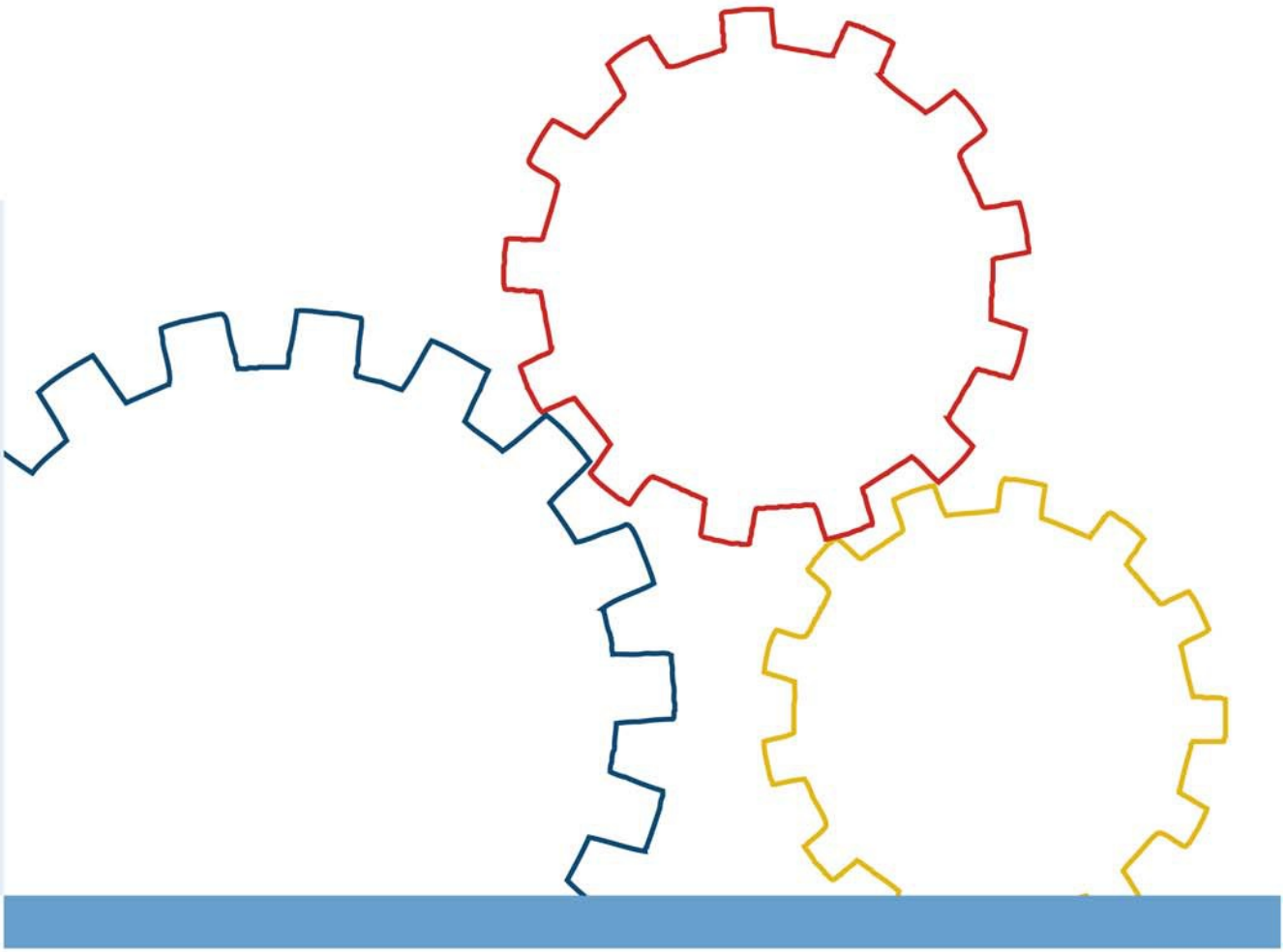
Bundesamt
für Sicherheit in der
Informationstechnik

Standard BSI 100-3

IT-etalonturbel põhinev riskianalüüs



www.bsi.bund.de/gshb

Versioon 2.5

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

Sisukord

1 Sissejuhatus

1.1 Versioonide ajalugu

Seis	Versioon	Muudatused
Veebruar 2004	1.0	
Detsember 2005	2.0	Kohandatud standardi BSI 100-2 nõuetega.
Mai 2008	2.5	Keskendub rohkem infoturbele võrreldes varasema IT-turbega, mistõttu on mõisteid kohandatud. Kohandatud standardi BSI 100-2 uue struktuuri ja liigendusega. Et vältida äravahetamist IT-etalonturbe kataloogide Z-meetmetega, kasutatakse termini „lisameetmed" asemel läbivalt termineid „täiendavad meetmed" ja „täiendavad turbemeetmed". Väliste objektide ohukirjeldused esitatakse peatükis 4. Ohtude OK-seisundi ühtlustatud käsitlus. Lisatud alapeatükk 6.2 „Riskide jälgimine".

1.2 Eesmärk

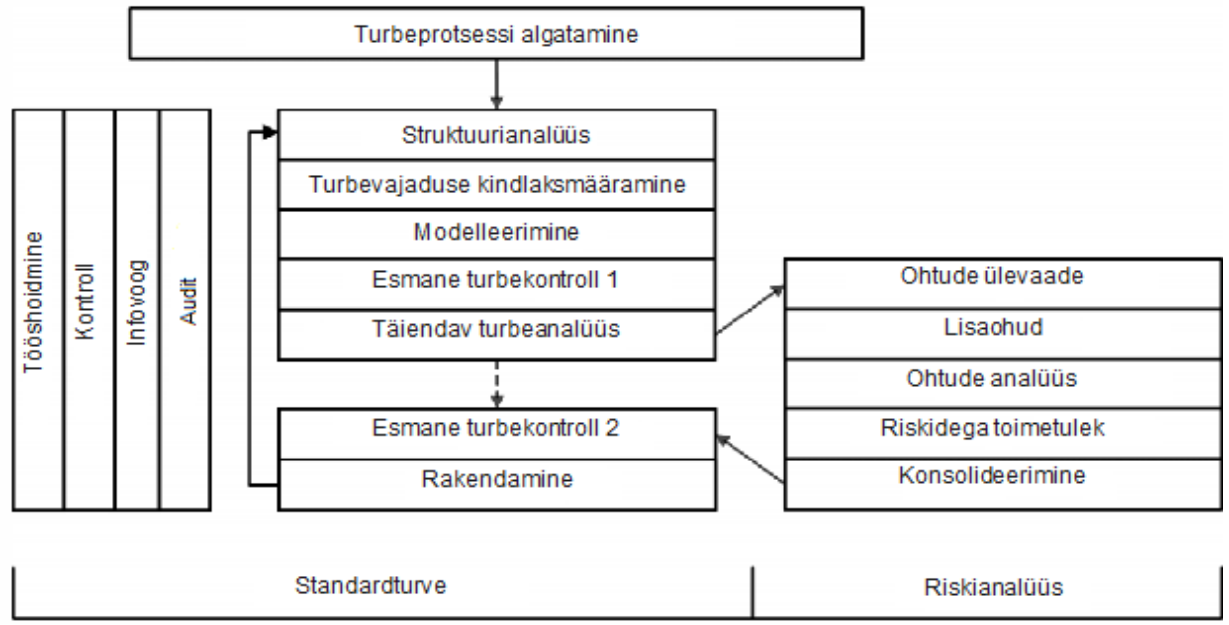
Järgnevalt kirjeldatakse infotöötluse valdkonna jaoks IT-etalonturbe kataloogides loetletud ohtudel põhinevat lihtsustatud riskianalüüsi metoodikat. Sellise analüüsi potentsiaalsed rakendusvaldkonnad on ametiasutuste ja ettevõtete sihtobjektid, mis vastavad järgmistele tingimustele:

- kolmest põhiväärtusest (konfidentsiaalsus, terviklus või käideldavus) on vähemalt ühe turbevajadus kas M või H;
- objektid ei ühildu IT-etalonturbe olemasolevate moodulitega piisavalt (objekte ei õnnestu nende põhjal modelleerida);
- objekte kasutatakse stsenaariumides (keskkondades, rakendustena), mida IT-etalonturve ei käsitle.

Nimetatud juhtudel tekivad järgmised küsimused:

- millistele infotöötlust ähvardavatele ohtudele on IT-etalonturbe asjakohaste turbemeetmete võtmisega reageeritud ebapiisavalt või üldse reageerimata jäetud?
- kas olukord nõuab täiendavate, IT-etalonturbe mudeli piiridest väljuvate turbemeetmete planeerimist ja võtmist?

Käesolevas dokumendis kirjeldatakse metoodikat, millega saab teatud liiki sihtobjektide jaoks võimalikult lihtsalt kindlaks määrata, kas ja millisel määral on infotöötlusega seotud ohtude maandamiseks tarvis võtta meetmeid, mis väljuvad IT-etalonturbe piiridest.



Joonis 1. Riskianalüüsi integreerimine turbeprotsessiga

ISKE rakendusjuhendis ning mõnes riski- ja turbeanalüüsi metoodikas puudutatakse riskikäsitlusega seotud otsuste lihtsustamiseks muu hulgas ka kahjujuhtumite esinemise tõenäosust. Kogemused on siiski näidanud, et tõenäosuse hindamine osutub praktikas sageli liiga keeruliseks, sest puuduvad põhimõtted, mille alusel võiks jõuda usaldusväärsete tulemusteni. Samuti võib paljudel juhtudel kahelda esinemistõenäosuse interpreteerimises. Seetõttu ei keskendu siin kirjeldatav metoodika otseselt ohtude esinemise tõenäosusele, vaid käsitleb seda kaudselt, pöörates tähelepanu riskide väljaselgitamisele ja nende raskuse hindamisele.

1.3 Sihtrühm

See dokument on suunatud töötajatele, kes vastutavad infoturbe tagamise eest, samuti turbeekspertidele ja -nõustajatele ning kõikidele teistele huvilistele, kes puutuvad kokku infoturbe haldamise või infotöötluse riskianalüüsiga.

Selles dokumendis kirjeldatud metoodika rakendajad peaksid tundma standardis BSI 100-2 kajastuvat IT-etalonturbe metoodikat.

1.4 Kasutussuunised

Selles dokumendis kirjeldatakse riskianalüüsi metoodikat, mille eesmärk on täiendada juba olemasolevat IT-etalonturbel põhinevat turbekontseptsiooni. Metoodika kasutab abivahendina IT-etalonturbe kataloogides esitatud ohtude kirjeldusi.

Peatükkides 2–8 kirjeldatud metoodikat on soovitatav rakendada järjest, samm sammu haaval.

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

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

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

2 Eeltööd

Enne riskianalüüsiga alustamist peavad olema tehtud IT-etalonturbe metoodikal põhinevas standardis BSI 100-2 loetletud järgmised eeltööd.

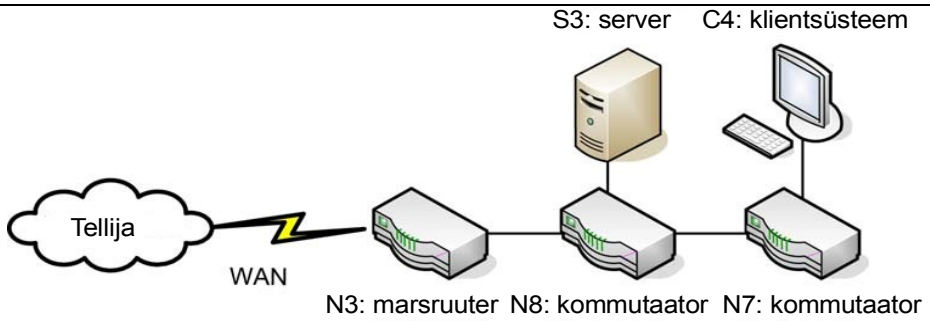
- Süstemaatilise infoturbeprotsessi algatamine. See on vajalik selleks, et kõik infoturbega seotud tegevused toimuksid organiseeritult. Näiteks tuleb kindlaks määrata töötajate rollid ja tööülesanded. Lisainfot infoturbeprotsessi algatamise kohta leiate IT-etalonturbe metoodika peatükist 3.
- IT-etalonturbe metoodika peatükist 4.1 lähtuv turbekontseptsiooni kehtivusala defineerimine. Kehtivusala nimetatakse edaspidi infokoosluseks.
- IT-etalonturbe metoodika peatükist 4.2 lähtuv infokoosluse struktuurianalüüs. Sellega selgitatakse välja infokoosluse olulisimad andmed, nt võrguplaan, loetelu infokoosluse tähtsaimatest rakendustest ning nende ja IT-süsteemide sõltuvusseostest.
- Lisaks peab IT-etalonturbe metoodika peatüki 4.3 põhjal olema kindlaks määratud infokoosluse turbevajadus. Selle tulemusel peab olema teada, milline on rakenduste, IT-süsteemide ja kasutatavate ruumide kaitsevajadus, ning koostatud kriitiliste sideühenduste loetelu. Turbevajadus põhineb kolme põhiväärtuse, st konfidentsiaalsuse, tervikluse ja käideldavuse hindamisel ning see võib olla kas L, Mvõi H.
- IT-etalonturbe metoodika peatüki 4.4 ja IT-etalonturbe kataloogide peatüki 2 põhjal peab olema tehtud modelleerimine. Sellega määratakse iga IT-etalonturbe kataloogide mooduli jaoks kindlaks, milliste infokoosluse sihtobjektide peal tuleb neid rakendada. Erinevates moodulites loetletud standardsed turbemeetmed moodustavad infokoosluse jaoks IT-etalonturbe kontseptsiooni aluse.
- Enne riskianalüüsi tegemist peab IT-etalonturbe metoodika peatüki 4.5 põhjal olema tehtud esmane turbekontroll. Sellega tuvastatakse, millised turbemeetmed on vaadeldavas infokoosluses juba võetud ja milliseid tuleks veel võtta.
- IT-etalonturbe metoodika peatüki 4.6 põhjal peab olema tehtud ka täiendav turbeanalüüs. Täiendava turbeanalüüsi käigus otsustatakse, milliste sihtobjektide puhul on riskianalüüs kindlasti vajalik ja milliste puhul võib riskianalüüsist loobuda.

Sihtobjekte, mille puhul täiendava turbeanalüüsi raames otsustati, et nende jaoks tuleb kindlasti teha riskianalüüs, tähistatakse edaspidi terminitega „vaadeldavad sihtobjektid” või „vaadeldavad komponendid”.

Näide

Tarneettevõttel on otsene sideühendus ühe oma suurima tellijaga. Sideühenduse kaudu edastab tellija tarnijale pidevalt uusi tellimusi, mis kajastavad toodete värvi, suurust ja sortimenti. Andmevoogude minimeerimiseks edastab tellija tarnijale ainult muudatused, st info, mille poolest uus tellimus eelmisest erineb. Tarnija kasutab tellijalt saadud infot oma tootmistegevuse planeerimiseks. Nii suudab tarnija tellijale tagada, et vajalikku värvi ja ettenähtud suurusega tooted jõuavad tellijani õiges koguses ja soovitud tähtajaks.

Sideühenduse tehnilise lahendusena kasutatakse renditud püsiühendust. Sideühenduse kas või kahetunnine katkestus tooks tootmisettevõttele kaasa juba märkimisväärse ületootmise või suutmatuse tarnida soovitud kaupa nõutud ajaks ja vajalikus koguses ning tekitaks seega suuri lisakulutusi. Seetõttu võib väita, et infokoosluse järgmises alamvaldkonnas on käideldavuse turbevajadus suur.



Joonis 2. Suure turbevajadusega alamvaldkonna väljavõte võrguplaanist

Asjaomased komponendid asuvad ruumides M.723 (serveriruum) ja M.811. Täiendava turbeanalüüsi käigus otsustati, et kõikide teiste suure turbevajadusega komponentide puhul ei ole riskianalüüs vajalik.

3 Ohuülevaate koostamine

Vaadeldavate sihtobjektide riskianalüüsi lähtepunktina saab kasutada IT-etalonturbe kataloogides loetletud ohte. Ohte, puudusi ja riske ei käsitleta siinkohal mitte eraldi, nagu IT-turbe käsiraamatus, vaid tervikuna.

Järgmiste tööetappide eesmärk on koostada infokoosluse sihtobjektidele mõjuvate ohtude ülevaade. Selleks tuleks kõigepealt luua ülevaade, milliseid infokoosluse komponente vaadeldakse ja milliseid mitte.

1. Infokoosluse modelleerimise raames koostatud ülevaatest tuleks esmalt välja jätta kõik sellised sihtobjektid või nende rühmad, mille kohta võeti täiendava turbeanalüüsi raames vastu otsus, et riskianalüüs ei ole vajalik. See tähendab, et modelleerimise tulemusest tuleb välja jätta kõik mittevaadeldavad sihtobjektid.

Näide (väljavõte)

Nr	**Mooduli pealkiri**	**Sihtobjekt**	
B 2.3	Bürooruum	~~Ruum M.501~~	Välja jätta
B 2.4	Serveriruum	Ruum M.723	
B 2.6	Tehnilise taristu ruum	Ruum M.811	
B 3.101	Server	~~S2~~	Välja jätta
B 3.101	Server	S3	
B 3.102	Unixi server	~~S2~~	Välja jätta
B 3.102	Unixi server	S3	
B 3.201	Klient	~~C2~~	Välja jätta
B 3.201	Klient	C4	
B 3.301	Turvalüüs (tulemüür)	N3	

2. Seejärel eemaldatakse allesjäänud tabelist kõik sellised moodulid, mille kohta ei ole alles enam ühtki sihtobjekti. Need moodulid ei ole vaadeldavate sihtobjektide jaoks olulised.

Enamasti saab välja jätta ainult 2. ja 5. kihi mooduleid, sest 1. kihi moodulid puudutavad kui mitte kõiki, siis kindlasti vähemalt paljusid sihtobjekte. Mõningatel juhtudel saab siiski välja jätta ka 1. kihi mooduleid, nt kui on ilmselge, et mooduli teema on konkreetse riskianalüüsi tegemiseks ebaoluline.

Näited

- Moodulid B 1.3 „Hädaolukorraks valmisoleku kontseptsioon” ja B 1.8 „Turvaintsidentide käsitlus” võib sageli välja jätta juhtudel, kus riskianalüüs hõlmab ainult selliseid valdkondi, mille käideldavuse turbevajadus on tavaline.
- Mooduli B 1.7 „Krüptokontseptsioon” võib sageli välja jätta juhtudel, kus riskianalüüs hõlmab ainult selliseid valdkondi, mille konfidentsiaalsuse ja käideldavuse turbevajadus on L.

Nende sammude tulemusel peab tekkima tabel, milles on loetletud ainult vaadeldavate sihtobjektide jaoks olulised moodulid. 1. kihi moodulid on olulised kõikide või paljude sihtobjektide jaoks, seevastu ülejäänud nelja kihi moodulid puudutavad ainult üksikuid sihtobjekte või nende rühmi.

Näide (väljavõte)

Nr	Mooduli pealkiri	Sihtobjekt
B 2.4	Serveriruum	Ruum M.723
B 2.6	Tehnilise taristu ruum	Ruum M.811
B 3.101	Server	S3
B 3.102	Unixi server	S3

B 3.201	Klient	C4
B 3.301	Turvalüüs (tulemüür)	N3

3. Igas IT-etalonturbe kataloogide moodulis on viited ohtude loeteludele. Iga tabelis oleva sihtobjekti puhul tuleb moodulitest välja otsida ohtude numbrid ja pealkirjad. Siinkohal on sageli mõistlik kajastada 1. kihi moodulite ohte teistest eraldi, nt koondada need ühe tervikliku sihtobjekti alla, mida võib nimetada terviklikuks infokoosluseks.
4. Selle tulemusel valmib tabel, kus on loetletud nii sihtobjektid kui ka nende peamised ohud. Tabeli põhjal tulevad välja ohud, mida on iga sihtobjekti puhul loetletud vähemalt kaks korda.
5. Seejärel tuleks iga sihtobjekti ohud teemade kaupa liigitada. Mõned IT-etalonturbe kataloogide ohud käsitlevad sarnaseid turbeprobleeme või sama ohu erinevaid variante (nt G 1.2 „IT-süsteemi avarii" ja G 4.31 „Võrgukomponendi avarii või tõrge").
6. Edasise analüüsi lihtsustamiseks tuleks tabelis iga sihtobjekti juurde märkida ka turbevajaduse kindlaksmääramise tulemused, st konfidentsiaalsust, terviklust ja käideldavust kajastav turbevajadus. Üldise sihtobjekti puhul, mis käsitleb infokooslust tervikuna, võib turbevajaduse märkimisest loobuda.

Valmiv tabel kujutab endast vaadeldavate sihtobjektide ohuülevaadet. Selle tabeli põhjal saab välja selgitada lisaohte.

Näide (väljavõte)

Kommunikatsiooniserver S3
Konfidentsiaalsus: L Terviklus: M Käideldavus: M
G 1.2 IT-süsteemi rike G 3.2 Seadme või andmete hävitamine hooletuse tõttu G 4.1 Toitevõrgu katkestus G 5.57 Võrguanalüüsi utiliidid G 5.85 Tundliku informatsiooni tervikluse kadu jne

Ruum M.811
Konfidentsiaalsus: L Terviklus: L Käideldavus: M
G 1.4 Tulekahju G 1.5 Vesi G 2.6 Volitamatu sisenemine kaitstavatesse ruumidesse G 5.3 Volitamatu sisenemine hoonesse

Ruum M.811
G 5.5 Vandalism
jne

4 Lisaohtude tuvastamine

Vaadeldavate sihtobjektide puhul võib esineda ka lisaohte, mida IT-etalonturbe mudelis loetletud ohtude hulgas ei ole. Nendega tuleb samuti arvestada. IT-etalonturbe kataloogides ei kajastu tavaliselt järgmised ohud:

- spetsiaalse tehnoloogia, toote või väga eriliste rakendusjuhtudega kaasnevad ohud;
- tavakasutuse korral vaid väga erilistel tingimustel kahjudega lõppeda võivad ohud;
- kurjategija väga häid eriteadmisi, juhuste kokkulangemist ja vahendeid eeldavad ohud.

Näiteks kuuluvad selliste ohtude hulka kogu asutuse või tootmishoone tööprotsesside seiskamine relva ähvardusel või tehniliselt keerukas rünne, milleks kasutatakse organisatsioonis töötava administraatori kaasabi.

Infoturbe lähtepunktist on olulised järgmised ohud:

- märkimisväärsete kahjudega lõppevad ohud;
- vaadeldava kasutusjuhu ja -keskkonna jaoks reaalsed ohud.

Oluliste lisaohtude tuvastamisel tuleks arvestada analüüsitava sihtobjekti turbevajaduse ehk infoturbe kolme põhiväärtusega: konfidentsiaalsuse, tervikluse ja käideldavusega.

1. Kui sihtobjekti kas või ühe põhiväärtuse turbevajadus on H, tuleks eelisjärjekorras tuvastada just seda valdkonda puudutavad ohud. Selle turbevajaduse kategooria korral tuleb lähtuda sellest, et oluliste ohtude hulgas on ka selliseid, mis väljuvad IT-etalonturbe kataloogide piiridest.
2. Eelisjärjekorras tuleks tuvastada ka need ohud, mille puhul on sihtobjekti kas või ühe põhiväärtuse turbevajadus M. Ka selle turbevajaduse kategooria korral võib leiduda olulisi ohte, mida IT-etalonturbe kataloogides ei käsitleta.
3. Kui sihtobjekti kas või ühe põhiväärtuse turbevajadus on L, piisab asjakohase turbe tagamiseks enamasti IT-etalonturbe kataloogides toodud ohtude käsitlemisest ja nende jaoks soovitatud vastumeetmete võtmisest.

Olenemata sellest, milline vaadeldavate sihtobjektide turbevajadus ka poleks, on lisaohtude väljaselgitamine kindlasti väga oluline siis, kui IT-etalonturbe kataloogides ei leidu sihtobjekti piisavalt hästi kajastavat moodulit või kui sihtobjekti kasutusvaldkond (kasutuskeskkond, rakendus) ei kuulu IT-etalonturbe kataloogide käsitlusalasse.

Lisaohtude väljaselgitamisel tuleks arvestada järgmiste küsimustega.

- Millised vääramatu jõu kategooriasse kuuluvad ohud ähvardavad infokooslust kõige enam?
- Milliseid organisatoorseid ehk töökorralduslikke vigu tuleb infoturbe tagamiseks kindlasti vältida?
- Mis liiki inimvead ähvardavad info ja rakenduste turvet kõige enam?
- Milliseid spetsiaalseid turbeprobleeme võivad vaadeldava sihtobjekti puhul esile kutsuda tehnilised rikked?
- Millised eriohud võivad kaasneda institutsioonivälistе ründajatega? Nende all mõeldakse isikuid, kes ei ole institutsiooni liikmed ning kellel pole erikokkuleppeid, mis võimaldaksid neil ligi pääseda institutsiooni siseressurssidele.
- Mil moel võivad institutsiooni enda töötajad ettekavatsetud rünnetega pärssida sihtobjekti nõuetekohast ja turvalist käitamist? Töötajate juurdepääsuvõimalused ja volitused ning siseinfo valdamine võib kätkeda ohte.
- Kas leidub eriohte, mida võivad põhjustada vaadeldavast infokooslusest välja jäävad objektid? Sellised välised objektid võivad olla nt võõrad rakendused ja IT-süsteemid või ehitustehnilised eripärad. Vaadeldava infokoosluse defineerimise eesmärk on piiritleda turbekontseptsiooni uurimisobjekt. Samas ei tohi piiritlemisega minna ka nii kaugele, et riskianalüüsist jäetakse välja kõik infokooslust väljastpoolt ähvardavad ohud.

Vaadeldava sihtobjekti jaoks on esmatähtis välja selgitada, kas selle puhul on tarvis arvestada lisaohtudega või mitte. Eriohtude allikad võivad olla nt järgmised:

- tootjafirma dokumentatsioon;
- internetis turvaaukude kohta avaldatud info;
- enda ohuanalüüsid.

Lisaohtude väljaselgitamisel võib olla kasu ka IT-etalonturbe ohukataloogidest G 1 kuni G 5. Nendest ohukataloogidest võite leida ohte, mida pole seni arvestatud põhjusel, et modelleerimise käigus ei võetud vastavaid mooduleid arvesse.

Praktika on näidanud, et tuvastatud lisaohud puudutavad enamasti korraga mitut sihtobjekti. Tuvastatud lisaohud tuleb märkida ohuülevaatesse.

Oluline! Kui oluliste ohtudega ei arvestata, võib tagajärjeks olla vigane turbekontseptsioon. Seetõttu tuleks kahtluste korral põhjalikult analüüsida, kas kõikide oluliste ohtudega on piisavalt arvestatud. Siinkohal on sageli mõttekas kasutada väliste ekspertide abi.

Lisaohtude väljaselgitamiseks on seni praktikas olnud palju kasu siis, kui kõik osalised korraldavad ühise ajurünnaku. Protsessi tuleks kaasata vaadeldava sihtobjekti jaoks olulised infoturbespetsialistid, projektijuhid, administraatorid ja kasutajad. Kõikidele osalejatele tuleb kätte jagada selgelt sõnastatud ülesanded ning ajurünnaku kestust tuleks piirata. Kogemused on näidanud, et selline tegevus võiks kesta maksimaalselt kaks tundi. Ajurünnakut peaks juhtima üks infoturbespetsialist.

Näide (väljavõte)

Ettevõte korraldas ajurünnaku, mille käigus tuvastati muu hulgas järgmised lisaohud.

Infokooslus tervikuna	
G 2.B1	Töö- ja varundussüsteemide ebapiisav sünkroniseerimine
	Kuna tööandjaga suhtlemiseks kasutatava sidesüsteemi käideldavusnõuded on ranged, on kõiki komponente topelt. Kui varundussüsteemi komponendid ei kajasta alati kõige värskemat infot, on oht, et tööandjaga ei õnnestu luua toimivat sideühendust.
G 5.70	Pereliikmete või külaliste manipulatsioonid kodutöökohas
	See oht on IT-etalonturbe kataloogides olemas ja seda kirjeldab moodul B 2.8 „Kodutöökoht". Seevastu vaadeldava infokoosluse modelleerimisel selle mooduliga ei arvestatud. Ohuga G 5.70 tuleb siiski arvestada, sest ettevõtte ruumides tehakse külalistele pidevalt ekskursioone. Seetõttu tuleb lisaohuna käsitleda ka ohtu G 5.70.
jne	

Kommutaator N7	
Konfidentsiaalsus:	L
Terviklus:	L
Käideldavus:	M
G 2.B2 Tootmisüksuse infotehnoloogia kahjustamine	
	Klientsüsteemi C4 ja kommutaatorit N7 käitatakse ettevõtte tootmisruumides, mistõttu ähvardavad neid füüsikalised eriohud. Neid seadmeid ähvardavad kahjustamine, hävimine ja kasutusea lühenemine.
jne	

Klientsüsteem C4	
Konfidentsiaalsus: L Terviklus: M Käideldavus: M	
G 2.B2	Tootmisüksuse infotehnoloogia kahjustamine
	Vt „Kommutaator N7”.
G 4.B1	Tootmis- ja kommunikatsioonitarkvara ühilduvusprobleemid
	Klientsüsteemi C4 ei kasutata mitte üksnes tööandjaga suhtlemiseks, vaid selles käitatakse ka teisi tootmisprotsessi jaoks vajalikke programme. Nende programmide vaheliste ühilduvusprobleemide tagajärjel võib arvuti kokku joosta ja see tähendaks käideldavuse kadu.
jne	

5 Ohuanalüüs

Järgmise sammuna töötatakse ohuülevaade süstemaatiliselt läbi ning kontrollitakse iga sihtobjekti ja ohu puhul seda, kas vastumeetmeid on juba võetud või kas turbekontseptsioonis nende ohtude vältimiseks ette nähtud meetmed suudavad tagada piisava turbe. Meetmete puhul on enamasti tegu IT-etalonturbe kataloogide standardsete turbemeetmetega. Kontrollimiseks kasutatakse turbekontseptsiooni ja järgmisi kriteeriume.

- Terviklik käsitlus
  Kas standardsed turbemeetmed pakuvad kõikide analüüsitava ohu aspektide vastu piisavalt head kaitset? (Näide: kas hoone turvalisuse puhul on arvestatud ka tagauste ja hädaväljapääsudega?)
- Mehhanismide tugevus
  Kas standardsetes turbemeetmetes soovitatud turbemehhanismid on vaadeldavate ohtude vastu piisavalt tõhusad? (Näide: kas paroolidele kehtestatud miinimumpikkus on piisav?)
- Usaldusväärsus
  Kas ette nähtud turbemehhanismidest on võimalik lihtsalt mööda hiilida? (Näide: kui kergesti on töötajatel võimalik volitamatult serveriruumi pääseda, et seejärel enda pääsuõigusi muuta?)

Kontrolli tulemus märgitakse ohuülevaates iga ohu juurde eraldi tulpa „OK", kasutades märget (J või E).

„OK = J" tähendab, et meetmed on juba võetud, turbekontseptsioonis ette nähtud meetmed suudavad pakkuda ohtude eest piisavat turvet või vaadeldav oht on praeguse riskianalüüsi jaoks niikuinii ebaoluline (nt põhjusel, et võib-olla tuleb keskenduda mõnele teisele turbe põhiväärtusele).

„OK = E" tähendab, et seni võetud või vähemalt turbekontseptsioonis ette nähtud turbemeetmed ei paku vaadeldava ohu vastu piisavat kaitset.

Teadmiseks: esimesed mõtted, milliseid meetmeid tuleks ohtude vastu võtta, tekivad sageli juba ohtude analüüsimise käigus. Kuna tegu võib olla järgmiste tööetappide jaoks väga kasulike mõtetega, tuleks need kirja panna.

Ohuanalüüsi tulemusel valmib ülevaade sellest, milliste vaadeldavate sihtobjektide puhul piisab turbe tagamiseks IT-etalonturbe kataloogide meetmetest (OK = J) ning milliste sihtobjektide puhul esineb veel jääkohte (OK = E). Tuvastatud riskide käsitlemist kajastab järgmine peatükk.

Näide (väljavõte)

Tarneettevõte tegi täiendava ohuülevaate põhjal ohuanalüüsi. Selle tulemusel selgus, et järgmiste ohtude puhul IT-etalonturbe kataloogide meetmetest ei piisa (OK = E).

Kommunikatsiooniserver S3	
Konfidentsiaalsus: L Terviklus: M Käideldavus: M	
G 1.2 IT-süsteemi rike	OK = E
Serveri S3 riket tuleb võimalikult hästi ennetada. IT-etalonturbe kataloogide meetmetest selleks ei piisa.	
G 5.85 Tundliku informatsiooni tervikluse kadu	OK = E
Tellimuse esitajalt laekuvate andmete võltsimine peab olema välistatud. Muidu võib tagajärjeks olla märkimisväärne ületootmine või probleemid tarnetähtaegadest kinnipidamisel, mis tekitavad ettevõttele suurt kahju.	
jne	

Klientsüsteem C4	
Konfidentsiaalsus: L Terviklus: M Käideldavus: M	
G 1.2 IT-süsteemi rike	OK = E
Tellijaga suhtlemiseks kasutatakse klientsüsteemis C4 spetsiaalset tarkvara, mille installimine on väga keeruline ja ajamahukas.	
G 2.B2 Tootmisüksuse infotehnoloogia kahjustamine	OK = E
Tootmismasinate infotöötluse turvet käsitletakse IT-etalonturbe kataloogides väga põgusalt.	
jne	

6 Riskikäsitlus

6.1 Riskikäsitluse alternatiivid

Ohuanalüüsi käigus leitakse sageli ka selliseid ohte, mille vastu võitlemisel võivad IT-etalonturbe kataloogide meetmed osutuda ebapiisavaks. Sellised jääkohud võivad ohustada infokoosluse tööd.

Seepärast tuleb otsustada, mida jääkohtudega ette võtta. Selle otsuse langetamises peab kindlasti osalema ka juhtkond, sest tagajärjeks võivad olla märkimisväärsed riskid või lisakulud. Kõikide täiendatud ohuülevaates kajastuvate ohtude jaoks, mille puhul on kasutatud märgendit „OK = E", on olemas järgmised alternatiivid.

A. *Riski vähendamine täiendavate turbemeetmetega*: jääkoht kõrvaldatakse ühe või mitme ohule vastava täiendava turbemeetme väljatöötamise ja võtmisega. Täiendavate turbemeetmete infoallikad võivad olla nt järgmised:
   - tootja dokumentatsioon ja teenindusettevõte, kui asjaomase sihtobjekti puhul on tegemist tootega;
   - standardid ja end tõestanud meetodid, nt sellised, mida töötavad välja infoturbe valdkonna komiteed;
   - muu info ja teenused, nt internetis avaldatud info ja spetsialiseerunud ettevõtete teenused;
   - oma institutsiooni või koostööpartnerite kogemused.

B. *Riski vältimine struktuuride ümberkorraldamisega*: jääkoht kõrvaldatakse tööprotsessi või infokoosluse struktuuri ümberkorraldamisega. Sellise tegutsemisviisi kasuks otsustamise põhjused võivad olla nt järgmised:
   - kõik tõhusad vastumeetmed on liiga kulukad, kuid jääkohuga ei saa siiski leppida;
   - struktuuride ümberkorraldamine on nii või teisiti vajalik, nt kulude vähendamiseks;
   - kõik tõhusad vastumeetmed piiraksid olulisel määral süsteemi funktsionaalsust või kasutusmugavust.

C. *Riskiga leppimine*: institutsioon lepib jääkohu ja sellest tuleneva riskiga. Sellise tegutsemisviisi kasuks otsustamise põhjused võivad olla nt järgmised:
   - oht võib põhjustada kahju ainult väga spetsiifiliste asjaolude kokkulangemisel;
   - tõhusad vastumeetmed ohu vältimiseks puuduvad ja ohu täielik vältimine on praktikas peaaegu võimatu;
   - tõhusate vastumeetmete kulud on suuremad kui kaitstava objekti väärtus.

D. *Riski ülekandmine*: allesjäänud ohust tulenev risk jäetakse mõne teise institutsiooni kanda, nt sõlmitakse kindlustusleping või kasutatakse väljasttellimist. Sellise tegutsemisviisi kasuks otsustamise põhjused võivad olla nt järgmised:
   - võimalikud ohud on puhtfinantsilised;
   - juba teistel põhjustel on nagunii tehtud plaane osa tööprotsesse institutsioonist välja suunata;
   - lepinguline partner suudab majanduslikel või tehnoloogilistel põhjustel riskiga palju paremini toime tulla.

Neljast riskikäsitluse alternatiivist kõige sobivama valimiseks tuleks korraldada ajurünnak, et selgitada välja, millised täiendavad turbemeetmed (alternatiiv A) oleksid mõeldavad. Seejuures tuleks kasutada eelmainitud infoallikaid.

Lisainfo

Riskianalüüsi raames saab täiendavate turbemeetmete pidepunktidena kasutada ka IT-etalonturbe meetmeid, mis on kataloogides märgendiga Z (täiendav). Nende puhul on tegu praktikas väga sageli

kasutatud näidetega, mida IT-etalonturve ei hõlma. Siiski tuleb arvestada, et märgendiga Z (täiendav) tähistatud IT-etalonturbe meetmed ei muutu isegi rangete turbenõuete korral automaatselt kohustuslikuks. Lisaks ei pea nendega riskianalüüsi raames otseselt arvestama.

Mõnikord on nende meetmete abil võimalik leida mõne ohu jaoks turbemeetmeid, kuid ka sel juhul kajastavad need ainult ohu üksikuid aspekte, mitte ohtu tervikuna. Siinkohal tekib aga küsimus, kuidas ohuga edasi toimida (kas valida alternatiiv A või C/D). Sellisel juhul tuleks vastav oht jagada kaheks ja rakendada kummalegi eraldi alternatiivi A või C/D.

Tuleks arvestada ka sellega, millised turbemehhanismid on vastava sihtobjekti jaoks juba kasutusele võetud. Seejuures võib kasutada esmase turbekontrolli tulemusi (vt IT-etalonturbe metoodika peatükki 4.5).

Otsuseid aitab paremini langetada teadmine, kui suur on vajalike turbemeetmete hüpoteetiline töökoormus ja kulu, ning olemasolevaid turbemehhanisme puudutav teave.

- Alternatiivi A puhul lisatakse täiendavad turbemeetmed turbekontseptsiooni. Piisab selgest viitest meetme detailsele kirjeldusele.
- Alternatiivi B puhul tuleb tavaliselt infokoosluse vastavate osade jaoks uuesti käivitada turbeprotsess. See algab tavaliselt struktuurianalüüsiga. Loomulikult saab seejuures kasutada juba olemasolevat infot ja dokumentatsiooni.
- Alternatiivi C puhul tuleb ilmtingimata võimalikult täpselt välja selgitada, millised võivad olla riski tagajärjed. Otsuse langetab juhtkond ning see tuleb arusaadavalt dokumenteerida.
- Alternatiivi D puhul on kõige olulisem koostada korralik leping. Eriti just väljasttellimisel tuleks siinkohal kindlasti kasutada põhjalike juriidiliste teadmistega isiku abi. Otsuse langetab juhtkond ning see tuleb arusaadavalt dokumenteerida.

Oluline! See, kuidas tullakse toime ohtudega, mille vastu pole IT-etalonturbe kataloogides piisavalt tõhusaid meetmeid, võib märkimisväärselt mõjutada vaadeldava infokoosluse koondriski. Seetõttu tuleks siinkohal kaaluda välise nõustamisteenuse kasutamist.

6.2 Riskide jälgimine

Riskianalüüsi käigus võidakse tuvastada ohte, millega kaasnevad riskid võivad praegu tunduda vastuvõetavad, kuid mis tulevikus võivad märkimisväärselt suureneda. See tähendab, et teatud aja möödudes võib tekkida vajadus võtta vastumeetmeid. Sellisel juhul on mõistlik täiendavad turbemeetmed juba ennetavalt välja töötada ja ette valmistada, et neid saaks võtta kohe, kui riskid muutuvad vastuvõetamatuks. Sellised täiendavad turbemeetmed tuleb eraldi dokumenteerida ja tähistada. Riskianalüüsi dokumentatsioonis märgendatakse vastavad ohud esmalt tähega C ja nendest tulenevaid riske hakatakse jälgima. Kohe, kui riskid muutuvad liiga suureks, kontrollitakse märgendatud täiendavaid turbemeetmeid ja vajaduse korral värskendatakse neid, seejärel integreeritakse need infoturbekontseptsiooniga. Asjakohaste ohtude käsitlemist kajastav info asendatakse riskianalüüsi dokumentatsioonis kategooriaga „A”. Alternatiivid „B” ja „D” on samuti võimalikud.

Pärast seda, kui ohuülevaates on iga allesjäänud ohu kohta langetatud otsus, mis määrab kindlaks, millist kirjeldatud tegutsemisviisi tuleks kasutada, võib vaadeldava infokoosluse turbekontseptsiooni koostamise lõpule viia.

Näide (väljavõte)

Viiendas peatükis märgendiga „OK = N” tähistatud ohtude kohta langetati järgmised otsused.

Kommunikatsiooniserver S3	
Konfidentsiaalsus:	L
Terviklus:	M
Käideldavus:	M
G 1.2	*IT-süsteemi rike*
„A” M 6.B1	Täiendav turbemeede: *Tervikliku asendussüsteemi käepärast hoidmine tellijaga suhtlemiseks* Tellijaga suhtlemiseks hoitakse käepärast terviklikku asendussüsteemi. See sisaldab kõiki tehnilisi komponente, muu hulgas sideühendusi. Asendussüsteemi hoitakse ruumis E.3. Tagatakse, et asendussüsteemil on alati sama konfiguratsioon nagu tootmissüsteemil ning et asendussüsteem on 30 minutiga kasutusvalmis. Tellijaga suheldakse sissevalimisühenduse kaudu. Kogu terviksüsteemi ja sissevalimisühendust katsetatakse vähemalt kord kvartalis ja iga kord, kui muudetakse konfiguratsiooni.
G 5.85	*Tundliku informatsiooni tervikluse kadu*
„C”	Riskiga leppimine: Edastus- ja infosüsteemidesse paigaldatud turbemehhanismid vähendavad riski ainult pisut, mistõttu on jätkuvalt võimalikud info võltsimisele suunatud ja seega ettevõttele suuri kulusid põhjustavad turvaintsidendid. Juhtkond lepib riskiga ja vastutab selle eest, sest kõik tõhusad vastumeetmed on majanduslikult vastuvõetamatud.
jne	

Klientsüsteem C4	
Konfidentsiaalsus:	L
Terviklus:	M
Käideldavus:	M
G 1.2	*IT-süsteemi rike*
„A”	Täiendav turbemeede:
M 6.B1	*Tervikliku asendussüsteemi käepärast hoidmine tellijaga suhtlemiseks* Teadmiseks: vt „Kommunikatsiooniserver S3”.
G 2.B2	*Tootmisüksuse infotehnoloogia kahjustamine*
„A” M 1.B1	Täiendav turbemeede: *Eriti kõrge turbeastmega tööstusarvuti kasutamine tootmisüksuses* Tootmisüksuse klientsüsteemi C4 suurimad ohud on saastunud õhk, veepritsmed ja vibratsioon. Tavalise arvuti asemel kasutatakse seega tööstusele mõeldud arvutit, mis on füüsikaliste ohtude eest paremini kaitstud. Tööstusarvuti peab vastama järgmistele nõuetele: - sobib paigaldamiseks standardsetesse 19-tollistesse kappidesse; - integreeritud või lahtiklapitav ekraan; - kergesti vahetatav õhufilter; - kaitseklassile IP 54 vastav veepritsmekaitse; - vibratsioonikaitse – vähemalt 0,2 g sagedusel 0–500 Hz.
jne	

7 Turbekontseptsiooni konsolideerimine

Kui jääkohtude käsitlemisel selgub, et standardsete turbemeetmete kõrval on vaja võtta ka täiendavaid turbemeetmeid, tuleb turbekontseptsiooni meetmed konsolideerida. See tähendab, et iga sihtobjekti turbemeetmeid tuleb kontrollida järgmiste kriteeriumide alusel.

Turbemeetmete sobivus ohtude tõrjumiseks

- Kas kõik oluliste ohtude aspektid on täielikult kaetud?
- Kas võetud meetmed ühtivad turbe-eesmärkidega?

Turbemeetmete koosmõju

- Kas meetmed toetavad oluliste ohtude tõrjumisel üksteist?
- Kas meetmete koostoimel moodustub tõhus tervik?
- Kas meetmete vastuolud on välistatud?

Turbemeetmete kasutajasõbralikkus

- Kas võetud meetmed arvestavad käsitsemisel ja käitamisel tehtavate vigadega?
- Kas võetud meetmed on kasutajatele arusaadavad?
- Kas kasutajad märkavad, kui meede pole enam tõhus?
- Kas kasutajatel on meedet võimalik kerge vaevaga eirata?

Turbemeetmete sobivus

- Kas võetud meetmed on ohtude tõrjumiseks sobivad?
- Kas meetmete võtmise kulud ja töövaev on sihtobjektide turbevajadusega sobivas proportsioonis?

Turbekontseptsiooni liigsete osade eemaldamisel ja selle konsolideerimisel tuleb lähtuda järgmistest põhimõtetest.

1. Sobimatud turbemeetmed tuleb kontseptsioonist kõrvaldada ja pärast põhjalikku analüüsi asendada tõhusate meetmetega.
2. Vasturääkivused ja ebakõlad turbemeetmetes tuleb lahendada ning asendada ühtsete ja kooskõlastatud mehhanismidega.
3. Turbemeetmed, millega kasutajad leppida ei taha, on kasutud. Tuleb leida praktiliseks kasutamiseks sobivad lahendused, mis kasutajaid võimalikult vähe nende töödes piiraks või takistaks.
4. Liiga töömahukad või kulukad turbemeetmed tuleb ümber töötada või kõrvale jätta ning asendada sobivate turbemeetmetega. Samal ajal tuleb arvestada, et infoturbe tõhusust ohustavad ka liiga nõrgad meetmed. Ka need tuleb kas ümber muuta või välja vahetada.

Infoturbe tõhustamiseks võib olla mõistlik kasutada peale riskianalüüsi ka teisi meetmeid, nt penetratsioonikatseid. Nende käigus matkitakse institutsioonisisese või -välise ründaja tahtlikku ründekäitumist. Nende tulemuste põhjal võib selguda, et olemasolevat turbekontseptsiooni on tarvis muuta.

Näide (väljavõte)

Tarneettevõtte turbekontseptsiooni konsolideerimisel leiti muu hulgas järgmist.

- IT-etalonturbe kataloogide meetmeid tuleb võtta ka meetmes M 6.B1 nõutud varusüsteemi jaoks.

Tootmissüsteemist erineb see ainult paigalduskoha ja WAN-ühenduse poolest. Seega tuleb varusüsteem integreerida IT-etalonturbe modelleerimisega.

- IT-etalonturbega ette nähtud meetme M 6.53 „Võrgukomponentide liiasus" nõudeid täpsustatakse kommutaatori N7 puhul meetmega M 6.B1. Pärast meetme M 6.B1 võtmist täidetakse sihtobjekti N7 puhul ka meetme M 6.53 nõudeid. Seega võib kommutaatori N7 puhul meetme M 6.53 turbekontseptsioonist eemaldada.
- Kahe aasta eest otsustati, et meede M 5.68 „Krüpteerimisprotseduuride kasutamine võrgusuhtluses" on liigne. Ühises projektirühmas otsustati koos tellijaga, et see otsus ei vasta enam tehnika tasemele. Seetõttu kontrollitakse marsruuterite konfiguratsiooninõudeid ja kohandatakse need tegelike vajadustega.
- Täiendav turbemeede M 1.B1 on ette nähtud klientsüsteemi C4 eriliste taristuliste raamtingimuste täitmiseks. Tootmisüksuses käitatakse peale selle klientsüsteemi ka muud infotehnoloogiat, mis pole küll riskianalüüsi sihtobjekt, kuid vajab sellegipoolest asjakohast turvet. Ettevõte seab eesmärgiks võtta meede M 1.B1 ning töötab selleks välja tootmisüksuse infotehnoloogia turvalise käitamise poliitika.
- Jne

8 Turbeprotsessi jätkamine

Pärast turbekontseptsiooni konsolideerimist saab jätkata IT-etalonturbe metoodikas kirjeldatud turbeprotsessi. Täiendatud turbekontseptsioon on seega aluseks järgmistele töösammudele.

- Esmane turbekontroll (IT-etalonturbe metoodika peatükk 4.5). Esmane turbekontroll tehti IT-etalonturbe mudelis ette nähtud meetmete jaoks juba eeltööde raames. Kuna riskianalüüsi käigus selgub tavaliselt, et turbekontseptsiooni on tarvis muuta, tuleb seejärel veel kontrollida lisatud või muudetud meetmete võtmise seisundit. Vananenud tulemusi tuleb värskendada.
- Turbekontseptsiooni elluviimine (IT-etalonturbe metoodika peatükk 5). Turbekontseptsioonis sihtobjektide jaoks ette nähtud turbemeetmeid tuleb kindlasti ka reaalselt võtta, et neist kasu oleks. See hõlmab muu hulgas kulude ja töömahu hindamist ning elluviimise järjekorra kindlaksmääramist.
- Turbeprotsessi kontroll kõikidel tasanditel (IT-etalonturbe metoodika peatükk 6.1). Infoturbe tagamiseks ja selle pidevaks tõhustamiseks tuleb muu hulgas regulaarselt kontrollida turbemeetmete elluviimist ja turbestrateegia sobivust. Kontrollide tulemusi kasutatakse turbeprotsessi täiendamiseks.
- Infoturbeprotsessi infovoog (IT-etalonturbe metoodika peatükk 6.2). Kontrollitavuse tagamiseks peavad kõik turbeprotsessi tasandid olema dokumenteeritud. Selle alla kuuluvad ka selged reeglid teavitamiskanalite ja infovoo kohta. Turbeosakond peab juhtkonda pidevalt ja piisaval määral infoturbe olukorrast informeerima.
- Andmete ülevõtmine ISKE tööriista (vt http://www.bsi.bund.de/gstool). Kui turbehalduses kasutatakse ISKE tööriistavõi mõnda muud samaotstarbelist tarkvara, tuleks riskianalüüsi tulemused võimaluste piires sinna sisse kanda. ISKE tööriistas kehtib see eriti just uute või muudetud turbemeetmete kohta, mida sellisel kujul IT-etalonturbe kataloogides ei eksisteeri.