„Ettevõtlus- ja infotehnoloogiaministri
16. detsembri 2022 määruse
nr 101 „Eesti infoturbestandard“
Lisa 1
(muudetud sõnastuses)

Nõuded infoturbe halduse süsteemile

1. Sissejuhatus

Eesti infoturbestandard on eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks. Eesti infoturbestandardi aluseks on Saksa päritolu BSI IT-Grundschutz etalonturbe meetod.

1.1. Käsitlusala

Käesolev lisa esitab nõuded ning juhised küberturvalisuse seaduse § 3 lõigetes 1 ja 4 nimetatud juriidilisele isikule, riigi- või kohaliku omavalitsuse asutusele, hallatavae asutusele, riigitulundusasutusele, avalik-õiguslik juriidilisele isikule või nende struktuuriüksusele (edaspidi koos *organisatsioon)* infoturbe halduse süsteemi (ingl *Information Security Management System*, ISMS) rajamiseks, evitamiseks, käigushoidmiseks ja täiustamiseks.
Eesti infoturbestandardiga vastavuse saavutamiseks tuleb täita jaotistes 5–10 esitatud nõuded.
Eesti infoturbestandard ei korraldata riigisaladuse ega salastatud välisteabe turvet.

1.2. Sihtgrupp

Infoturbe halduse süsteemi nõuete dokumendi peamised sihtgrupid on:

- Eesti infoturbestandardi rakendajad: infoturbejuhid, äriprotsessijuhid, üksuste juhid, infotehnoloogia valdkonna töötajad;
- audiitorid;
- konsultandid.

1.3. Normiviited

Käesolev lisa toimib koosmõjus etalonturbe kataloogiga (edaspidi koos *E-ITS*), millesse on koondatud parimad tavad infoturbeprotsessi loomiseks ja käigushoidmiseks.

2. Kasutatud terminid

Nr	Termin või lühend	Lähtekeeles (inglise / saksa)	Lühike definitsioon
1	konfidentsiaalsus	*confidentiality*	teabe kättesaamatus või paljastamatus volitamata isikutele, olemitele või protsessidele. Üks kolmest infoturbe põhikomponendist, märgitakse tähega C lühendis C-I-A.
2	terviklus	*integrity*	teabe õigsus ja täielikkus, lubamatute muudatuste

			puudumine, hõlmab ka autentsust ja salgamatust. Üks kolmest infoturbe põhikomponendist, märgitakse tähega I lühendis C-I-A.
3	käideldavus	*availability*	teabe omadus olla volitatud olemi nõudel õigel ajal kättesaadav ja kasutuskõlblik. Üks kolmest infoturbe põhikomponendist, märgitakse tähega A lühendis C-I-A.
4	kahju	*loss*	soovimatu muutuse mõõt, riskianalüüsi aluskomponent, esmane infoturbevajadust otsustav tegur
5	alusohud	-	riskide kaalutlemisel kasutatud ohud; etalonturbe meetmete koostamise alus
6	risk	*risk*	ohu võimekus tekitada organisatsioonile kahju.
7	infoturbe halduse süsteem	*Information Security Management System* (edaspidi ISMS)	süsteem, mis koosneb poliitikatest, protseduuridest, juhistest ning nendega seotud ressurssidest ja tegevustest, mida organisatsioon kollektiivselt haldab, et kaitsta oma infovarasid infoturbe halduse süsteemis on suunatud ärieesmärkide saavutamisele ning kujutab endast süstemaatilist lähenemist infoturbe rajamisele, käigushoiule, seirele, hooldamisele ja täiustamisele. See põhineb riski kaalutlemisel ja selle aktsepteerimisel tasemetele, mis tagavad riskide toimiva käsitluse ja halduse.
8	infoturvapoliitika	*Information Security Policy*	organisatsiooni keskne infoturbealane dokument, mis sätestab arengusuunad ja taotletavad sihid, määrab lubatu ja lubamatu
9	käsitlusala	*scope*	Infoturbe halduse süsteemi kontekstis: organisatsiooni kaitstavad elemendid, nagu taristu, töö korraldus, personal, tehnilised komponendid
10	kaitseala*	*Informations-verbund* (saksa)	turbekontseptsiooni koostamise ja rakendamise käsitlusala. Organisatsioon liigitab

			kaitsealasse kogumi sihtobjekte, mida turbeprotsess hakkab edaspidi kaitsma.
11	sihtobjekt*	*Zielobjekt* (saksa)	kaitseala allosa – igasugune infosüsteemi kuuluv kaitsetarbega vara, nagu äriprotsess, rakendus, IT-lahenduse komponent, komponendirühm, hoone, kinnistu, allüksus. Sihtobjektile vastendatakse etalonmoodul(id).
12	protsess	*process*	omavahel seotud või interakteeruvate tegevuste kogum, mis muundab lähtematerjali tulemiteks.
13	äriprotsess	*business process*	organisatsiooni tegevuse element, mingi eesmärgi saavutamisele suunatud tegevuste, toimingute või protseduuride kogum. Äriprotsessi tulemusena võidakse luua sise- või väliskliendile väärtust toodete või teenustena.
14	kaitsetarve	*protection requirement* (ingl), *Schutzbedarf* (saksa.k)	vara väärtusest tulenev vajadus seda kaitsta. Kaitsetarve on andmete ja teabe vajadus kaitsta neid kahju eest, mille võib tekitada konfidentsiaalsuse, tervikluse või käideldavuse või kõigi kolme rikkumine. E-ITSi kontekstis laieneb kaitsetarve ka äriprotsessile, mille korral hinnatakse kaitsetarvet, lähtudes kahjustsenaariumitest (nt õigusaktide, eeskirjade või lepingute rikkumine; teabelise enesemääramisõiguse rikkumine; isiku füüsilise puutumatuse rikkumine; ülesannete täitmise võime kahjustamine; negatiivsed sisemised või välised toimed; rahalised tagajärjed). Kaitsetarvet väljendatakse kolmeastmelises skaalas: „normaalne“, „suur“ või „väga suur“. Kuna kaitsetarbe määramine on organisatsiooniriskihalduse osa,

			siis riskihalduse metoodikas määratleb organisatsioon ise kaitsetarbe kahjustsenaariumid ja täpsustab skaalat enda kontekstist ja tegelikest potentsiaalsetest mõjudest lähtuvalt.
15	normaalne kaitsetarve	-	kaitsetarbe skaala määrang, kus võimaliku kahjustuse toime on piiratud ja ohjatav. Sellise kaitsetarbe korral on etalonturbe meetmed asjakohased ja nende rakendamisest üldjuhul piisab.
16	suur kaitsetarve	-	kaitsetarbe skaala määrang, kus võimaliku kahjustuse toimed võivad olla tõsised. Sellise kaitsetarbe korral ei pruugi etalonturbe meetmetest alati piisata. Tuleb läbida etalonturbe väline riskianalüüs ja vajaduse korral määrata lisaturvameetmed.
17	väga suur kaitsetarve	-	kaitsetarbe skaala määrang, kus kahjustuse toimed võivad ulatuda katastroofilise tasemeni, ähvardades organisatsiooni olemasolu või ülesannete täitmise täielikku katkemist. Sellise kaitsetarbe korral ei piisa etalonturbe meetmetest kindlasti. Riskianalüüs on kohustuslik, konkreetsele ohule eraldi tuleb määrata asjakohased turvameetmed.
18	meetme teostatuse määr	-	märge infoturbe meetmete rakendusplaanis, mis väljendab meetme käsitlusviisi ja teostuse hetkestaatust.
19	turbeviis	-	meetod E-ITSi standardil põhineva infoturbe halduse süsteemi rajamiseks. Turbeviisi valikul lähtutakse regulatsioonidest, lähtudes õigusaktidest, asjakohasest eeskirjadest ja standarditest ja kaitsetarbest, aga ka organisatsiooni infoturbe küpsusest.

			Organisatsioonil on võimalik valida turbeviisiks: a) põhiturve, kui kaitsetarve on normaalne. Põhiturbe rakendamine on eelduseks standardturbe rakendamisele; b) standardturve, kui kaitsetarve on suur või väga suur; c) tuumikuturve kaitseala osale, kus kaitsetarve on suur või väga suur, ent kogu organisatsioonile pole võimalik standardturvet rakendada.
20	teave	-	teadmus inimesele sobival kujul inimsuhtluses. Eesti keel eristab teavet informatsioonist kui teadmuse masinale sobivast kujust. Seejuures puudub andmetel kontekst ja tähendus, teabel ja informatsioonil on see olemas.
21	infoturbe meetmete rakendusplaan (IMR)	-	dokument, milles loetletakse ja kirjeldatakse infoturbe halduse süsteemile kohaldatavaid turvameetmeid, põhjendatakse meetmete teostamise valikuid ning määratakse vastutajad ja tähtajad
22	vastutaja	*responsibility, responsible*	E-ITSi tähenduses roll, mille täitjale on parimate tavade kohaselt määratud infoturbe meetmete rakendamise ülesanne E-ITSis kasutatakse terminit „vastutaja“, sealhulgas ka terminit „lisavastutaja“ meetme rakendamisel, et tööülesannete jagamisel siduda rolli vastutus soovitusliku ametikoha nimetusega organisatsioonis.

(*) – etalonturbe spetsiifiline mõiste

3. Jaotiste lühiülevaade

Jaotises 4 kirjeldatakse E-ITSi ning selgitatakse selle suhet riskihaldusega ja standardiga EVS-EN ISO/IEC 27001. Lisaks esitatakse infoturbe halduse süsteemi lühikirjeldus.

Jaotises 5 esitatakse nõuded infoturbeprotsessi tsükli igakordsele algatamisele ja juhtkonna kohustumusele.

Jaotises 6 esitatakse nõuded infoturbe protsessi kavandamisele ja plaanimisele ning selle korraldamise struktuuridele.

Jaotises 7 esitatakse nõuded infoturbe halduse süsteemi riskihaldusele, sealhulgas etalonturbe modelleerimisele ja täiendavale välisele riskihaldusele.
Jaotises 8 esitatakse nõuded riskihalduse abil väljaselgitatud meetmete rakendamisele.
Jaotises 9 esitakse nõuded infoturbeprotsessi pidevaks käigushoidmiseks.
Jaotises 10 esitatakse nõuded infoturbe protsessi täiustamiseks ja sõltumatu läbivaatuse korraldamiseks.
Jaotises 11 kirjeldatakse võimalusi infoturbe halduse süsteemi toimimisele välise kinnituse saamiseks – auditeerimist.
Jaotis 12 loetleb viited rakendaja jaoks vajalikule lisateabele.

4. E-ITS olemus

E-ITSi eesmärk on tagada avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kõikehõlmav kaitse ning saavutada infoturbe ühtlane tase nende kõigis osades kogu elutsükli jooksul.

E-ITSi põhimeetod on BSI IT-Grundschutz päritolu etalonturve. E-ITSi lähenemine infoturbele põhineb tegevusriskide haldamisel.

E-ITSi etalonturve lõimituna riskihaldusega
Toimingud jagunevad kaheks:

1. Äriprotsesside toimimiseks vajalikud sihtobjektid seatakse vastavusse etalonmoodulitega, mille tulemusel tüüpsete ohtude riskikäsitlus toimub tüüpmeetmete rakendamisega. Sellega saavutatakse toimiv turbehaldus enamikus organisatsiooni äriprotsessides.
2. Äriprotsesside toimimiseks vajalike ebatüüpsete etalonturbesse sobimatute või normaalselt kõrgema kaitsetarbega sihtobjektide osas sooritatakse etalonturbe väline riskianalüüs täiemahulise riskihalduse abil. Kasutatava metoodika kinnitab organisatsiooni juhtkond. Ebatüüpsetele sihtobjektidele rakendatakse infoturbe meetmeid vastavalt etalonturbe välise riskihalduse tulemustele.

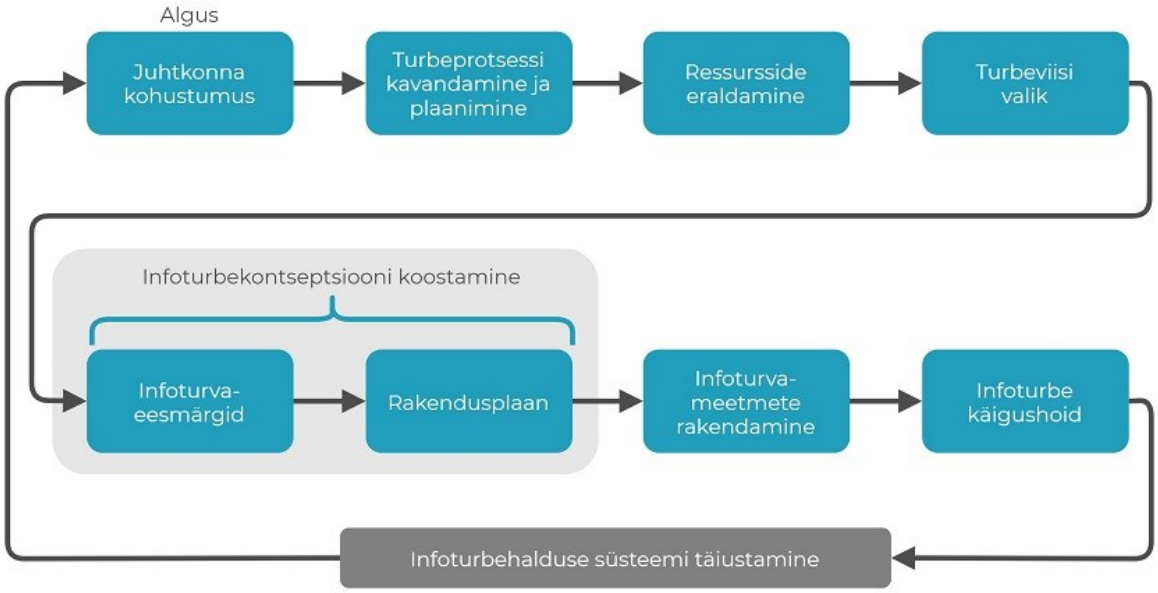
E-ITSi rakendatust tõendatakse välisaudiitori E-ITS auditi järeldusotsusega. Auditeerimise vajadus võib tuleneda õigusaktis, valdkonna standardis või lepingus sätestatud kohustusest. Auditeerida võib ka organisatsiooni enda soovil.
E-ITSi rakendamisega standardturbe ulatuses saavutatakse üldine vastavus Eesti standardiga EVS-EN ISO/IEC 27001 või rahvusvahelise standardiga EN ISO/IEC 27001.
(*) - *Ebatüüpne ja vahetut riskikäsitlust nõudev sihtobjekt on vähemalt üks järgmistest: a) sihtobjekti kaitsetarve osutub infoturbe ühe või enama põhikomponendi (C I A) osas suureks või väga suureks; b) sihtobjekti ei õnnestu vastendada ühegagi olemasolevatest moodulitest, enamasti uudsuse või erilisuse tõttu; c) sihtobjekti kasutusviis erineb etalonmoodulis kirjeldatust.*

4.1. Infoturbe halduse süsteem

ISMS on organisatsiooni juhtimise osa, mis tegeleb infoturbe rajamise, evitamise, käigushoiu ja pideva täiustamisega.
ISMS hõlmab:

- organisatsiooni struktuuri, protsesse, protseduure ja tavasid;
- poliitikaid ja plaanimistegevusi;
- kohustusi;
- ressursse ja varasid.

Infoturbe halduse süsteemi protsesse ja sooritatavaid tegevusi kujutab Joonis 1. ISMSi tegevusi sooritatakse vajadusel paralleelselt. Infoturbe täiustamise käigus naastakse iga kord protsessi algusesse. Infoturbe kontseptsiooni koostamisel lähtutakse E-ITSi kataloogi meetmetest ja vajadusel etalonturbe välisest riskihalduse käigus tuvastatud riskikäsitlusmeetmetest.
ISMSi teostusjuhised on esitatud etalonturbe kataloogis, moodulis ISMS.1 „Turbehaldus".



Joonis 1. Infoturbe halduse süsteemi käivitamise ja uuendamise tegevused

5. Infoturbeprotsessist üldiselt

5.1. Infoturbeprotsessi algatamisest üldiselt

5.1.1 Infoturve lähtub organisatsiooni eesmärkidest ja tegutsemisviisidest. Infoturbe eestvedaja (ingl *leadership*) on organisatsiooni struktuuris kõrgeim juhtimistasand (tippjuhtkond). Infoturbeprotsessi algatab tippjuhtkond ja nimetab infoturbejuhi rolli täitja. Infoturbejuht korraldab organisatsiooni infoturbetegevust. Infoturbejuhi nimetamata jätmise korral täidab seda rolli juhtkond.
5.1.2 Infoturve keskendub teabe ja sellest sõltuvate äriprotsesside kaitsmisele ning sellest tulenevalt infotöötluse või infotehnoloogia kaitsmisele. Seetõttu kirjeldab organisatsioon esmalt äriprotsessid ja alles siis võtab arvele oma äriprotsessidega seotud varad ja määrab kaitseala koos sihtobjektidega.

5.2. Tippjuhtkonna kohustumus

5.2.1 Kuna organisatsiooni äriprotsesside toimimise eest vastutab tippjuhtkond, siis tippjuhtkond vastutab ka äriprotsesse ohustavate sündmuste käsitlemise, sh infoturbe halduse eest. Infoturbealase vastutuse võtmist tippjuhtkonnas nimetatakse juhtkonna kohustumuseks (ingl *commitment*).
5.2.2 Tippjuhtkonna kaasatus tagab infoturbe lõimitusse kaitseala kõigisse protsessidesse ja infoturbe jätkusuutlikkuse. Tippjuhtkond vastutab infoturbe elluviimise, käigushoidmise ja täiendamise eest. Selleks määrab juhtkond turbealased õigused ja kohustused ning eraldab ressursid.
5.2.3 Tippjuhtkond peab saama infoturbe kohta regulaarselt, õigeaegselt ja sobivas ulatuses järgmist teavet:
a) organisatsiooni ja selle teabe turvariskid ning nendega seotud toimed ja kulud;

b) turvaintsidentide toime äriprotsessidele;
c) regulatsioonidest (nt õigusaktid, eeskirjad, standardid) ja lepingutest tulenevad turvanõuded
d) tegevusalale tüüpilised infoturbe protseduurid;
e) infoturbe hetkeseis ja sellest tulenevad tegevussoovitused (infoturbe meetmete rakendusplaan);
f) infoturbeprotsessi täiendusettepanekud (sh sõltumatu läbivaatuse ja auditeerimise tulemid);
g) huvipooltega seotud kohustused ja tagasiside.
5.2.4 Infoturbealaseid tegevusi plaanib ja koordineerib infoturbejuht.
5.2.5 Äriprotsessi infoturbe meetmete rakendamist korraldab protsessijuht. Rakendatav infoturve peab olema normaalse tööprotsessi osa ning olema kooskõlas töö eesmärkidega.
5.2.6 Infoturbeprotsessi peavad olema kaasatud kõik töötajad. Töötajate motiveerimiseks ja koolitamiseks kaasatakse ISMSi rakendamisse personaliosakond ja protsessijuhid..

6. Infoturbeprotsessi kavandamine ja plaanimine

6.1. Infoturvapoliitika

6.1.1 Infoturvapoliitika on organisatsiooni infoturbe juhtdokument, milles esitatakse infoturbealane kohustumus ning sõnastatakse organisatsiooni infoturbe sihid (ingl goal), vajadused ja põhimõtted (ingl *principle)*. Infoturvapoliitika põhimõtteid kasutatakse organisatsiooni väärtuste kaitseks.
6.1.2 Organisatsiooni kaitstavad väärtused tuletatakse üldisest keskkonnast ja organisatsiooni põhieesmärkidest. Põhieesmärgid tulenevad ettevõtte puhul ärieesmärkidest, avaliku sektori asutuse puhul põhikirjast või põhimäärusest.
6.1.3 Organisatsiooni väärtustena võetakse arvesse vähemalt järgmist:
a) toimingute, sealhulgas teabekäitluse kõrge usaldatavus (käideldavus, terviklus, konfidentsiaalsus jne);
b) organisatsioonisisene ja -väline hea maine;
c) investeering tehnoloogiasse, teabesse, tööprotsessidesse ja teadmusse;
d) töödeldav informatsioon (selle suur või korvamatu väärtus vajab kaitset, sh isikuandmed);
e) regulatsioonide (õigusaktide, eeskirjade, standardite) ja lepingute nõuete täitmine;
f) inimeste füüsiline ja vaimne heaolu.
6.1.4 Organisatsiooni infoturvapoliitika koostamisel arvestatakse:
a) organisatsiooni eesmärke ja strateegiat;
b) organisatsiooni struktuuri;
c) organisatsiooni olemasolevaid haldussüsteeme, nt kvaliteedihaldus, riskihaldus, keskkonnahaldus;
d) õigusalaseid raamtingimusi, sh kohalikud ja rahvusvahelised õigusaktid, valdkondlikud määrused;
e) klientide, tarnijate, partnerite jt huvipoolte nõudeid;
f) tegevusala turvastandardeid ja -praktikaid.
6.1.5 Infoturvapoliitika sisaldab infoturvaeesmärke või loob raami infoturvaeesmärkide püstitamiseks.
6.1.6 Infoturvapoliitika kinnitab juhtkond. Infoturvapoliitika tehakse teatavaks töötajatele ning vajadusel teistele huvipooltele.
6.1.7 Organisatsioon vaatab infoturvapoliitika perioodiliselt või oluliste muutuste korral üle ja ajakohastab vajadusel.

Joonis 2. Infoturvapoliitika põhilised elemendid
Joonis 2 esitab infoturvapoliitika põhilised elemendid.

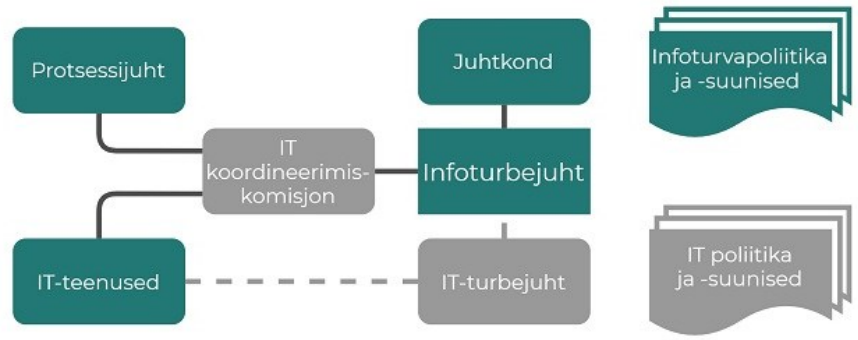
6.2. Infoturvaeesmärgid

6.2.1 Infoturvaeesmärgid (ingl *security objective*) lähtuvad infoturbe tähtsusest organisatsioonile, on realistlikud, praktilised (seotud toimingutega), põhjendatud, arusaadavad ja võimaluse korral mõõdetavad. Infoturvaeesmärkidele on määratud eesmärgi saavutamise tähtaeg.
6.2.2 Organisatsioon kasutab infoturvaeesmärkide sõnastamisel järgmist teavet:
a) äriprotsessid, protsessijuhid, protsesside kirjeldus ja äriprotsesside seosed organisatsiooni eesmärkidega;
b) äriprotsesside omavahelised seosed ja sõltuvused;
c) äriprotsessidega seotud varad ja kaitstavad sihtobjektid;
d) äriprotsesside ja alusteabe kaitsetarvet konfidentsiaalsuse, tervikluse ja käideldavuse ning vajadusel teiste infoturbe komponentide kohta;
e) organisatsiooni tegevusriskid, nt turu hetkeseis, konkurentsiolukord, geopoliitiline olukord ja muud turuspetsiifilised sõltuvused;
f) olemasolev infoturbedokumentatsioon.
6.2.3 Eelnimetatud teabe kogumiseks organisatsioon:
a) kirjeldab äriprotsessid ja võtab arvele varad;
b) määrab organisatsiooni infoturbe kaitseala ja sihtobjektid;
c) valib etalonturbe korral turbeviisi (põhi-, standard-, tuumikuturve);
d) määrab sihtobjektide kaitsetarbe skaalal „normaalne“, „suur“, „väga suur“;
e) dokumenteerib infoturvaeesmärgid ja määrab eesmärkide saavutamise ajaraamid.
6.2.4 Organisatsioon sõnastab infoturvaeesmärgid, vaatab neid regulaarselt läbi ja vajadusel ajakohastab.

6.3. Infoturbeprotsessi korraldus

6.3.1 Infoturbeprotsessi rakendamiseks ja edendamiseks loob organisatsioon turbekorraldus- ja teavitusstruktuuri.
6.3.2 Infoturbe korraldusstruktuuriga määrab juhtkond:
a) rollid ja vajadusel rollipädevusnõuded;
b) rollide täitjad;
c) volitused ja vastutusalad.
6.3.3 Organisatsioon tagab rollitäitjate pädevuse ja vajalike pädevustõendite säilitamise.

6.3.4 Organisatsioon tuvastab sisemised ja välised infoturbealase teavituse vajadused ning määrab teavitusviisid, osalevad rollid jm tingimused.
6.3.5 Turbekorraldus tehakse töötajatele teatavaks.



Joonis 3. Infoturbe korraldusstruktuuri näidis
NÄIDE. Joonisel 3 on kujutatud üht võimalust, kuidas infoturbealane töö organisatsioonis korraldada. Igal äriprotsessil on protsessijuht. IT-koordineerimiskomisjon on korralduslik foorum, kus arutatakse IT-teenuste ja infoturbeaspektidega seonduvat. IT-turbejuht on nõutud vaid suurtes organisatsioonides, kus infoturbealase töö koordineerimine vajab eristamist IT-lahenduste turvastrateegiate täideviimisest. Halli värviga on märgitud elemendid, mida väiksem organisatsioon ei pruugi vajada.

6.4. Infoturbealane koolitus

6.4.1 Vastavuses infoturvapoliitika eesmärkidega tagab organisatsioon kõikide töötajate vajaliku infoturbealase pädevuse ja pädevuse uuendamise.
6.4.2 Regulaarsete infoturvet käsitlevate koolituste eesmärk on motiveerida töötajaid järgima infoturvanõudeid, käsitlema teavet ja töövahendeid korrektselt, vältima riskikäitumist ja asjakohaselt reageerima infoturbeintsidentidele.

6.5. Ressursside eraldamine

Juhtkond eraldab rahalised ja mitterahalised ressursid infoturbeprotsessi elluviimiseks. Juhtkond aktsepteerib töötajate põhitööga kaasnevaid infoturbekohustusi.

6.6. Juhtkonna kinnitus

Juhtkond kinnitab infoturvapoliitika, turvaeesmärgid ja infoturbele ressursside eraldamise.

6.7. Infoturbeprotsessi dokumenteerimine

6.7.1 Dokumenteerimise abil tagatakse infoturbeprotsessi jätkusuutlikkus ja jälgitavus. Dokumendid tuleb koostada taasesitamist ja ajakohastamist võimaldavas vormis ning versioonihaldusega kaetud viisil. Tuleb tagada, et käibelt on kõrvaldatud vananenud dokumendid ja versioonid
6.7.2 Organisatsioon kehtestab dokumentide koostamise, vormistamise ja hoidmise reeglid.
6.7.3 Poliitikad ja eeskirjad vaadatakse üle vähemalt üks kord aastas ning muudatused kinnitab juhtkond. Korrad ja protseduurijuhendid hoitakse tegelike protsessidega kooskõlas.
6.7.4 Organisatsioon loob ja säilitab tegevusdokumentatsiooni, mis tekib või luuakse infoturbeprotsessi käigus.
6.7.5 Dokumenteeritakse:
a) infoturbeprotsessi alusdokumendid ja nende väljatöötamise kulg konteksti jäädvustamiseks;

b) otsused, sh infoturbe meetmete rakendusplaan, et tagada otsuste ja meetmete rakendamise käigu jälitatavus (ingl *traceability*);
c) infoturbesündmused sisendiks riskihaldusse infoturbe täiustamiseks;
d) organisatsiooni reaktsioon sündmustele ja otsustele, et näidata parandusmeetmete toimivust;
e) muu teave, mida organisatsioon ise peab vajalikuks säilitada infoturbe halduse toimivuse huvides.
6.7.6 Infoturbeprotsessi dokumentatsioon on volitatuile kättesaadav ja kaitstud kõrvalise juurdepääsu eest.

7. Infoturbeprotsessi riskihaldus

7.1 Kaitsetarbe määramine

7.1.1 Etalonturbe kontseptsioon lähtub põhimõttest, et infoturvaohud ja kaitstavad varad on erinevate organisatsioonide puhul tüüpsed. E-ITSi etalonturbe kataloog esitab moodulitesse koondatud eelanalüüsitud meetmekomplektid, mis katavad tüüpsete sihtobjektide riskihalduse ja infoturvavajadused. Tervikliku turbe saavutamiseks rakendatakse ebatüüpsetele ja kõrgendatud kaitsetarbega („suur“ ja „väga suur“) sihtobjektidele etalonturbe välist riskihaldust.
7.1.2 Organisatsioon määrab kaitsetarbe määramise põhimõtted, sh organisatsioonile kohandatud kahjustsenaariumid, riski aktsepteerimise kriteeriumid, kaitsetarbe komponendid (vähemalt konfidentsiaalsus, terviklus, käideldavus ehk C-I-A) ja täpsustab kaitsetarbe määramise skaala, lähtudes organisatsiooni eripäradest.
7.1.3 Kaitsealasse kuuluvate sihtobjektide kaitsetarve tuvastatakse ja dokumenteeritakse, sh määratakse kaitsetarve väljast tellitavatele teenustele (tarneahel).
7.1.4 Riskihalduse käik ja tuvastatud või määratud meetmete rakendamise otsused dokumenteeritakse korratavuse ja võrreldavuse eesmärgil.

7.2. Etalonturbe modelleerimine

7.2.1 Organisatsioon vastendab kaitsealasse kuuluva iga sihtobjekti etalonturbe kataloogi ühe või mitme mooduliga. Moodulite rakendamise järjekord määratakse lähtuvalt organisatsiooni infoturvapoliitikast ja reaalsetest vajadustest.
7.2.2 Moodulist sihtobjekti turvameetmete tuvastamisel arvestatakse:
a) turbeviisi (põhiturve, standardturve või tuumikuturve);
b) sihtobjekti kaitsetarvet;
c) meetme seost infoturbeprotsessi ja sihtobjekti elutsükliga.
7.2.3 Etalonturbe kataloogi protsessimoodulrühmade kõik moodulid kaasatakse rakendusplaani. Mooduli käsitlemata jätmine peab olema põhjendatud.
7.2.4 Süsteemimoodulid rakendatakse vastavuses kaitseala määratlusega.
7.2.5 Kui organisatsioon on normaalse kaitsetarbe korral valinud turbeviisiks põhiturbe, tuleb etalonturbe meetmete rakendamisel tagada esmajärjekorras põhimeetmete rakendamine. Pideva infoturbe täiendamise protsessi eesmärk on standardturbe rakendamine. Väljajätud põhiturbest tuleb põhjendada, lähtudes eelkõige riskide aktsepteerimise kriteeriumitest.
7.2.6 Standardturbe puhul rakendatakse lisaks esmajärjekorras rakendatud põhimeetmetele ka standardmeetmed ja veendutakse etalonturbe välise riskihaldusega etalonturbe meetmete piisavuses. Vajadusel rakendatakse olenevalt kaitsetarbest kõrgmeetmed ja etalonturbe välised lisameetmed. Väljajätud põhimeetmetest ja standardmeetmetest põhjendatakse, lähtudes eelkõige riskide aktsepteerimise kriteeriumitest.

7.3. Etalonturbe väline riskihaldus

7.3.1 Organisatsioon suunab etalonturbe välisesse riskihaldusse sihtobjektid, mille jaoks puudub etalonturbe kataloogis sobiv moodul. Lisaks suunatakse välisesse riskihaldusse sihtobjektid, kui sihtobjektid, mille puhul on täidetud üks järgmistest tingimustest:
a) kaitsetarve on suur või väga suur;
b) kaitsetarve on määramata või ebaselge;
c) kasutusviisid ei ole vastavuses etalonturbe kataloogi moodulite kirjeldustega;
d) etalonturbe kataloogi meetmed osutuvad turvaeesmärkide täitmisel puudulikuks (jääkrisk ei ole aktsepteeritav;
e) kui sihtobjektist sõltub samaaegselt mitme organisatsiooni jaoks olulise äriprotsessi toimimine.

7.3.2 Organisatsioon määrab etalonturbe välise riskihalduse protsessi. Riskihalduse asjaolud, kulg ja tulemused dokumenteeritakse.

7.3.3 Etalonturbe väline riskihaldus määrab sihtobjektidele lisaturvameetmeid, lähtudes sihtobjekti kaitsetarbest ja infoturvaeesmärkidest.

8. Infoturvameetmete rakendamine

8.1 Tehnilised meetmed rakendatakse kõigile kaitseala sihtobjektidele.

8.2 Organisatsioonilised meetmed lõimitakse organisatsiooni kõigisse protsessidesse.

8.3 Meetmete rakendamise eest vastutab vastava protsessi juht või etalonturbe kataloogis nimetatud vastutaja rolli täitja. Rakendamist koordineerib ja nõustab infoturbejuht.

8.4 Organisatsioon hindab tuvastatud ja määratud meetmete:
a) ressursside ühekordseid ja korduvaid kulusid;
b) sobivust, teostatavust, piisavust, võimalikku toime efektiivsust ja meetmete omavahelisi mõjusid.

8.5 Infoturvaeesmärkide järgi määrab organisatsioon eelnevalt tuvastatud info põhjal infoturbe meetmete rakendusplaanis (IMR) vähemalt:
a) rakendatavad turvameetmed koos nimetuse ja identifikaatoritega, sh etalonturbe välise riskihalduse käigus määratud lisameetmed;
b) meetme teostatuse määra;
c) meetme rakendamise puhul selgitus ajakohase ülevaate ja hilisema jälitatavuse eesmärgil, kuidas meede on organisatsioonis rakendatud; meetme mitterakendamisel selle kohaldamata jätmise põhjendus; meetme osalise rakendamise puhul täpsustav selgitus, milliste äriprotsesside, varade või alammeetme osas on meede täitmata;
d) meetme rakendamise eest vastutajad;
e) meetmete rakendamise või meetme järgmise sisulise ülevaatuse tähtajad.

8.6 Organisatsiooni juhtkond teadvustab ja aktsepteerib regulaarselt jääkriskid ning nende alusel kinnitab rakendusplaani.

8.7 Meetmed rakendatakse vastavalt rakendusplaanile.

8.8 Organisatsioon tagab meetmetes kirjeldatud korduvate ja regulaarsete tegevuste tõendatavuse, võrreldavuse, järjepidevuse ja õigeaegsuse.

9. Infoturbe käigushoid

9.1 Organisatsioon tagab infoturbeprotsessi ning -turvameetmete pideva ja jätkusuutliku toimimise. Jälgitakse ja mõõdetakse:
a) infoturvaeesmärkide saavutatust ja -meetmete sobivust ning tõhusust;
b) ressursside kasutamist.

9.2 Organisatsioon reageerib muutustele organisatsiooni eesmärkides, regulatsioonide nõuetes ja lepingulistes kohustustes ning ümbritsevas infoturbeolukorras. Protsessijuhid tagavad infoturvet puudutava teabe õigeaegse edastamise asjakohaste rollide täitjatele.
9.3 Seiratakse protsesside ja süsteemide töö käigus tekkinud teavet. Olulistele infoturbe sündmustele reageeritakse ja need registreeritakse.
9.4 Seire, ülevaatuste ja kontrollide dokumenteeritud tulemusi ja järeldusi kasutab organisatsioon riskihalduses ettepanekute koostamiseks infoturbeprotsessi ja -meetmete täiustamiseks ning muutmiseks.
9.5 Infoturbeprotsessi käigus ilmnenud asjaoludest ja nende muutumisest teavitatakse vajalikus ulatuses:
a) organisatsiooni juhtkonda;
b) määratud rollide täitjaid;
c) organisatsiooni töötajaid;
d) teisi huvipooli.

10. Infoturbeprotsessi täiustamine

10.1. Infoturbe parendamine

10.1.1 Organisatsioon kontrollib perioodiliselt infoturbeprotsessi, infoturvapoliitika ja infoturvaeesmärkide sobivust ja asjakohasust.
10.1.2 Infoturbeprotsessi täiustamise põhjused on muu hulgas järgmised:
a) organisatsiooni eesmärkide ja nõuete muutused;
b) infoturvapoliitika ja infoturvaeesmärkide muutused;
c) turvaolukorra muutused;
d) regulatsioonide ja standardite muutused;
e) kaitseala ja kaitsetarbe olulised muutused;
f) infoturbeprotsessi käigus ilmnenud asjaolud, sh intsidentide, läbivaatuste, auditeerimiste järeldused ja ettepanekud.
10.1.3 Organisatsiooni juhtkond teeb otsused infoturbe täiustamiseks, tuginedes punktis 5.2.3 nimetatud teabele.

10.2. Sõltumatu läbivaatus

10.2.1 Organisatsioon korraldab regulaarselt infoturbeprotsessi tulemite ja seisundi sõltumatu läbivaatuse. Sõltumatuks läbivaatuseks võib olla ka käsitlusala hõlmav siseaudit.
10.2.2 Sõltumatul läbivaatusel hinnatakse organisatsiooni infoturbehalduse vastavust:
a) siinse dokumendiga;
b) organisatsiooni infoturvapoliitikaga.
10.2.3 Sõltumatu läbivaatuse elluviijaks on vastavalt infoturvapoliitikale kas siseaudiitor, siseaudiitori rollitäitja (nt välisaudiitor) või käsitlusala suhtes asjakohase pädevusega sõltumatu töötaja. Sõltumatul läbivaatusel välditakse kontrollija ja rakendaja rollide huvikonflikti.
10.2.4 Organisatsioon määrab sõltumatu läbivaatuse käsitlusala ja eesmärgid. Läbivaatuse elluviimisel arvestatakse:
a) organisatsiooni eesmärke;
b) regulatsioonide nõudeid ja lepingulisi kohustusi;
c) organisatsiooni infoturvapoliitikat ja -eesmärke;
d) varasemate läbivaatuste tulemusi.
10.2.5 Läbivaatuste tulemused ja ettepanekud dokumenteeritakse täiustamise ja jälitatavuse eesmärgil. Tulemusi arvestatakse organisatsiooni protsesside täiustamisel.

11. E-ITS auditeerimine

11.1 E-ITS auditi eesmärk on hinnata, kas organisatsiooni infoturbe halduse süsteem ning selle raames rakendatud meetmed on vastavuses antud dokumendiga ning on piisavad organisatsiooni äriprotsesside kaitseks ja organisatsiooni eesmärkide täitmiseks

11.2 Infoturbe halduse süsteemi auditeerimine viiakse läbi vastavalt määruse lisas 3 toodud auditeerimiseeskirjale.

11.3 Infoturbe halduse süsteemi rakendatust auditeeritakse:

a) kohustuslikult – regulatsioonidest lähtuvalt või

b) lepingukohustuste täitmiseks või

c) vabatahtlikult – vastavalt organisatsiooni eesmärkidele ja infoturvapoliitikale.

11.4 E-ITS auditi järeldusotsus on tõend organisatsiooni infoturbe toimivuse kohta.