust. Juhtimisvajaduse ignoreerimine, ebasobiv juhtimisstrateegia ja valed otsused võivad viia väga negatiivsete tagajärgedeni, nagu turvaintsidendid, käest lastud võimalused ja väärinvesteeringud.

Seetõttu kirjeldatakse selles standardis sammhaaval seda, mida kätkeb edukas infoturbehaldus ning milliseid rolle täidavad seejuures ettevõtete ja ametiasutuste juhtkonnad.

## 1.3 Sihtrühm

See dokument on suunatud töötajatele, kes vastutavad IT-süsteemide käitamise ja infoturbe tagamise eest, samuti infoturbespetsialistidele, -ekspertidele ja -nõustajatele ning kõikidele teistele huvilistele, kes puutuvad kokku infoturbehaldusega.

Infoturbe efektiivne ja säästlik haldus pole oluline mitte üksnes suurtele, vaid ka keskmise suurusega ja väikestele organisatsioonidele ning ka füüsilisest isikust ettevõtjatele. Samas tuleb tõdeda, et sobiva haldussüsteemi valimisel on kindlasti vaja lähtuda ka institutsiooni suurusest. See standard ja ennekõike IT-etalonturbe hästi konkreetsed juhised peaksid olema abiks kõikidele vastutavatele töötajatele, kes soovivad oma kompetentsi piires infoturbe tõhusust suurendada. Järgnevas tekstis esitatakse korduvalt viiteid ka sellele, kuidas kohandada siinseid soovitusi organisatsiooni suuruse ja vajadustega.

## 1.4 Kasutussuunised

Selles standardis kirjeldatakse, kuidas luua infoturbehalduse süsteemi (ISMS). See haldussüsteem peab sisaldama kõiki reegleid ja suuniseid, mida organisatsioonil tuleb järgida, et saavutada seatud turbe-eesmärk. Seega tuleb infoturbehalduse süsteemiga kindlaks määrata, milliste vahendite ja meetoditega hakkab organisatsiooni juhtorgan suunama infoturvet puudutavaid ülesandeid ja tegevusi.

See BSI standard vastab muu hulgas järgmistele küsimustele:

- millised tegurid mõjutavad kõige enam infoturbehalduse edukust?
- kuidas peaks infoturbehalduse süsteem infoturvet haldama?
- kuidas töötatakse välja pädev turbestrateegia ja sobivad turbe-eesmärgid?
- kuidas valida turbemeetmeid ja koostada turbekontseptsiooni?
- kuidas hoida ja parendada kord juba saavutatud turbeastet?

Selles haldusstandardis kirjeldatakse lühidalt ja ülevaatlikult turbehalduse peamisi ülesandeid. Nende soovituste rakendamisel aitab teid BSI loodud IT-etalonturbe metoodika. IT-etalonturbe dokumentatsioonist leiate sammsammulise juhendi, kuidas infoturbehaldust praktikas üles ehitada, ning viiteid infoturbe kõikvõimalikke aspekte puudutavatele konkreetsetele meetmetele. IT-etalonturbe metoodikat käsitleb standard BSI 100-2 (vt [BSI2]), milles kirjeldatakse, kuidas saavutada võimalikult väikeste kuludega võimalikult kõrge turbeaste. Eesmärgiks seatud turbeastme saavutamiseks soovitame muu hulgas kasutada ka IT-etalonturbe kataloogides kajastuvaid standardseid turbemeetmeid.

## 1.5 Kasutatud kirjandus

[BSI1] „Managementsysteme für Informationssicherheit (ISMS)”, standard BSI 100-1, versioon 1.5, mai 2008, www.bsi.bund.de

[BSI2] „IT-Grundschutz-Vorgehensweise”, standard BSI 100-2, versioon 2.0, mai 2008, www.bsi.bund.de

[BSI3] „Risikoanalyse auf der Basis von IT-Grundschutz”, standard BSI 100-3, versioon 2.5, mai 2008, www.bsi.bund.de

[COBIT] CobiT („Control objectives for information and related technology”), versioon 4.1, ISACA, http://www.isaca.org/cobit

[GSK] „IT-Grundschutz-Kataloge – Standard-Sicherheitsmaßnahmen”, BSI, ilmub kord aastas, http://www.bsi.bund.de/gshb

[ITIL] „IT Infrastructure Library, Service Management – ITIL (IT Infrastructure Library)”,

http://www.ogc.gov.uk/guidance_itil.asp, jaanuar 2008

[OECD] „Guidelines for the security of information systems and networks", Organisation for Economic Co-operation and Development (OECD), 2002, www.oecd.org/sti/security-privacy

[SHB] „IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik", BSI, versioon 1.0, märts 1992, Saksa riiklik trükikoda

[ZERT] „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits", BSI, versioon 1.2, märts 2008, www.bsi.bund.de/gshb/zert

[ZERT2] „Zertifizierungsschema für Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz", BSI, märts 2008, www.bsi.bund.de/gshb/zert

[27000] ISO/IEC 27000 (3. CD, 2008) „Information technology – Security techniques – ISMS – Overview and vocabulary", ISO/IEC JTC1/SC27

[27001] ISO/IEC 27001:2005 „Information technology – Security techniques – Information security management systems requirements specification", ISO/IEC JTC1/SC27

[27002] ISO/IEC 27002:2005 „Information technology – Security techniques – Code of practice for information security management", ISO/IEC JTC1/SC27

[27005] ISO/IEC 27005 (2. FCD, 2008) „Information technology – Security techniques – Information security risk management", ISO/IEC JTC1/SC27

[27006] ISO/IEC 27006:2007 „Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems", ISO/IEC JTC1/SC27

# 2 Sissejuhatus infoturbesse

**Mis on infoturve?**

Infoturbe eesmärk on mis tahes liiki ja päritolu andmete kaitsmine. Andmed võivad olla nii paberil, arvutisüsteemides kui ka inimeste peas. IT-turve tegeleb esmajoones elektrooniliselt salvestatud andmete ja nende töötlemise kaitsmisega.

Seevastu infoturbe klassikalised väärtused on konfidentsiaalsus, terviklus ja käideldavus. Paljud kasutajad suudavad neid väärtusi enda vaatevinklist ka täiendada. Olenevalt konkreetsest tegevusvaldkonnast võib see olla väga kasulik. Infoturbe üldmõistete hulka kuuluvad ka veel autentsus, siduvus, usaldusväärsus ja väärennetus.

Infoturvet ei ohusta aga mitte üksnes sellised ettekavatsetud tegevused nagu arvutiviiruste levitamine, side pealtkuulamine või arvutite vargus. Järgnevad mõned selgitavad näited.

- Vääramatu jõud (tulekahju, üleujutus, torm, maavärin) võib IT-süsteeme kahjustada või sulgeda juurdepääsu arvutuskeskusesse. Selle tagajärjel pole dokumente, IT-süsteeme või teenuseid enam võimalik harjumuspäraselt edasi kasutada.
- Pärast tarkvaravärskenduse ebaõnnestunud installimist ilmneb, et vajalikud rakendused ei tööta enam või andmeid on märkamatult muudetud.
- Olulises tööprotsessis tekib viivitus, sest kõik töötajad, kes oskavad vajalikku tarkvara kasutada, on haigeks jäänud.
- Töötaja võib konfidentsiaalsed dokumendid eksikombel anda valedele isikutele, sest dokumendile on jäetud lisamata märge „konfidentsiaalne".

**Sõnavalik: IT-turve *versus* infoturve**

Kirjanduses kasutatakse termineid „infotehnoloogia", „info- ja kommunikatsioonitehnoloogia" või „info- ja telekommunikatsioonitehnoloogia" väga sageli sünonüümidena. Kuna need terminid on väga pikad, on praktikas hakatud kasutama lühemaid vorme, mistõttu räägitakse sageli lihtsalt IT-st. Elektrooniline andmetöötlus on saanud peaaegu kõikide eluvaldkondade lahutamatuks osaks, mistõttu ei ole enam kohane vahet teha, kas andmete töötlemiseks kasutatakse info- või kommunikatsioonitehnoloogiat või töödeldakse neid hoopis paberil. Seega on „infoturve" tähenduselt parem ja laiem termin kui „IT-turve". Kuna aga erialakirjanduses kasutatakse endistviisi terminit „IT-turve" (muu hulgas selle lühiduse pärast), on see nii siin kui ka teistes IT-etalonturvet käsitlevates väljaannetes jätkuvalt kasutusel, kuigi tekstide koostamisel liigutakse järk-järgult siiski infoturbe suunas.

## 2.1 Infoturvet käsitlevate standardite ülevaade

Infoturbe kohta on välja töötatud mitmeid standardeid, mis erinevad kas sihtrühma või käsitletud valdkonna poolest. Turbestandardite rakendamine ei aita mitte üksnes suurendada ettevõtte või ametiasutuse turbeastet, vaid kergendab ka institutsioonidevahelisi kokkuleppeid selle kohta, mil määral ja milliseid turbemeetmeid tuleks võtta. Järgnev ülevaade kajastab olulisimaid standardeid.

### 2.1.1 ISO infoturbestandardid

Rahvusvahelised standardiorganisatsioonid ISO ja IEC on kokku leppinud, et infoturvet käsitlevaid standardeid, mille hulk pidevalt kasvab, tähistatakse seerianumbriga 2700x. Olulisimad on järgmised standardid.

- ISO 27000

  See standard kätkeb infoturbehalduse süsteemide (ISMS) ülevaadet ja standardite ISO 2700x

perekonda liigitatavate standardite kokkupuutepunkte. Lisaks kajastuvad selles ka ISMS-i põhimõtted, kontseptid, terminid ja definitsioonid.

- ISO 27001

  Kuna IT-valdkond on keeruline ja nõudlus sertifitseerimise järele aina kasvab, on viimastel aastatel avaldatud arvukalt infoturbeteemalisi juhendeid, standardeid ja riiklikke norme. Standard ISO 27001 „Information technology – Security techniques – Information security management systems requirements specification" on infoturbehalduse esimene rahvusvaheline standard, mis võimaldab ka sertifitseerimist. Standardis ISO 27001 loetletakse kümmekonnal leheküljel üldisi soovitusi, kuidas infoturbehalduse süsteemi evitada ja töös hoida ning kuidas dokumenteeritud süsteemi parandada, keskendudes muu hulgas ka võimalikele riskidele. Norme kajastavas lisas viidatakse ka standardist ISO/IEC 27002 pärit *controls*'itele. Seevastu praktilisi evitamisjuhiseid see standard ei anna.

- ISO 27002

  Standardi ISO 27002 (varem ISO 17799:2005) „Information technology – Code of practice for information security management" eesmärk on määrata kindlaks infoturbehalduse raamistik. Seetõttu hõlmab standard ISO 27002 peamiselt selliseid samme, mis on vajalikud turbehalduse ülesehitamiseks ja selle integreerimiseks organisatsiooni tööprotsessidega. Ent standardis ISO/IEC 27002 käsitletakse vajalikke turbemeetmeid sadakonnal leheküljel siiski ainult väga lühidalt. Soovitused keskenduvad eeskätt juhatusele, mistõttu ei sisalda need peaaegu üldse konkreetseid tehnilisi juhiseid. Standardi ISO 27002 turbesoovituste rakendamine on üks paljudest võimalustest, kuidas täita standardi ISO 27001 nõudeid.

  Teadmiseks: standard ISO 17799 liideti 2007. aastal ilma sisuliste muudatusteta standardiga ISO 27002, et rõhutada selle kuuluvust ISO standardite seeriasse 2700x.

- ISO 27005

  ISO standard „Information security risk management" sisaldab üldisi soovitusi infoturvet puudutava riskihalduse kohta. Sellest on muu hulgas abi standardiga ISO/IEC 27001 kehtestatud nõuete täitmisel, kuid see ei käsitle siiski mitte ühtki konkreetset riskihalduse evitamise meetodit. ISO/IEC 27005 asendab varasemat standardit ISO 13335-2. See varasem standard, ISO 13335 „Management of information and communications technology security, Part 2: Techniques for information security risk management", kätkes infoturbehalduse soovitusi.

- ISO 27006

  Standardis ISO 27006 „Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems" täpsustatakse ISMS-i sertifitseerimisüksuste akrediteerimisele seatavaid nõudeid ja käsitletakse ka ISMS-i sertifitseerimisprotsesside iseärasusi.

- Muud ISO 2700x seeria standardid

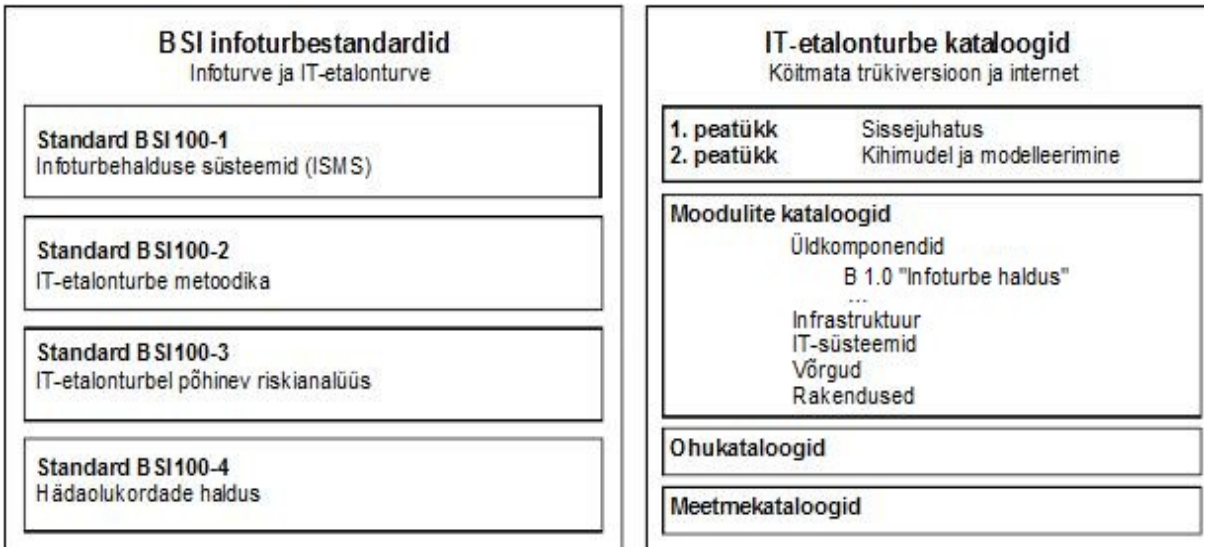
  Standardite seeriasse ISO 2700x hakkavad tulevikus eeldatavasti kuuluma standardid vahemikus ISO 27000–27019 ja 27030–27044. Kõikides selle seeria standardites käsitletakse turbehalduse erinevaid aspekte, tuginedes standardile ISO 27001. Nende eesmärk on hõlbustada standardi ISO 27001 mõistmist ja selle rakendamist praktikas. Käsitletavad teemad võivad olla nt standardi ISO 27001 evitamine ehk riskide hindamine ja riskihaldusmeetodid.

### 2.1.2 Valik BSI väljaandeid ja standardeid infoturbe kohta

**IT-etalonturbe kataloogid**

Kuni 2005. aastani oli BSI kõige tuntum väljaanne IT-etalonturbe käsiraamat, mille avaldamisega tehti algust aastal 1994 ja milles kirjeldati peale infoturbehalduse väga põhjalikult ka tehnikat,

töökorraldust, personali ja erinevaid taristuid käsitlevaid turbemeetmeid. Alates 2005. aastast pole IT-etalonturbe käsiraamatut ei uuendatud ega ümber korraldatud. Muudatuste käigus lahutati teineteisest IT-etalonturbe metoodika ja kataloogid.




Joonis 1. Turbehaldust käsitlevate BSI väljaannete ülevaade

IT-etalonturbe kataloogid on liigendatud mooduliteks, mis käsitlevad tüüpilisi protsesse, rakendusi ja IT-komponente. Iga teema kohta tuuakse välja nii soovituslikud turbemeetmed kui ka olulisemad ohud, mille eest peaks organisatsioon end kaitsma. Nii saavad kataloogide kasutajad keskenduda kohe nendele moodulitele, mis on nende töövaldkonna jaoks kõige olulisemad. IT-etalonturbe katalooge värskendatakse ja täiendatakse pidevalt, et käia kaasas tehnika arenguga. Seetõttu avaldatakse neid katalooge nii trükiversioonis ja internetis. IT-etalonturbe metoodika raames kirjeldatakse, kuidas standardsete turbemeetmete põhjal turbemeetmeid valida ja evitada ning nende täitmist kontrollida. Seda metoodikat kirjeldab BSI infoturbestandardite seerias avaldatud standard nr 100-2.

**BSI infoturbestandardid: infoturbehalduse teema**

100-1 Infoturbehalduse süsteemid (ISMS)

Standardis esitatakse ISMS-i üldnõuded. See standard on täielikult kooskõlas standardiga ISO 27001 ning arvestab ka standardite ISO 27000 ja 27002 soovitustega. Standard annab lugejale kergesti arusaadavad ja süstemaatilised üldkehtivad juhised, mida saab rakendada mis tahes evitamismeetodiga.

BSI koondab nende kahe ISO standardi sisu ühte BSI standardisse, et käsitleda mõningaid teemasid veidi põhjalikumalt ja anda materjalile didaktiline rakendus. Muudetud on ka algmaterjalide liigendust, et see oleks paremini kooskõlas IT-etalonturbe metoodikaga. Ühtlustatud pealkirjad ja päised aitavad lugejal soovitud materjali kergemini üles leida.

100-2 IT-etalonturbe metoodika

IT-etalonturbe metoodika raames kirjeldatakse samm-sammult, kuidas infoturbehalduse süsteemi praktikas üles ehitada ja töös hoida. Peamised teemad on infoturbehaldusega seotud ülesanded ja infoturbe rakendamiseks vajaliku organisatsioonistruktuuri loomine. IT-etalonturbe metoodika raames käsitletakse väga põhjalikult, kuidas turbekontseptsiooni praktikas koostada ja asjakohaseid turbemeetmeid valida ning mida jälgida turbekontseptsioonide rakendamisel. Standard annab põhjaliku vastuse ka küsimusele, kuidas infoturvet jooksvalt tagada ja paremaks muuta.

Seega käsitlevad IT-etalonturve ja standard BSI 100-2 ühekoos väga üldsõnalisi standardeid ISO 27000, 27001 ja 27002 ning annavad kasutajatele palju juhiseid, taustteadmisi ja näiteid,

kuidas infoturbele seatavaid nõudeid praktikas rakendada. IT-etalonturbe kataloogides ei kirjeldata mitte ainult seda, mida tuleks teha, vaid antakse ka väga konkreetseid juhiseid, kuidas midagi ellu viia (kuni tehniliste lahendusteni välja). IT-etalonturbe meetod kätkeb seega juba järele proovitud ja efektiivset võimalust, kuidas eelnimetatud ISO standardite nõudeid ellu viia.

100-3 IT-etalonturbel põhinev riskianalüüs

BSI on välja töötanud IT-etalonturbel põhineva riskianalüüsi metoodika.
Seda metoodikat saab kõige tõhusamalt rakendada juhtudel, kus ettevõttes või ametiasutuses on juba hakatud järgima IT-etalonturbe põhimõtteid ning nende tõhususe kontrollimiseks soovitakse IT-etalonturbe analüüsi täiendada turbeanalüüsiga.

100-4 Hädaolukordade haldus

Standardis BSI 100-4 käsitletakse metoodikat, mille abil on võimalik evitada ning töös hoida ettevõtteid ja ametiasutusi ähvardavate hädaolukordade haldust. See standard põhineb standardi BSI 100-2 metoodikal ja täiendab seda.

### 2.1.3 Muud standardid

**COBIT**

COBIT („Control objectives for information and related technology") kirjeldab kriitilise tähtsusega tööprotsesse toetavate IT-lahenduste riskide ohjamise metoodikat. COBIT-i dokumente annab välja infosüsteemide auditi ja juhtimise assotsiatsiooni (Information Systems Audit and Control Association, ISACA) IT juhtimise instituut (IT Governance Institute, ITGI). COBIT-i väljatöötamisel on autorid keskendunud peamiselt turbehalduse kohta juba avaldatud standarditele, nt standardile ISO 27002.

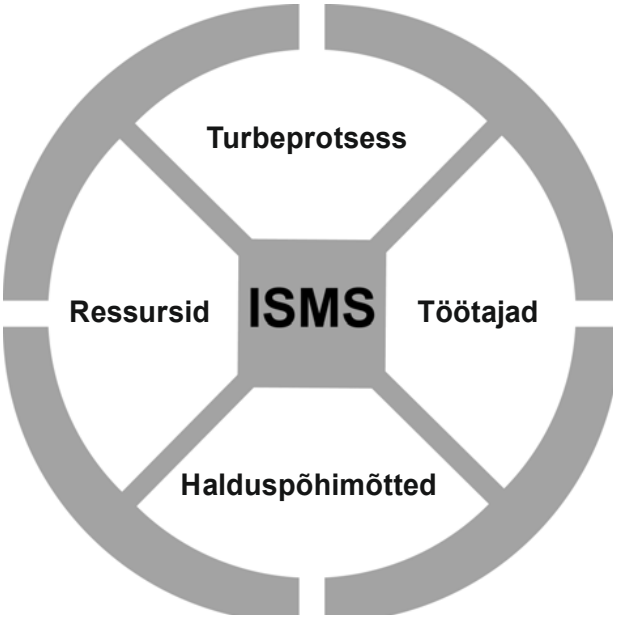
**ITIL**

ITIL („IT infrastructure library") on IT- infrastruktuuri käsitlevate raamatute kogum. Selle on välja töötanud Suurbritannia Office of Government Commerce (OGC). ITIL-is käsitletakse IT-teenuste haldust IT-teenusepakkuja vaatevinklist. IT-teenusepakkujate hulka liigitatakse nii organisatsiooni enda IT-osakond kui ka välised teenusepakkujad. Peamine eesmärk on IT-teenuste kvaliteedi parandamine ja kulude vähendamine.

# 3 ISMS-i definitsioon ja protsessi kirjeldus

## 3.1 Infoturbehalduse süsteemi komponendid

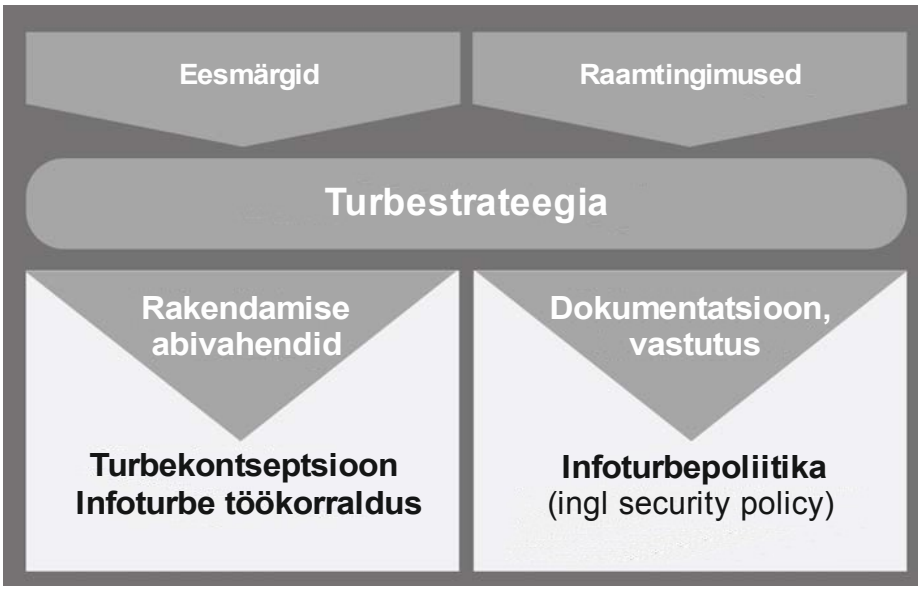
Igal ettevõttel ja ametiasutusel on olemas juhttöötajad, st töötajad, kes juhivad, suunavad ja planeerivad tööprotsesse. Järgnevas tekstis nimetatakse neid töötajaid kokkuvõtvalt juhtkonnaks.




Joonis 2. Infoturbehalduse süsteemi (ISMS) komponendid

Haldussüsteem peab sisaldama kõiki reegleid ja suuniseid, mida organisatsioonil tuleb järgida, et saavutada seatud turbe-eesmärk. Seda haldussüsteemi osa, mis tegeleb infoturbega, nimetatakse infoturbehalduse süsteemiks (ISMS). ISMS määrab kindlaks vahendid ja metoodika, mille põhjal hakkab juhtkond korraldama infoturbe-eesmärgi saavutamiseks vajalikke tööprotsesse ja -ülesandeid (sisaldab protsesside planeerimist, evitamist, tööshoidmist, seiret ja parendust). ISMS koosneb järgmistest põhikomponentidest (vt ka joonis 2):

- halduspõhimõtted;
- ressursid;
- töötajad;
- turbeprotsess;
- infoturbepoliitika, mis sisaldab muu hulgas turbe-eesmärke ja nende evitamise strateegiat;
- turbekontseptsioon;
- infoturbe töökorraldus.




Joonis 3. Infoturbestrateegia kui ISMS-i keskne komponent

Infoturbeprotsessi töökorraldus ja turbekontseptsioon on tööriistad, millega juhtkond saab oma eesmärke ellu viia. Joonised 3 ja 4 selgitavad nende seoseid. Turbestrateegia põhipunktid sõnastatakse infoturbepoliitikas. Infoturbepoliitika on väga oluline dokument, sest see sisaldab juhtkonna strateegiavalikut.


Joonis 4. Turbestrateegia rakendamine turbekontseptsiooni ja infoturbe töökorraldusega

## 3.2 Protsessi kirjeldus ja kasutustsükli mudel

### 3.2.1 Infoturbe all mõistetav kasutustsükkel

Turve ei ole muutumatu seisund, mille saavutamiseks tuleb vaid üks kord vaeva näha. Iga institutsioon on pidevalt dünaamiliste muudatuste meelevallas. Muudatused võivad puudutada tööülesandeid, taristuid, organisatsiooni struktuuri, IT-d ja ka infoturbe valdkonda. Institutsiooni piiridesse jäävate hoomatavate muudatuste kõrval võib esineda ka ettenägematuid väliseid muudatusi, nt seaduste ja lepingute muutmist, ning pole välistatud, et uusi nõudmisi võib seada ka pidevalt arenev info- ja

sidetehnoloogia. Seetõttu tuleb kord juba saavutatud turbeastme säilitamiseks ilmtingimata hoolitseda turbevaldkonna aktiivse juhtimise eest.

Tööprotsesside ühekordsest juurutamisest ja uute IT-süsteemide kasutuselevõtust selleks kindlasti ei piisa. Meetmete võtmise kõrval tuleb regulaarselt kontrollida, kas need on toimivad ja ajakohased, samuti tuleb vaadata, kas neid on võimalik reaalselt rakendada ja milline on nende tegelik toime. Olukordades, kus tuvastatakse kitsaskohti või leitakse võimalusi, kuidas midagi täiendada või parandada, tuleb kehtestatud meetmeid täiendada ja muuta. Ka muudatuste ja täienduste tegemist on vaja ilmtingimata planeerida ning seejärel see plaanipäraselt ellu viia. Turbeaspekte tuleb järgida ka nt siis, kui tööprotsesside kasutamine lõpetatakse või kui IT-süsteeme ja nende komponente utiliseeritakse või asendatakse (töötajate volituste tühistamine ja kõvaketta turvaline kustutus). Lugejale parema ülevaate andmiseks on IT-etalonturbe kataloogides kasutatud turbemeetmete kajastamisel järgmist liigendust:

- planeerimine ja kontseptsioon;
- soetamine (kui on vaja);
- rakendamine;
- käitamine (jooksva töö käigus infoturvet tagavad meetmed, mille alla kuuluvad ka seire ja tõhususe kontroll);
- ümbertöötlemine(kui on vaja);
- valmisolek hädaolukorraks.

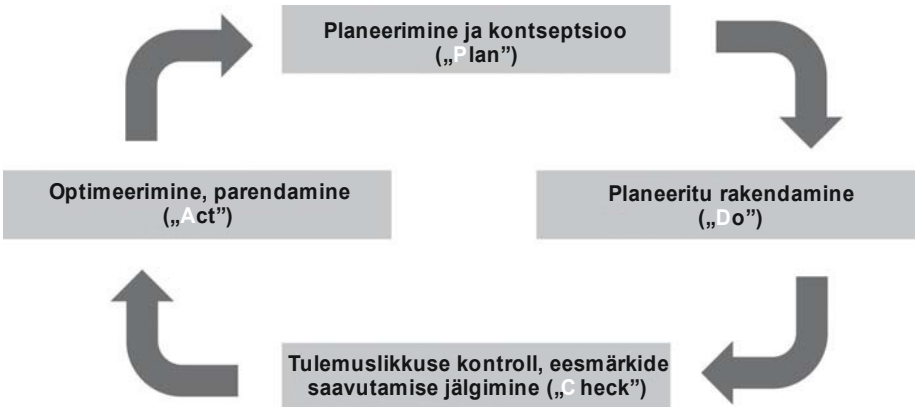
### 3.2.2 Infoturbeprotsessi kirjeldus

Termin „kasutustsükkel" ei käi ainult tööprotsesside ja IT-süsteemide kohta. Nii turbekontseptsioon, infoturbe töökorraldus kui ka kogu turbeprotsess toimivad tsüklitena. Turbeprotsessi võimalikult lihtsaks kirjeldamiseks jagatakse protsess erialakirjanduses enamasti järgmisteks faasideks:

1) planeerimine;
2) planeeritu rakendamine, st plaanide teostus;
3) tõhususe kontroll, st eesmärkide saavutamise jälgimine;
4) leitud puuduste kõrvaldamine, st optimeerimine ja parendamine.

Neljandas faasis kirjeldatakse, kuidas kõrvaldada väiksemat sorti puudusi. Põhjalike ja laiaulatuslike muudatuste tegemisel tuleb siiski alustada taas planeerimisfaasiga.

Sellist mudelit nimetatakse faaside ingliskeelsete nimetuste („Plan", „Do", „Check", „Act") esitähtede järgi ka PDCA-mudeliks.




Joonis 5. Demingu kasutustsükkel (PDCA-mudel)

PDCA-mudelit kirjeldatakse ka standardis ISO 27001. Seda on võimalik rakendada peaaegu piiramatult kõikide turbeprotsesside puhul. Selle mudeliga on võimalik ülevaatlikult kirjeldada ka turbekontseptsiooni ja infoturbe töökorralduse kasutusiga. Seetõttu toetub ka selle dokumendi vastavate peatükkide liigendus neljale kasutustsükli mudeli faasile.

Infoturbeprotsessi planeerimise faasis analüüsitakse raamtingimusi, määratakse kindlaks turbe-eesmärgid ja töötatakse välja turbestrateegia, mis peab sisaldama põhiväiteid selle kohta, milliseid eesmärke soovitakse saavutada. Turbestrateegia rakendamisel toetutakse turbekontseptsioonile ja struktuurile, mis tagab infoturbe asjakohase töökorralduse. Nii turbekontseptsiooni kui ka infoturbe töökorraldust tuleb planeerida ning pärast nende rakendamist hinnata nende tõhusust. Turbeprotsessi tõhususe kontrollimise raames uuritakse regulaarselt, kas raamtingimused (nt seadused või organisatsiooni eesmärgid) on vahepeal muutunud ning kas turbekontseptsioon ja infoturbe töökorraldus toimivad efektiivselt.

Kuna erinevatel organisatsioonidel on ka erinevad raamtingimused ja turbenõuded ning erineva suurusega eelarve, annab see metoodika siiski vaid hea lähtekoha, mida iga ettevõte ja ametiasutus peab oma vajadustega kohandama. Iga institutsioon peab iseseisvalt kindlaks määrama või täpsustama, millist kasutustsükli mudelit nad rakendavad.

Väiksed ametiasutused ja ettevõtted ei tohiks lasta end sellest metoodikast kohutada, sest turbeprotsessiga kaasnevate tööde maht oleneb väga sageli ka organisatsiooni suurusest. Näiteks tuleb väga suurtes ettevõtetes, kus on palju osakondi ja kus töötab palju inimesi, ilmselt välja töötada protsess, millega määratakse täpselt kindlaks, millised on vajalikud sise- ja välisauditid, kes keda teavitab, kes valmistab ette otsused ja kes informeerib turbeprotsessist juhtkonda. Seevastu väiksemates ettevõtetes võib turbeprotsessi tõhususe hindamiseks piisata ka ainult iga-aastasest nõustamiskoosolekust, kus kohtuvad juhatuse esimees ja IT-teenust osutava firma esindaja, et arutada möödunud aastal esinenud probleeme, teenuse kulukust, tehnika arenguga kaasnevaid uuendusi jms.

# 4 Juhtimispõhimõtted

Terminiga „infoturbehaldus" tähistatakse planeerimis- ja juhtimisülesandeid, mis seavad eesmärgiks, et turbeprotsess oleks võimalikult hästi läbimõeldud ning et kõik selleks vajalikud turbemeetmed oleksid otstarbekad, praktiliselt rakendatavad ja efektiivsed. Siia alla kuulub ka seadustest ja muudest õigusnormidest tulenevate ettekirjutuste täitmine. Efektiivse infoturbehalduse ja selleks vajaliku organisatsioonistruktuuri kohta on välja töötatud mitmeid kontseptsioone. Siiski tuleb kõikide infoturbehalduse süsteemide puhul arvestada teatud üldpõhimõtetega.

Mõned järgnevalt kirjeldatud juhtimispõhimõtted võivad teile tunduda banaalsed, sest paljude juhttöötajate jaoks on need vahepeal muutunud juba iseenesestmõistetavaks. Seevastu praktika on näidanud, et see, kus kõige rohkem vigu tehakse või mida kõige rohkem tegemata jäetakse, puudutabki just kõige lihtsamaid asju. Distsipliin, kannatlikkus, vastutuse võtmine ning projektide realistlik ja hoolikas ettevalmistus on paljudes organisatsioonides küll vägagi hinnatud väärtused, kuid kahjuks juhtub väga sageli, et teooria ei kandu üle praktikasse. Kogemused on näidanud, et turbeastet saab sageli märkimisväärselt tõsta ka sellega, kui tegeleda selliste vähem põnevate valdkondadega nagu tööprotsesside optimeerimine, töötajate koolitamine ja motiveerimine või arusaadava dokumentatsiooni koostamine. Seevastu keerulisi ja seetõttu ka kalleid turbemeetmeid, nt suurprojekte ja suurinvesteeringuid tehnoloogiasse, peetakse tihti väga tõhusaks ning pärast seda, kui praktika on tõestanud vastupidist, asutakse kritiseerima turbevaldkonda kui liigset kuluallikat. Järgnevalt kirjeldatakse juhtimispõhimõtteid, mis on eduka infoturbehalduse eelduseks.

## 4.1 Juhtkonna ülesanded ja kohustused

Infoturvet puudutavad juhtkonna ülesanded ja kohustused võib kokku võtta järgmiste punktidena.

1. Koguvastutuse võtmine infoturbe eest

   Iga ametiasutuse ja ettevõtte juhtkonna kõrgeim tasand vastutab institutsiooni sihipärase ja nõuetekohase funktsioneerimise eest ning tagab seeläbi infoturbe nii organisatsiooni sees kui ka sellest väljaspool. Riigiti ja organisatsiooniti võivad seadustest tulenevad ettekirjutused erineda. Juhtkond ja kõik teised juhttöötajad peavad võtma vastutuse ja tegutsema selle nimel, et nende alluvad mõistaksid infoturbe valdkonna olulisust.

2. Infoturbehalduse integreerimine

   Infoturbehaldus tuleb integreerida kõikide institutsiooni tööprotsesside ja projektidega, mille raames töödeldakse andmeid ja kasutatakse IT-d. See tähendab nt seda, et turbenõuetega ei tule arvestada mitte ainult IT-seadmete soetamisel, vaid ka tööprotsesside väljatöötamisel ja töötajate koolitamisel.

3. Infoturbehalduse juhtimine ja tööshoidmine

   Juhtkond peab aktiivselt tegelema turbeprotsessi algatamise, suunamise ja kontrollimisega. Siia alla kuuluvad nt järgmised ülesanded:

   - infoturbehalduse strateegia ja eesmärkide kinnitamine;
   - turberiskide mõju hindamine seoses tööprotsesside täitmisega;
   - infoturbe toimimiseks vajalike organisatsiooniliste raamtingimuste loomine;
   - piisavate ressursside eraldamine infoturbehaldusele;
   - turbestrateegia regulaarne kontrollimine ja selle eesmärkide pidev järgimine, tuvastatud puuduste ja vigade kõrvaldamine. Selleks tuleb väljendada organisatsiooni valmisolekut pidevalt edasi areneda ning luua töötingimused ja õhkkond, mis soosivad uuendusi;
   - töötajate teavitamine ja motiveerimine, et nad mõistaksid, kui olulise osa moodustab

infoturve nende tööülesannetest. Selleks tuleb töötajaid muu hulgas piisavalt koolitada ja teha ohualast teavitustööd.

4. Realistlike eesmärkide püstitamine

   Mis tahes projektid takerduvad tihti kas ebarealistliku või liiga julge eesmärgipüstituse taha. Ka infoturbe valdkond ei ole siin erand. Seetõttu on oluline, et turbestrateegia oleks kooskõlas olemasolevate ressurssidega. Kõiki projekte ei pea ilmtingimata kohe alguses suurelt ette võtma. Sobiva turbeastme saavutamiseks võib teinekord palju rohkem kasu olla sellest, kui esmalt astutakse palju väikseid samme ning võetakse eesmärgiks olukorda pidevalt parandada. Nii võib olla alguses mõistlik seada eesmärgiks juurutada soovitud turbeaste esmalt ainult üksikutes valdkondades. Seejärel saab need valdkonnad juba eeskujuks võtta ja turbeastme suurendamisega institutsiooni teistesse valdkondadesse kiiremini edasi liikuda.

5. Turbevaldkonna kulude ja kasu analüüs

   Infoturbe kulude ja sellest saadava kasu analüüsimine on üks raskemaid ülesandeid. Seetõttu on ülimalt oluline, et esmalt investeeritaks ainult sellistesse meetmetesse, mis on kas üliefektiivsed või millega soovitakse kõrvaldada kõige suuremaid riske. Kõige efektiivsemad turbemeetmed ei pruugi olla alati kõige kallimad. Parimate turbemeetmete väljavalimine eeldab analüüsi ning analüüs omakorda väga häid teadmisi sellest, mil määral oleneb tööülesannete täitmine ja tööprotsesside teostamine andmetöötluse toimimisest.

   Siinkohal tuleb rõhutada, et infoturve toimib alati ainult tehniliste ja organisatsiooni töökorralduslike meetmete koostöös. Tehnikasse investeerimise võimalused saab institutsiooni eelarve põhjal üpris kergesti välja selgitada. Selleks, et kulud ennast kõige paremini õigustaksid, tuleb turbetooteid rakendada nõnda, et saadav kasu oleks optimaalne. Selleks tuleb tooteid hoolikalt valida ning töötajad peavad oskama neid ka õigesti kasutada, st tooted peavad kajastuma üldkehtivas turbekontseptsioonis ja töötajad peavad läbima asjakohased koolitused. Samas on tehnilisi lahendusi sageli võimalik asendada turbemeetmetega, mis põhinevad organisatsiooni töökorralduse muutmisel. Praktikas on aga taas küllaltki raske tagada, et organisatsiooniliste meetmete võtmine oleks piisavalt järjepidev. Pealegi suureneb personaliressursi vähenemisel töötajate töökoormus.

6. Eeskujuks olemine

   Juhtkond peab infoturbe valdkonnas andma eeskuju. Siia alla kuulub muu hulgas see, et juhtkond peab ka ise kõikidest etteantud turbereeglitest kinni pidama ja koolitustel osalema.

## 4.2 Infoturbe tagamine ja pidev täiustamine

Infoturbe tagamine ei ole mitte ajaliselt piiratud, vaid pidev projekt. Infoturbehalduse süsteemi elemente tuleb pidevalt kontrollida, et välja selgitada, kas need on jätkuvalt sobivad ja piisavalt tõhusad. See tähendab, et regulaarselt ei tule kontrollida mitte ainult turbemeetmete täitmist, vaid ka turbestrateegiat.

Turbemeetmete tõhusust tuleks kontrollida regulaarsete siseauditite̊ga. Need peaksid aitama kaasa ka sellele, et institutsioon saaks koguda ja analüüsida töötajate praktilisi töökogemusi. Auditite kõrval tuleb kindlasti hoolitseda ka töötajate teavitamise ja koolitamise eest, sest ainult nii saab kindel olla, et võimalikus hädaolukorras kõik ettenähtud protsessid toimivad ja et töötajad reageerivad olukorrale adekvaatselt. Süsteemis leitud puudused tuleb eranditult kõrvaldada ja parandusvõimalusi infoturbe töökorralduses arvesse võtta. Peale selle on potentsiaalsete ohtude avastamise ja ennetamise ning sobivate turbemeetmete võtmise jaoks oluline, et institutsioon suudaks võimalikult vara tuvastada, mis suunas võib areneda nende kasutatav tehnoloogia ning mil moel võivad muutuda tööprotsessid ja institutsiooni struktuur. Olukorras, kus tööprotsessides või organisatsiooni struktuuris leiavad aset suured muutused, tuleb nende muutustega arvestada ka infoturbehalduses. Ka neil juhtudel, kus infoturbehaldus on organisatsiooni tööprotsessidega selgelt integreeritud, ei peaks turbevaldkonna

töötajad siiski käed rüpes istuma ja ootama enda kaasamist, vaid ka ise selle eest hoolitsema, et turbeküsimustega tegeldaks kõikjal õigel ajal.

Kõikide auditite puhul tuleks arvestada sellega, et auditeid ei peaks tegema need isikud, kes osalesid turbekontseptsiooni planeerimisel ja väljatöötamisel, sest oma vigu tavaliselt ei nähta. Mida suurem on institutsioon, seda rohkem võib esineda organisatsioonisisest lühinägelikkust, mistõttu võib olla mõttekas tellida auditid väljast.

Infoturbe tagamine on oluline ka väikestele ja keskmise suurusega ettevõtetele ning ametiasutustele. Nende auditid on küll väiksema mahuga, kuid neid ei tohi mitte mingil juhul ära jätta. Juhtkonna iga-aastase juhtimisprotsesside hindamise raames tuleb muu hulgas kontrollida, kas vahepeal on ilmunud uusi seadusi vms, mida tuleb järgida, ja kas mõned muud raamtingimused on muutunud.

Turbeprotsessi kontrollitakse ka selle täiustamise eesmärgil. Seetõttu tuleks kontrollide tulemusi kasutada väljavalitud turbestrateegia efektiivsuse hindamiseks ja selle võimalikuks täiustamiseks. Turbestrateegia tuleb ümber teha ka siis, kui muutuvad turbele seatud eesmärgid või selle raamtingimused. Seda teemat käsitletakse lähemalt selle standardi seitsmendas peatükis.

## 4.3 Suhtlemine ja teadmised

Turbe-eesmärkide saavutamisel saab kõikides turbeprotsessi faasides määravaks suhtlus. Turbeprobleemide sagedamad põhjused on muu hulgas valestimõistmine ja ebapiisavad teadmised. Seetõttu tuleb kõikidel institutsiooni tasanditel hoolitseda, et kogu turbeinfo, st teave nii aset leidnud sündmuste kui ka võetud turbemeetmete kohta, liiguks võimalikult hästi. Selle alla kuuluvad järgmised punktid.

- Juhtkonnale esitatavad aruanded

  Juhtkonna kõrgeim tasand peab oma juhtimisülesannete täitmiseks laskma end regulaarselt informeerida probleemidest, kontrollide ja auditite tulemustest, samuti kõikvõimalikest arengusuundumustest, muutunud raamtingimustest ja tehtud parandusettepanekutest.

- Infovoog

  Ebapiisav kommunikatsioon ja puudulikud teadmised võivad peale turbeprobleemide tuua kaasa ka väärotsused ja liigsed tööprotsessid. Selliseid olukordi tuleb ennetada sobivate meetmete ja organisatsiooni läbimõeldud töökorraldusega. Töötajatele tuleb selgitada turbemeetmete mõtet ja eesmärki ennekõike neil juhtudel, kus need põhjustavad kas lisatööd või vähendavad kasutusmugavust. Turbemeetmete eesmärgi kõrval tuleb töötajatele selgitada nii infoturvet kui ka andmekaitset puudutavaid õigusküsimusi, mis on seotud nende tööülesannetega. Lisaks tuleb töötajad kaasata võetavate meetmete planeerimisse, et võimaldada ideede kaasamist ja hinnata paremini meetmete praktilist rakendatavust.

- Dokumentatsioon

  Turbeprotsessi järjepidevuse ja ühtluse tagamiseks on selle dokumenteerimine kindlasti vältimatu. Ainult nii saab tagada, et langetatud otsuseid ja protsessi raames läbi tehtud samme on võimalik ka hiljem veel mõista. Pealegi tagab hea dokumentatsioon selle, et sarnaseid töid tehakse ühtmoodi, st protsesse peab saama muuta ja korrata. Dokumentatsiooni põhjal saab muu hulgas tuvastada ka protsessi üldisi puudujääke ning see aitab vältida vigade kordamist. Vajalikul dokumentatsioonil on turbevaldkonniti erinev ülesanne ning see on adresseeritud erinevatele sihtrühmadele. Dokumentatsiooni puhul on võimalik eristada järgmisi alaliike.

  1. Tehniline dokumentatsioon ja tööprotsesside dokumentatsioon (sihtrühm: eksperdid)

     Tõrgete ja turvaintsidentide korral peab olema võimalik taastada nii tööprotsesside kui ka nende täitmiseks vajalike IT-süsteemide ettenähtud seisund. Seetõttu tuleb tehnilised üksikasjad ja töötoimingud dokumenteerida nõnda, et taastamine õnnestuks vastuvõetava aja jooksul.

Siia alla kuuluvad kõik juhised, mis käsitlevad nt IT-rakenduste installimist, andmete varundamist, andmete taastamist varukoopiate põhjal, telefonikeskjaama konfigureerimist, elektrikatkestusejärgset rakendusserveri taaskäivitamist, samuti dokumentatsioon toodete katsetamise ja kasutusse lubamise kohta ning töötajate käitumisjuhised rikete ja turvaintsidentide puhuks.

2. IT kasutamisjuhised (sihtrühm: IT kasutajad)

   Tööprotsessid, tööga seotud ettekirjutused ja töötajatele kohustuslikud tehnilised turbemeetmed tuleb dokumenteerida selliselt, et need aitaksid vältida teadmatusest ja väärast käitumisest põhjustatud turvaintsidente. Siia kuuluvad nt meiliteenuse ja interneti kasutamise turbepoliitika, juhised arvutiviiruste vältimiseks ja inimestega manipuleerimise tuvastamiseks ning käitumisreeglid juhtudeks, mil on alust kahtlustada turvaintsidenti.

3. Juhtimisülesandeid toetavad raportid (sihtrühm: juhtkond, turbehalduse juhttöötajad)

   Juhtkonna jaoks tuleb kogu juhtimisülesannete seisukohast oluline info (nt auditite järeldused, efektiivsuse mõõtmise tulemused, turvaintsidentide aruanded) dokumenteerida vajaliku detailsusega.

4. Juhtimisotsuste dokumentatsioon (sihtrühm: juhtkond)

   Juhtkond peab põhjendama valitud turbestrateegiat ja selle dokumenteerima. Dokumenteerida tuleb ka kõikide teiste valdkondade kohta langetatud turvet käsitlevad otsused, et need oleksid igal ajal kättesaadavad ja tagantjärele mõistetavad.

- Dokumentidele esitatavad vormistusnõuded

  Dokumendid ei pea ilmtingimata olema paberile välja prinditud. Dokumendi liik tuleks valida olenevalt vajadustest. Näiteks võib hädaolukordade halduse jaoks olla mõistlik rakendada tarkvaralahendusi, mis aitavad juba eeltööna registreerida kõik kontaktisikud ja hädaolukorras võetavad meetmed ning mida saab kriisiolukorras kohe mobiilselt kasutada. Samal ajal tuleb arvestada, et hädaolukorras peab selline tarkvaralahendus, kogu vajalik info ja tehnika (nt sülearvuti) ka reaalselt käepärast olema. Olenevalt turvaintsidendi tõsidusest võib teinekord jällegi olla parem kasutada ülevaatlikku ja praktilist väljaprinditud käsiraamatut.

  Institutsioonid peavad sageli järgima seadustest või lepingutest tulenevaid kohustusi, nt andmete säilitamise kohustust või töödeldava info detailsusastet. Dokumentatsioon täidab oma ülesannet vaid juhul, kui selle koostamisse ei teki suuri lünki ning kui seda pidevalt värskendatakse. Peale kõige muu tuleb dokumentatsioon ka selliselt märgistada ja hoiustada, et see oleks vajaduse korral kiiresti kättesaadav ja kasutatav. Dokumentatsioonist peab saama üheselt välja lugeda selle osade koostaja ja koostamise kuupäeva. Kui dokumentatsioonis viidatakse teistele allikatele, peab dokumentatsioonis ka need olema loetletud. Lisaks tuleb hoolitseda ka muude dokumentide kättesaadavuse eest.

  Turvet kajastav dokumentatsioon võib sisaldada konfidentsiaalset infot ning seetõttu tuleb seda asjakohaselt kaitsta. Dokumentatsiooni jaoks tuleb kindlaks määrata selle kaitsevajadus, säilitamise viis, kestus ja hävitamistingimused. Protsessikirjeldused peavad kajastama, kas ja kuidas dokumente nende nõuete suhtes analüüsitakse.

- Saadaolevate andmeallikate ja kogemuste kasutamine

  Infoturve on keeruline valdkond ning selle eest vastutavad töötajad peavad ennast teemaga hoolikalt kurssi viima. Teadmisi tuleb hankida väga paljudest allikatest. Nende hulka kuuluvad nt kõikvõimalikud normid ja standardid, internetis ja muul moel avaldatud väljaanded. Turvet puudutava info ja kogemuste vahetamise eesmärgil tuleks kindlasti teha koostööd ka erialaliitude, partnerite, nõukodade ning teiste ettevõtete ja asutustega (nt CERT-iga). Kuna infoturve on lai valdkond, on oluline, et iga institutsioon määraks enda jaoks kindlaks ja dokumenteeriks

andmeallikatele seatavad raamtingimused ning koostööpartnerid, kellega sel teemal suheldakse.

# 5 Infoturve ja ressursid

Soovitud turbeastme tagamine eeldab teatud ressursse, st nii raha, personali kui ka aega, ning selle eest peab hoolitsema juhtkond. Olukorras, kus seatud eesmärke ei ole võimalik saavutada puudulike ressursside tõttu, ei vastuta lõpptulemuse eest mitte töötajad, kellele tehti ülesandeks meetmete võtmine, vaid juhtkond, kes seadis kas ebarealistlikud eesmärgid või ei võimaldanud töötajatele piisavaid ressursse. Ebarealistlike eesmärkide vältimiseks on oluline, et kulusid ja nendest saadavat kasu analüüsitaks juba eesmärkide seadmisel. Sama analüüsiga tuleks kindlasti jätkata ka turbeprotsessi kestel, et vältida ühelt poolt ressursside raiskamist ning tagada teisalt, et soovitud turbeastme hoidmiseks tehtaks siiski vähemalt hädavajalikud investeeringud.

Väga sageli seostatakse IT-turvet eksikombel ainult tehniliste lahendustega. Ka see on põhjus, miks tuleks termini „IT-turve" asemel kasutada pigem terminit „infoturve". Ennekõike on aga oluline teada, et investeeringud personali on tihti palju efektiivsemad kui investeeringud turbetehnoloogiasse. Tehnika lahendab probleeme vaid juhul, kui see on tihedalt seotud organisatsiooni töökorralduse raamtingimustega. Piisavad ressursid tuleb muu hulgas tagada ka neile, kelle ülesanne on hinnata turbemeetmete tõhusust ja toimimist.

Praktika on näidanud, et organisatsioonisisestel turbeekspertidel on sageli liiga vähe aega, et analüüsida kõiki olulisi turbetegureid ja raamtingimusi (nt seadusi või tehnilisi küsimusi). Vahel puuduvad neil ka asjakohased baasteadmised, kuidas sellist analüüsi teha. Seetõttu on juhtudel, kus küsimusi ja probleeme ei suudeta oma töötajatega lahendada, kindlasti mõttekas kasutada välisekspertide abi. Selleks peavad institutsiooni turbeeksperdid esmalt olukorra dokumenteerima, et juhtkond saaks seejärel eraldada piisavalt ressursse.

IT-turbe üks peamine eeldus on hästi toimiv IT-käitus. Seetõttu tuleb IT-süsteemide käitamiseks eraldada piisavalt ressursse. Turbemeetmed saavad efektiivselt toimida enamasti alles pärast seda, kui institutsioon on suutnud lahendada IT-süsteemide käitamise tüüpprobleemid, milleks on nt väike eelarve, ülekoormatud administraatorid või halvasti struktureeritud ja hooldatud IT.

# 6 Töötajate kaasamine turbeprotsessi

Infoturve puudutab eranditult kõiki töötajaid. Igaüks saab vastutustundliku ja tagajärgedele mõtleva käitumisega anda panuse kahjude vältimisse ja turbeprotsessi edu tagamisse. Infoturbeaspektide teadvustamine ning töötajate ja ka kõikide juhttöötajate erialased koolitused on seega infoturbe tagamise põhieelduseks. Turbemeetmete nõuetekohane võtmine eeldab, et töötajatel on olemas vajalikud algteadmised. Siia alla kuuluvad teadmised nii sellest, kuidas turbemeetmetega ümber käia, kui ka sellest, mis on nende meetmete mõte ja eesmärk. Infoturbe tagamist mõjutavad oluliselt ka töökliima, ühised väärtused ja töötajate koostöövalmidus.

Uute töötajate lisandumisel või olemasoleva personali tööülesannete muutumisel tuleb töötajad põhjalikult teemaga kurssi viia ja välja õpetada. Koolitus peab hõlmama ka töökoha turbenõudeid. Olukorras, kus töötaja lahkub institutsioonist või tema pädevusvaldkond muutub, tuleb võtta asjakohaseid turbemeetmeid (nt volituste tühistamine, võtmete ja lubade tagasiküsimine).

Töötajatele tuleb selgitada, et neil on kohustus järgida nende tööd puudutavaid seadusi, ettekirjutusi ja reegleid. Selleks tuleb nad esmalt muidugi asjakohaste infoturvet puudutavate reeglite ja muuga kurssi viia, hoolitsedes samal ajal ka selle eest, et nad oleksid piisavalt motiveeritud neid reegleid järgima. Töötajad peavad kindlasti teadma, et igast olukorrast, mil esineb turvaintsident (või sellekohane kahtlus), tuleb kindlasti teavitada infoturbehalduse eest vastutavaid töötajaid, samuti peab olema selge, kuidas ja kellele nad peaksid sellest teada andma.

# 7 Infoturbeprotsess

Juhtkond peab määrama kindlaks ametiasutuse või ettevõtte turbe-eesmärgid, võttes sealjuures arvesse kõiki olulisi raamtingimusi ja institutsiooni eesmärki, ning looma eeldused, mis lubaksid seda eesmärki täita. Strateegia viiakse ellu turbekontseptsiooniga ja infoturbehalduse töökorraldusega. Järgnevalt kirjeldatakse kasutustsükli iga faasi jaoks olulisi haldustegevusi. Turbekontseptsiooni käsitletakse eraldi peatükis, et anda sellest mahukast teemast parem ülevaade.

## 7.1 Turbeprotsessi planeerimine

**ISMS-i kehtivusala kindlaksmääramine**

Infoturbehalduse süsteemi ei pea ilmtingimata juurutama terves institutsioonis. Esmalt tuleks välja selgitada ISMS-i kehtivusala, st valdkond, mille eest see peaks hakkama vastutama. Kehtivusala võib sageli hõlmata tervet institutsiooni, kuid võib piirduda ka ainult ühe või mitme tööprotsessi või organisatsiooni allüksusega. Siinkohal on oluline, et tööprotsessid jääksid täielikult vastutusala piiridesse. IT-etalonturbes nimetatakse kehtivusala ka infokoosluseks. Infokooslus hõlmab sel juhul vaadeldava kasutusvaldkonna kõiki info töötlemiseks mõeldud taristuid ning töökorraldust, personali ja tehnilisi komponente.

**Raamtingimuste väljaselgitamine**

Infoturbe tagamine ei ole eesmärk omaette. Värske ja usaldusväärne info on väga paljude tööprotsesside põhieeldus. IT ja sidelahendused toetavad mõistlikul määral institutsiooni tööd ja tegevuse eesmärke. Infoturbestrateegia väljatöötamisel tuleks arvestada vähemalt järgmiste aspektidega:

- ettevõtte või ametiasutuse tegevusele seatud eesmärgid;
- seadustest tulenevad nõuded ja ettekirjutused, nt andmekaitse valdkonnas;
- klientide ootused ja kehtivad lepingud;
- institutsioonisisesed raamtingimused (nt institutsiooniülene riskihaldus või IT-taristu);
- (IT-toega) tööprotsessid;
- tööprotsesse tabavate turvaintsidentide võimalikud globaalsed ohud (nt imago kaotus, seaduste või lepingu nõuete rikkumine, uurimistööde vargus).

**Turbe-eesmärkide sõnastamine ja infoturbepoliitika väljatöötamine**

Esmalt sõnastatakse turbe-eesmärgid ja seejärel võetakse vastu strateegilised otsused, kuidas neid eesmärke täita. Põhitõed tuleks koondada infoturbepoliitikasse (ingl Information Security Policy või IT Security Policy). Turbepoliitika peaks kajastama vähemalt järgmisi teemasid:

- ettevõtte või ametiasutuse turbe-eesmärgid;
- infoturbe eesmärkide seos institutsiooni eesmärkide ja ülesannetega;
- eesmärgiks seatud turbeaste;
- olulisemad väited selle kohta, kuidas tuleks soovitud turbeastet saavutada;
- olulisemad väited selle kohta, kas ja kuidas tuleks turbeastme saavutamist tõendada.

Infoturbepoliitika peab vastu võtma juhtkond ning see tuleb institutsioonis avalikustada.

**Infoturbe töökorralduse ülesehitus**

Infoturbe töökorralduse hulka kuulub organisatsiooni struktuuri kindlaksmääramine (nt osakonnad, rühmad ja kompetentsikeskused) ning rollide ja tööülesannete defineerimine. Juhatuse kõrgeimal

tasandil tuleb ametisse nimetada infoturbe eest vastutav töötaja, nt tegevjuht. Lisaks tuleb ametisse nimetada vähemalt üks infoturbespetsialist. Spetsialistil peab olema võimalik teha oma tööd teistest sõltumatult ning ta peab juhtkonnale regulaarselt aruandeid esitama.

## 7.2 Infoturbepoliitika rakendamine

Soovitud turbe-eesmärkide saavutamiseks tuleb koostada turbekontseptsioon. Parema ülevaate tagamiseks käsitletakse turbekontseptsiooni planeerimist, rakendamist ning saavutatud turbeastme säilitamist ja parandamist eraldi peatükis. Turbemeetmete kontrolli tulemusi käsitletakse turbeprotsessi tõhususe kontrolli osana ning neid hindab juhtkond.

## 7.3 Turbeprotsessi tõhususe kontroll

Juhtkond peaks regulaarselt hindama turbeprotsessi tõhusust (andma juhtkonna hinnangu). Vajaduse korral (nt kui esineb tavapärasest rohkem turvaintsidente või kui raamtingimustes peaks toimuma suuri muutusi) tuleks asjakohaseid koosolekuid pidada ka kokkulepitust sagedamini. Kõik tulemused ja otsused tuleb arusaadavalt dokumenteerida .

Arutelude käigus tuleb muu hulgas arutada järgmisi küsimusi:

- kas raamtingimustes on toimunud selliseid muutusi, mis sunnivad muutma senist infoturbe tagamise metoodikat?
- kas turbe-eesmärgid on jätkuvalt asjakohased?
- kas infoturbepoliitika on jätkuvalt piisavalt ajakohane?

Turbeprotsessi tõhususe kontrollimisel ei tuleks keskenduda mitte üksikute turbemeetmete või töökorraldust puudutavate meetmete kontrollimisele, vaid tervikliku ülevaate saamisele.

Kindlasti on abiks, kui kontrollida, kuidas on turbekontseptsioon ja turbevaldkonna töökorraldus ennast seni õigustanud. Turbemeetmete täpsemat kontrollimist käsitletakse lähemalt turbekontseptsiooni peatükis. Kontrolli tulemustega tuleks arvestada ka turbestrateegia tõhususe hindamisel. Näiteks kui peaks selguma, et senised turbemeetmed kas ei toimi piisavalt hästi või on liiga kallid, on see piisav põhjus, et võtta ette turbestrateegia analüüs ja kohandamine. Esitada tuleks järgmised küsimused:

- kas turbestrateegia on jätkuvalt asjakohane?
- kas turbekontseptsioon võimaldab saavutada seatud eesmärke ning kas nõudeid, nt seadusi, täidetakse?
- kas infoturbe töökorraldus tagab eesmärkide saavutamise ning kas tööd korraldavate töötajate kompetentsi tuleks suurendada või tuleks neid senisest tugevamini tööprotsessidesse kaasata?
- kas turbe-eesmärkide saavutamiseks (nii vahenditele kui ka personalile) tehtud kulutused on proportsionaalsed nendest saadava kasuga?

Tõhususe kontrolli tulemusi tuleb järjekindlalt kasutada asjakohaste korrektuuride tegemiseks. See võib tähendada nt turbe-eesmärkide, -strateegia või -kontseptsiooni muutmist ning infoturvet tagava töökorralduse ümberkujundamist. Olukorras, kus olemasolevate vahenditega ei õnnestu infoturvet piisavalt hästi tagada, tuleb võib-olla tööprotsesse või IT-kooslust suuresti ümber kujundada, millestki loobuda või otsustada väljasttellimise kasuks. Kui otsustatakse teha suuremaid muudatusi ja parandusi, tuleb turbehaldusega tegelevatel töötajatel taas kord alustada turbe planeerimisest.

# 8 Turbekontseptsioon

## 8.1 Turbekontseptsiooni koostamine

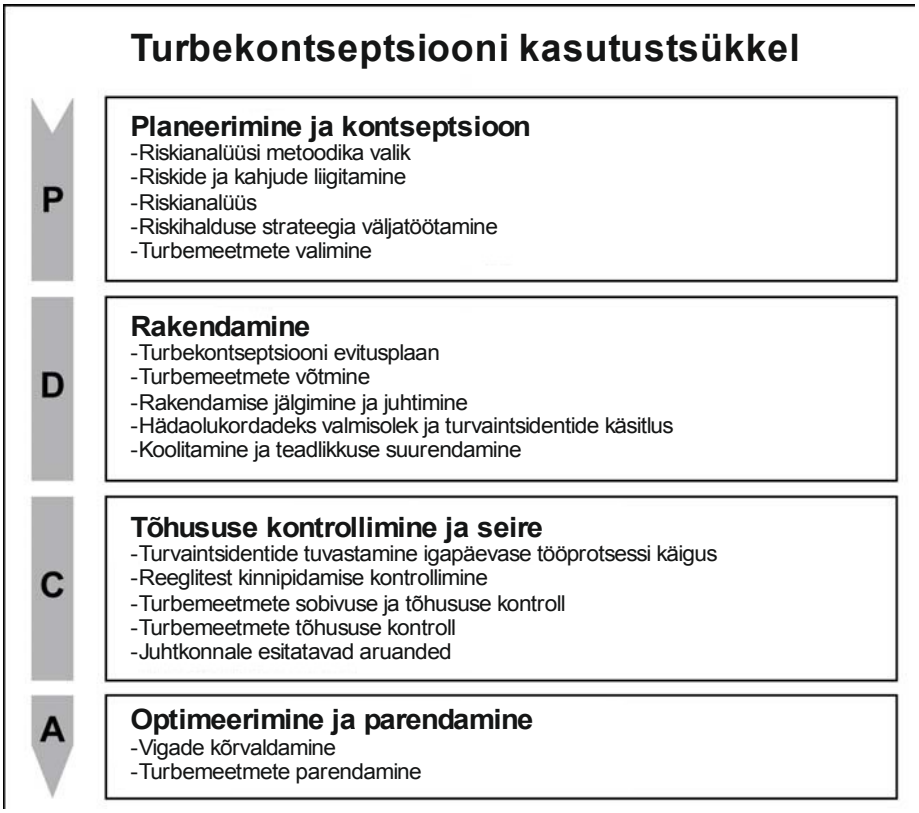
Infoturbele seatud eesmärkide täitmiseks ja soovitud turbeastme saavutamiseks tuleb esmalt aru saada, mil määral oleneb tööprotsesside täitmine info konfidentsiaalsusest, terviklusest ja käideldavusest. Selleks tuleb muu hulgas jõuda selgusele, kui palju võivad tööprotsesse ohustada erinevad tegurid, nt vääramatu jõud, halb töökorraldus, inimvead ja IT-riskid. Seejärel tuleb otsustada, kuidas nende riskidega toimida. Läbi tuleb teha järgmised sammud.

**Riskianalüüsi metoodika valik**

Institutsioon peab analüüsima ja hindama, kui tugevasti võivad turvaintsidendid mõjutada igapäevaseid tööprotsesse. Seetõttu on igas infoturbehalduse süsteemis oma kindel koht ka riskianalüüsil. Riskide tõenäosuse hindamiseks tuleb välja selgitada ohud ning hinnata nende kahjupotentsiaali ja esinemise tõenäosust. Olenevalt institutsiooni tegevusvaldkonnast, töökorralduslikest raamtingimustest ja eesmärgiks seatud turbeastmest võib riskianalüüsiks kasutada erinevaid metoodikaid. Infoturbehalduse eest vastutavad töötajad peavad valima välja metoodika, mis oleks kooskõlas institutsiooni liigi ja suurusega. Metoodika valikust oleneb suuresti turbekontseptsiooni koostamiseks kuluv vajalike tööde maht.

Erinevaid riskianalüüsi liike kirjeldab standard ISO/IEC 27005. Väga praktiline lahendus on kindlasti IT-etalonturbe metoodika, mida saab rakendada IT-etalonturbe kataloogide põhjal. Seda täiendab omakorda standard BSI 100-3 „IT-etalonturbel põhinev riskianalüüs”.

IT-etalonturbe või teiste hea tava alla kuuluvate metoodikate kasutamise eelis seisneb selles, et isiklik töövaev on viidud miinimumini, sest autorid toovad välja täiesti konkreetsed meetodid ja pakuvad välja sobivaid turbemeetmeid.



Joonis 6. Turbekontseptsiooni kasutustsükli ülevaade

**Riskide ja kahjude liigitamine**

Infoturbehaldus peab valitud riskianalüüsi metoodika põhjal kindlaks määrama, kuidas ohte ning nende potentsiaalset kahju ja esinemise tõenäosust ning nendest tulenevaid riske liigitada.

Siinkohal tuleb tõdeda, et kahjude ja nende tekke tõenäosuse väljaselgitamine on väga raske, töömahukas ning peale selle ka veel küllaltki aldis vigadele. Seetõttu tuleks vigade ja nende tekke tõenäosuse hindamisel loobuda liigsest täpsusest, et sellele ei kuluks liiga palju aega. Paljudel juhtudel on seda tööd tunduvalt lihtsam teha, kui kasutada nii kahju suuruse kui ka selle esinemise tõenäosuse hindamiseks kategooriaid. Neid ei tohiks aga luua liiga palju, piisab kolmest kuni viiest kategooriast:

- esinemise tõenäosus: harva, tihti, väga tihti;
- kahju potentsiaalne suurus: keskmine, suur, väga suur.

Pärast seda, kui kategooriad on institutsiooni jaoks sobivalt kindlaks määratud, saab neid kasutada riskianalüüsis.

**Riskianalüüs**

Iga riskianalüüs peab koosnema järgmistest etappidest:

- kaitstava info ja tööprotsesside tuvastamine;
- kaitstava info ja tööprotsessidega seotud peamiste ohtude tuvastamine;
- ohtudele aldiste kohtade tuvastamine;
- konfidentsiaalsuse, tervikluse ja käideldavuse kadumisel tekkivate kahjude tuvastamine ja võimalike tagajärgede hindamine;
- tööprotsesside võimalike turvaintsidentide mõju analüüs;
- turvaintsidentide kahjuriski kohta hinnangu andmine.

**Riskihalduse strateegia väljatöötamine**

Juhtkonna kõrgeim tasand peab kehtestama suunised, kuidas riskidega ümber käia. Asjakohaste suuniste koostamine juhtkonna jaoks on infoturbehalduse eest vastutavate isikute ülesanne. Võimalikud on järgmised variandid:

- riske püütakse vältida adekvaatsete turbemeetmete võtmisega;
- riske püütakse vältida tööprotsesside ümberstruktureerimise või nendest loobumisega;
- riske võidakse delegeerida, nt väljasttellimise või kindlustuslepingute sõlmimisega;
- riskidega võidakse leppida.

Juhtkonna kõrgeim tasand peab riskidega ümberkäimise suunised kinnitama ja dokumenteerima. Strateegia elluviimiseks tuleb planeerida ja eraldada vajalikud ressursid.

Strateegia väljatöötamisel peab juhtkond arvestama, et võimalike kulude kõrval on oluline otsustuskriteerium kindlasti ka valitud strateegiaga kaasnevad jääkriskid. Seetõttu tuleb jääkriske analüüsida ning need tuleb dokumenteerida.

**Turbemeetmete valimine**

Juhtkonna kehtestatud üldiste turbe-eesmärkide ja turbenõuete põhjal tuleb välja valida konkreetsed turbemeetmed. Turbemeetmete valimisel ei tule arvestada mitte üksnes sellega, kuidas need võivad mõjutada turbeastet või kas kulud ja saadav kasu on omavahel kooskõlas, vaid ka sellega, kas meetmed on piisavalt praktilised.

Tehniliste turbemeetmete kõrval tuleb võtta kindlasti ka töökorraldust puudutavaid meetmeid (nt kasutussuunised, volituste andmine, turbekoolitused, katsetamise ja kasutusse lubamise protseduurid). Reguleerida tuleb muu hulgas järgmisi valdkondi:

- töökorraldus (k.a vastutusalade kindlaksmääramine, tööülesannete jaotamine ja ametite lahutamine, info, rakenduste ja IT-komponentide kasutamise reeglid, riist- ja tarkvara haldus, muudatuste haldus);
- personal (nt uute töötajate juhendamine, asenduste reguleerimine);
- infoturbekoolitused ja teadlikkuse suurendamine;
- andmevarundus (eri liiki andmed, rakendused ja IT-komponendid);
- andmekaitse;
- viirusetõrje;
- info kaitsmine andmetöötluse ja -edastuse ning salvestamise käigus (nt krüptograafia kasutamine);
- riist- ja tarkvara arendamine;
- käitumine turvaintsidentide korral (ingl *incident handling*);
- hädaolukordadeks valmistumine ja tööprotsesside tagamine hädaolukorras (ingl *business continuity*);
- väljasttellimine.

Otsused tuleb dokumenteerida, et oleks võimalik aru saada, kuidas peavad valitud turbemeetmed suutma täita nii turbe-eesmärke kui ka -nõudeid.

## 8.2 Turbekontseptsiooni rakendamine

Pärast turbemeetmete väljavalimist tuleb need evitusplaani alusel kasutusele võtta. Selle juures tuleb järgida järgmisi etappe.

**Turbekontseptsiooni evitusplaani koostamine**

Evitusplaan peab kajastama järgmisi teemasid:

- prioriteetide kindlaksmääramine (evitustööde järjekord);
- evitamise algatamise eest vastutavate isikute kindlaksmääramine;
- ressursside eraldamine juhtkonna poolt;
- meetmete evitusplaan (tähtajad, kulud, meetmete evitamise, evitamise kontrollimise ja meetmete efektiivsuse eest vastutavate töötajate kindlaksmääramine).

**Turbemeetmete võtmine**

Planeeritud turbemeetmeid tuleb võtta vastavalt evitusplaanile. Nende tööde käigus tuleb infoturve integreerida organisatsiooni töökorralduse ja -protsessidega. Kui rakendamisel peaks tekkima tõrkeid, tuleks nendest viivitamatult teada anda, et neid saaks analüüsida ja seejärel kõrvaldada. Tüüplahendustena võivad kõne alla tulla nt suhtluskanalite ja volituste muutmine või teistsuguste tehniliste meetmete võtmine.

**Rakendamise juhtimine ja kontrollimine**

Eesmärkide täitmist tuleb regulaarselt kontrollida. Olukorras, kus eesmärkide täitmine osutub võimatuks, tuleb sellest teavitada juhtkonna tasandil infoturbe eest vastutavat isikut, et probleemidele saaks õigel ajal reageerida.

## 8.3 Turbekontseptsiooni tõhususe kontroll ja parandamine

Turbeastme säilitamiseks tuleb ühelt poolt hoolitseda selle eest, et heakskiidetud turbemeetmeid võetaks võimalikult korrektselt, ning teisalt selle eest, et turbekontseptsiooni pidevalt edasi arendataks. Kindlasti tuleb tagada ka see, et turvaintsidendid avastataks kiiresti ning neile reageeritaks võimalikult pädevalt ja viivitusteta. Seetõttu tuleb turbekontseptsiooni tõhusust regulaarselt kontrollida. Võetud meetmete tõhusust tuleks kontrollida siseauditite raames. Kui selleks ei ole piisavalt ressursse, st pole piisaval hulgal pädevaid töötajaid, tuleks auditid tellida väljast.

Kuna auditite töömaht oleneb institutsiooni suurusest ja keerukusest, on väiksematele ettevõtetele ja ametiasutustele seatavad nõuded suurte institutsioonidega võrreldes kindlasti väiksemad ning seega ka lihtsamini täidetavad.

Kontrollimine peaks sisaldama järgmisi tegevusi.

**Reageerimine igapäevases tööprotsessis tehtavatele muudatustele**

Kui igapäevastes tööülesannetes midagi muudetakse (lisatakse juurde uusi tööprotsesse, muudetakse töökorraldust, võetakse kasutusele uusi IT-süsteeme), tuleb uuendada nii turbekontseptsiooni kui ka teisi sellega seotud dokumente (nt töötajate vastutusalasid ja IT-süsteemide inventari loetelu).

**Turvaintsidentide tuvastamine igapäevase tööprotsessi käigus**

Tuleb võtta meetmeid, mis aitaksid vältida infotöötluses esinevaid vigu (konfidentsiaalsust, käideldavust või terviklust pärssivaid vigu), turbe vaatevinklist vääri tegevusi ja turvaintsidente, et nende tagajärjed oleksid kas võimalikult väiksed või vähemalt kiiresti avastatavad. Turbeprobleemide võimalikult varajaseks tuvastamiseks võib kasutada nt erinevaid tarkvaralisi ja muid lahendusi, nt süsteemiseiret, tervikluse kontrolle, pöörduste, tegevuste ja vigade logimist, hoonete ja ruumide sissepääsukontrolle, tule- ja veeohutuse andureid ning kliimaandureid.

Tuvastussüsteemide salvestisi ja logisid tuleb regulaarselt analüüsida.

**Reeglitest kinnipidamise kontrollimine**

Regulaarselt tuleb kontrollida, kas kõiki turbemeetmeid võetakse täpselt nii, nagu turbekontseptsioon seda ette näeb. Selleks tuleb kontrollida nii tehniliste turbemeetmete (konfiguratsioonide) kui ka töökorralduse (tööprotsesside) vastavust nõuetele. Lisaks tuleks kontrollida seda, kas meetmete võtmiseks on olemas vajalikud ressursid ning kas kõik isikud, kellel on määratud teatud rollid, täidavad oma ülesandeid piisavalt kohusetundlikult.

**Turbemeetmete sobivuse ja tõhususe kontroll**

Regulaarselt tuleb kontrollida, kas võetud turbemeetmetega on võimalik saavutada eesmärgiks seatud turbeastet. Sobivuse kontrollimiseks tuleks nt analüüsida seni aset leidnud turvaintsidente, küsitleda töötajaid või teha penetratsioonikatseid. Siia alla kuulub ka ametiasutuse või ettevõtte tööprotsesside olulisemate arengusuundumuste jälgimine. Võib juhtuda, et vahepeal on tehtud kas tehnilisi muudatusi või on muutunud tööd reguleerivad raamtingimused. Enda kursishoidmiseks peaks turbe eest vastutav töötaja lugema nt erialast kirjandust, külastama turbekonverentse ja otsima uut infot ka internetist. Kui oma töötajatel vajaminevaid teadmisi ja aega napib, tuleks kasutada väliseid eksperte.

Selles kontekstis oleks muu hulgas mõistlik uurida, kas võetud turbemeetmed on efektiivsuse poolest parim võimalik valik või õnnestuks teistsuguste meetmete võtmisega turbe-eesmärke saavutada ka väiksemate ressurssidega. Samuti tuleks kontrollida tööprotsesside ja -korralduse praktilisust ja efektiivsust. Sellistest kontrollidest saadakse sageli palju uusi ideid, kuidas tööprotsesse ümber korraldada.

**Juhtkonna hinnangud**

Infoturbehaldus peab juhtkonda oma kontrollide tulemustest regulaarselt ja sobivas vormis informeerima. Juhtkonda tuleb teavitada probleemidest, õnnestumistest ja võimalustest, kuidas midagi

paremaks muuta.

Juhtkonnale esitatavad aruanded peavad kajastama turbeprotsessi juhtimiseks vajalikku infot. Selline info on nt:

- turbeprotsessi hetkeseisundi ülevaade;
- hinnang juhtkonna eelmise hinnangu põhjal võetud meetmete tõhususele;
- klientidelt ja töötajatelt laekunud tagasiside;
- töös esinenud uute ohtude ja turvaaukude ülevaade.

Juhtkond võtab turbehalduse aruanded teadmiseks ning teeb seejärel vajalikud otsused ressursside kasutamise ja turbeprotsessi ümberkorraldamise kohta (nt otsus riske vähendada või enda vastutusel riski taluda).

Turbeprotsessi tõhususe regulaarse kontrollimise eesmärk on kõrvaldada tuvastatud vead ja turvaaugud ning muuta turbemeetmed efektiivsemaks.

Tegevus ei tohiks piirduda üksnes tehniliste meetmetega. Mõnikord on tarvis töötajaid ka koolitada või teavitada. Siinkohal tuleks suurendada ka töötajate vastuvõtlikkust turbemeetmete suhtes. Selleks, et töötajad nendega paremini lepiks, tuleb nii tehnilised turbemeetmed kui ka töökorraldus muuta võimalikult praktiliseks.

# 9 BSI infoturbehalduse süsteem (ISMS): IT-etalonturve

## 9.1 Sissejuhatus

Infoturbehalduse süsteemi kirjeldus on nii selles dokumendis kui ka standardites ISO 27000, 27001 ja 27002 esitatud ainult väga lühidalt ning kajastab vaid üldist raamistikku. Seetõttu tuleb praktikas sageli silmitsi seista tõsiasjaga, et üldiste soovituste rakendamiseks on väga palju võimalusi. Keeruliseks muudab olukorra see, kuidas juurutada institutsioonis asjakohane infoturbehalduse süsteem, mis mitte üksnes ei aitaks turbe-eesmärke saavutada, vaid teeks seda ka võimalikult väikeste kuludega.

Kõige keerulisem etapp, mis siinjuures tuleb läbida, on institutsiooni turbekontseptsiooni koostamine. Turbekontseptsiooni väljatöötamisel tuleb lähtuda riskianalüüsist ja valitud turbemeetmetest. Oluline on siinkohal ka riskianalüüsi metoodika, sest sellest oleneb suurel määral analüüsi koostamiseks kuluvate tööde maht. Enamasti sobib selleks IT-etalonturbe metoodika. See metoodika on klassikaliste, st kvantitatiivsete riskianalüüsimeetoditega võrreldes palju soodsam ning praeguseks juba ka aastaid praktikas järele proovitud. IT-etalonturbe metoodika väärtus seisneb selles, et see mitte üksnes ei kirjelda infoturbehalduse süsteemi üldisi tööpõhimõtteid, vaid annab IT-etalonturbe kataloogide näol ka praktilisi näpunäiteid, kuidas meetmeid võtta.

Selles peatükis kirjeldatakse IT-etalonturbe olulisimaid komponente ja näidatakse, et IT-etalonturbe metoodika on täielikult kooskõlas standardiga ISO 27001 . IT-etalonturbe metoodika põhjalikuma kirjelduse leiate standardist BSI 100-2 .

IT-etalonturbe metoodika raames kirjeldatakse infoturbehalduse süsteemi juurutamist ja selle tööshoidmist, lähtudes IT-etalonturbe kataloogidest. Selles dokumendis mainitud teemasid käsitletakse põhjalikumalt IT-etalonturbe kataloogides, mis sisaldavad muu hulgas ka praktilisi juhiseid. Iga IT-etalonturbe kataloogides toodud moodul järgib kasutustsükli mudelit ning sisaldab erimeetmeid alates planeerimisest ja lõpetades utiliseerimisega.

## 9.2 IT-etalonturbel põhinev turbeprotsess

Kõik infoturbehalduse levinud meetodid, head tavad ja standardid on oma teostuses üpris sarnaste tööülesannetega: tegelevad turbeprotsessi tagamisega või juhtkonna juhtimisülesannetega. Kõige suuremad erinevused seisnevad turbekontseptsiooni koostamises, st selles, kuidas tehakse riskianalüüs ja kuidas valitakse sobivad turbemeetmed. Seetõttu kirjeldatakse siinkohal lähemalt IT-etalonturbel põhineva turbekontseptsiooni koostamist.

### 9.2.1 Riskianalüüs

**Infoturbe riskianalüüs**

Infoturbe riskianalüüs erineb oluliselt kindlustusfirmade või juhtkonna klassikalisest riskianalüüsist. Klassikalisi või kvantitatiivseid riskianalüüsimeetodeid on enamasti võimatu järgida, sest puuduvad andmed, mis lubaksid täpselt välja arvutada kahjude suurust või nende tekke tõenäosust. Ka neil juhtudel, kus see on siiski võimalik, osutub tulemuste lahtimõtestamine väga raskeks.

Näide. Klassikalises riskianalüüsis saadakse risk kahju suuruse ja tekke tõenäosuse jagatisest. Oletame, et arvutuskeskuse puhul soovitakse hinnata hävingu riski seoses lennukatastroofidega. Seega kui arvutuskeskuse väärtuseks hinnatakse 20 mln eurot ja statistika põhjal leitakse, et lennukatastroofi tekke tõenäosus on üks kord 20 000 aasta kohta, on teoreetiline risk 1000 eurot aastas. Sama tulemus saadakse ka siis, kui sülearvuti (või selles hoitavate andmete) väärtus hinnatakse 2000 eurole ja vaadeldakse statistilist tõenäosust, et sülearvuti võidakse vähemalt kord kahe aasta jooksul ära varastada. Kuigi riski suurus on matemaatiliselt võrdne, tuleb neid kahte juhtumit infoturbe valdkonna puhul käsitleda erinevalt.

Paljude oletatavate riskijuhtumite kohta puuduvad empiirilised andmed, mis lubaksid nende tekke tõenäosuse kohta midagi kindlat väita, sest nt uue tehnoloogia evitamisel lihtsalt ei ole piisavalt võrdlusmaterjali. Seevastu juhtudel, kus riskide tõenäosuse ja kahjude suuruse väljaarvutamiseks on enam-vähem tõsiselt võetavad andmed juba olemas, pole turbekontseptsiooni koostamine klassikaliste riskianalüüsimeetoditega eriti mõttekas, sest see on väga töömahukas ja kallis. Kõikide oluliste tööprotsesside ja nendega seotud IT-süsteemide kitsaskohtade analüüsimiseks, samuti selleks võimalikke kahjusid ning nende tõenäosust ja suurust kajastava loetelu koostamiseks läheb tarvis väga põhjalikke algteadmisi ning see eeldab väga suurte andmehulkade läbitöötamist.

IT-etalonturbe metoodika sisaldab muu hulgas riskianalüüsi kvalitatiivset meetodit, mis aitab koguda alginfot tööprotsesse ähvardavate turvaintsidentide hindamiseks. IT-etalonturbe metoodika lähtub asjaolust, et olenemata institutsiooni liigist ja eesmärgist on kõikjal alati tarvis tagada olulise tööinfo turvaline töötlus, kõikjal kasutatakse enim levinud ja seega sarnaseid IT-süsteeme ning kõikjal valitsevad kui mitte sarnased, siis vähemalt võrreldavad tingimused. Seetõttu on sageli tegu ka sarnaste ohtudega. Tööprotsesside turbenõuded on küll individuaalsed ja võivad suuresti erineda, kuid praktikas viivad need siiski sageli küllaltki sarnaste turbemeetmete võtmiseni.

BSI analüüsib oma IT-etalonturbe metoodikast lähtuvates IT-etalonturbe kataloogides tüüpsete kasutusvaldkondade ja komponentide kitsaskohti ning toob nende põhjal välja levinud ohud. Ohtudest käsitletakse ainult selliseid, mis on hoolika analüüsi põhjal liigitatud sageli esinevate ohtude hulka ning mis on nii suurte tagajärgedega, et nende vastu tuleb võtta turbemeetmeid. Tüüpilised ohud, mille vastu igaüks peab end kaitsma, on tulekahjud, veekahjustused, sissemurdmine, arvutiviirused ja riistvara defektid. Sellise käsitluse eelis seisneb selles, et IT-etalonturbe metoodika kasutaja ei pea ohtude ja kitsaskohtade väljaselgitamiseks hakkama iseseisvalt otsast lõpuni tervet infokooslust analüüsima, vaid saab kasutada teiste eeltööd.

Ohtude kõrval kirjeldatakse IT-etalonturbe kataloogides ka tüüpobjektidel rakendatavaid, end juba praktikas tõestanud ning tehnikat, taristuid, personali ja töökorraldust puudutavaid standardseid turbemeetmeid.

Info ja tööprotsesside jaoks, mille turbevajadus on kas suur või väga suur ning mida IT-etalonturve ei käsitle, tuleb teha täiendav turbeanalüüs ja võib-olla ka riskianalüüs. IT-etalonturbe metoodikal põhinevat lihtsustatud riskianalüüsi meetodit kirjeldab standard BSI 100-3.

Nii IT-etalonturbel põhinev riskianalüüs kui ka dokumendis BSI 100-3 kirjeldatud riskianalüüs on kvantitatiivse riskianalüüsiga võrreldes märgatavalt lihtsamad ja odavamad. IT-etalonturbel põhineva riskianalüüsi eelis on ka veel see, et seda saavad kasutada väga erinevad institutsioonid, luues ühtse ja selgelt defineeritud aluse oma riskide hindamiseks.

**Riskide liigitamine**

IT-etalonturve kasutab riskide liigitamiseks järgmisi tööetappe.

1. Lähtumine kahjustsenaariumidest

   Turvaintsidentidega kaasneva kahju ja teiste negatiivsete tagajärgede näitlikustamiseks ja kirjeldamiseks tuleks neid vaadelda erinevate stsenaariumidena:

   - seaduste, ettekirjutuste või lepingute rikkumine;
   - infot puudutava iseseisva otsustamise õiguse piiramine;
   - isikupuutumatuse rikkumine;
   - tööülesannete täitmise piiramine;
   - negatiivsed sise- ja välismõjud;
   - rahalised tagajärjed.

   Stsenaariume läbi mängides tuleks uurida, millised kahjud võivad konfidentsiaalsuse, tervikluse ja

käideldavuse kadumisel tekkida.

Näiteks tuleks seaduste rikkumise stsenaariumi analüüsimisel muu hulgas uurida, milliseid andmeid peab seaduste kohaselt käsitlema konfidentsiaalsena ning millised on nende nõuete tahtliku rikkumise tagajärjed.

2. Kahjupõhine liigitus: turbevajaduse kategooriate defineerimine

Oletatavate kahjude suurust ei ole sageli üldse mõistlik täpselt välja arvutada, sest see võib olla isegi võimatu ning sobivate turbemeetmete valimiseks pole seda tarvis. Seetõttu on soovitatav kahjud liigitada vähestesse klassidesse. Levinud soov – arvutada välja kahjude võimalikult täpne suurus – võib mõningatel juhtudel turvet isegi kahjustada, sest täpne osutub sageli hoopis ebatäpseks ja siis ei lähtu vastutavad töötajad mitte reaalsest turbeolukorrast, vaid hoopis oletustest.

IT-etalonturbes defineeritakse turbevajaduse hindamiseks kolm kategooriat, mida kasutatakse ka objektide (nt IT-süsteemide) turbevajaduse liigitamiseks:

| | |
|---|---|
| tavaline turbevajadus: | kahjude tagajärjed on piiratud ja ülevaatlikud |
| suur turbevajadus: | kahjudel võivad olla ulatuslikud tagajärjed |
| väga suur turbevajadus: | kahjude tõttu võib ohtu sattuda institutsiooni edasitoimimine, kahjudel on katastroofilised tagajärjed |

Iga institutsioon peab enda jaoks ise kindlaks määrama, mida L, M, H turbevajadus nende jaoks tähendab, st defineerima, mille poolest turbevajaduse kategooriad üksteisest erinevad. Kuna sellest olenevad suuresti nii riskidega ümberkäimine kui ka vajadus ressursside järele, peab asjakohased definitsioonid kinnitama juhtkonna kõrgeim tasand. Turbevajaduse kategooriate kindlaksmääramine võib eri institutsioonides olenevalt nende liigist ja suurusest väga erineda ning seega saab neid defineerida ainult juhtkonna ja infoturbehalduse eest vastutavate töötajate koostöös. Seetõttu saab BSI siinkohal tuua vaid asjakohaseid näiteid, mida tuleb tingimata kohandada konkreetse olukorraga.

Rahaliste kahjude liigitamise näide

Tavalise turbevajaduse all käsitletakse kahjusid, mille rahalised tagajärjed on institutsioonile talutavad. Väiksema ettevõtte puhul võib see tähendada nt seda, et turvaintsidendist tekkiv kahju ei tohi olla suurem kui 10 000 eurot. Suur turbevajadus tähendab, et rahaline kahju võib olla märkimisväärne, kuid ei ohusta ettevõtte edasitoimimist. Väiksema ettevõtte puhul võib see tähendada kahju suurusjärgus 10 000–100 000 eurot. Väga suur turbevajadus tähendaks seda, et rahaline kahju seab ohtu institutsiooni edasitoimimise. Väiksemate ettevõtete puhul võib see tähendada enam kui 100 000 euro suurust kahju. Seevastu suuremate pankade puhul on need numbrid kindlasti teistsugused.

**Riskianalüüs**

1. Struktuurianalüüs: kaitstavate objektide väljaselgitamine

   Struktuurianalüüsiga selgitatakse vaadeldava infokoosluse, nt kehtivusala või tööprotsessi jaoks välja selle olulised kaitstavad objektid, nt info, rakendused, IT-süsteemid, võrgud, ruumid, hoone ja vastutavad töötajad.

   Lisaks tuleb struktuurianalüüsiga ära näidata ka kaitstavate objektide kokkupuutepunktid ja sõltuvusseosed. Sõltuvusseoste kirjeldamise peamine eesmärk on aidata välja selgitada tööprotsesse ohustavate turvaintsidentide võimalikud mõjud, et neile saaks asjakohaselt reageerida.

   Näide. Kui serverit xy tabab turvaintsident, tuleb kiiresti välja selgitada, milliseid rakendusi või tööprotsesse see intsident ohustab.

2. Turbevajaduse kindlaksmääramine: tööprotsesse tabavate turvaintsidentide mõjude analüüs

Iga struktuurianalüüsi raames tuvastatud väärtuse kohta tuleb kindlaks määrata selle turbevajadus.

Näide. Kui turvaintsidendi tõttu lakkab IT-süsteem töötamast ja selle tagajärjel võib tekkida suur kahju, loetakse selle IT-süsteemi turbevajadus suureks.

Esmalt tuleb välja selgitada seotud tööprotsesside turbevajadused. Seejärel saab sellele infole toetudes tuvastada struktuurianalüüsi käigus üles märgitud rakenduse turbevajadused. Sealjuures tuleb arvestada, millist infot erinevate rakendustega töödeldakse. Väga paljudes institutsioonides piisab info kirjeldamiseks juba väga vähestest kategooriatest. Nendeks võivad olla nt kliendiandmed, avalik info (nt aadress, lahtiolekuajad) ja juhtkonna strateegilised andmed. Seejärel tuleks jõuda selgusele, kuidas tööprotsessid toimivad, st milliseid andmeid kus ja milliste IT-süsteemidega töödeldakse.

Rakenduste jaoks kindlaksmääratud turbevajadus kandub üle IT-süsteemidele, kus neid rakendusi käitatakse. Ruumide turbevajaduse hindamisel tuleb lähtuda ruumis paiknevate IT-süsteemide ja nendes töötavate rakenduste turbevajadusest.

Näide. Igapäevaste tööülesannete täitmiseks on hädavajalik, et kliendiandmete haldamine toimiks laitmatult. Seda tööprotsessi käitatakse serveris xy, millel on suur turbevajadus. Seetõttu on ruum, milles server töötab, samuti suure turbevajadusega.

3. Täiendav turbeanalüüs

IT-etalonturbe metoodika rakendamine võimaldab saavutada turbeastme, mis vastab tavalisele turbevajadusele. Kui teatud valdkonna (nt mõne rakenduse või IT-süsteemi) turbevajadus on tavapärasest suurem või kui puututakse kokku valdkonnaga, mille jaoks ei ole meetmeid veel välja töötatud, tuleks pärast IT-etalonturbe evitamist teha täiendav turbeanalüüs.

BSI on välja töötanud IT-etalonturbe rakendamisel põhineva riskianalüüsi metoodika. Seda kirjeldatakse standardis BSI 1003 . Riskianalüüsiks võib samas rakendada ka klassikalist kvantitatiivset metoodikat. Kui analüüsitav valdkond on väike, on ka täiendava riskianalüüsi töö- ja ajakulu üpris väike. Näiteks kui vajadused on seotud ainult mõne konkreetse IT-süsteemiga, mille kohta ühtki IT-etalonturbe moodulit pole veel koostatud, võib riskide hindamiseks ja asjakohaste turbemeetmete valimiseks piisata ka sellest, kui konsulteerida sel teemal kas seadme tootja või sõltumatute turbeekspertidega.

Tavapärasest suurema turbevajadusega valdkondade puhul on kindlasti palju rohkem kasu standardsete turbemeetmete võtmisest ja täiendavast riskianalüüsist kui puhtkvantitatiivsest riskianalüüsist. Seejärel tuleb uued tuvastatud meetmed kaasata üldisesse turbeprotsessi ja need ülejäänud meetmetega kooskõlla viia.

### 9.2.2 Turbekontseptsiooni koostamine

IT-etalonturbe kataloogid sisaldavad tüüpseid mooduleid, ohte ja meetmeid. Moodulites kirjeldatakse infoturbehalduse tüüpilisi ülesandeid ning IT-süsteemide kasutamisega seotud levinud ohte ja nende vastu võetavaid standardseid turbemeetmeid. Lisaks pööratakse tähelepanu infoturbe töökorraldust, personali ning taristuid ja tehnikat puudutavatele aspektidele.

IT-etalonturbe kataloogide moodulid käsitlevad järgmisi valdkondi:

- üldkomponendid (nt töökorraldus, personal, hädaolukorraks valmistumine);
- infrastruktuuri (nt hoone ja arvutuskeskuse) turve;
- IT-süsteemide (nt serverite, klientsüsteemide, võrgukomponentide) turve;
- võrguturve (võrkude ja süsteemide haldus);
- rakenduste (nt meiliteenuse) turve.

Pärast struktuuri analüüsimist saab nende moodulitele toetudes alustada töökorralduse modelleerimisega. Selle käigus seostatakse vaadeldava kehtivusala valdkonnad IT-etalonturbe moodulitega (infokooslusega). Modelleerimise tulemusel valmib soovituslike meetmete kogu, mille saab võtta turbekontseptsiooni koostamise aluseks.

IT-etalonturbe kataloogides käsitletud meetmed sisaldavad ühelt poolt konkreetseid soovitusi standardites ISO 27001 ja ISO 27002 loetletud meetmete juurutamiseks, kuid teisalt ka palju tehnilisi nõuandeid, kuidas enim levinud IT-süsteeme ja rakendusi turvaliselt käitada. Vajalike ja oluliste turbeaspektide valikul aitab teid täpne moodulite valimise juhend (etalonturbel põhinev modelleerimine). Selle abil saab ametiasutus või ettevõte endale eesmärgiks seatud turbeastme saavutada kas väliste ekspertide abita või vähemalt kergema vaevaga.