29.11.2023

Ettevõtlus- ja infotehnoloogiaministri 16. detsembri 2022. a määruse nr 101 „Eesti infoturbestandard“ muutmise määruse eelnõu seletuskiri

1. Sissejuhatus

Eelnõu eesmärk on kehtestada Eesti infoturbestandardi 2023. aasta versioon.

Eesti infoturbestandardi (edaspidi E-ITS) siht on:

- arendada ja edendada Eesti avaliku sektori asutuste ning erafirmade infoturbe taset;
- esitada eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks, mis ühtlasi vastab rahvusvahelisele standardile ISO/IEC 27001.[1]

E-ITS esitab etalonturbe rakendamise süsteemi, mis aitab organisatsioonil saavutada tema vajadustega sobivat infoturbe taset.

Organisatsiooni juhtkond ise otsustab, milliseid objekte ja protsesse on tarvis kaitsta. Etalonturve seab kaitstavad objektid ja protsessid vastavusse etalonturbe kataloogi tüüpmoodulitega. Etalonturbe kataloogis esitatud tüüpmoodulid kirjeldavad tüüpilisi ohte ja neile vastavaid, riskianalüüsi põhjal valitud turvameetmeid. Turvameetmete rakendamine vähendab infoturbeohtude realiseerumise tõenäosust. Etalonturve võimaldab organisatsioonil taaskasutada infoturbe parimaid praktikaid ja seeläbi kokku hoida infoturbe rakendamisele kuluvaid vahendeid.

E-ITS põhineb Saksa etalonturbe süsteemil BSI IT-Grundschutz (BSIG) ja standardil EVS-ISO/IEC 27001:2014 „INFOTEHNOLOOGIA. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded“.[2]

Ettevõtlus- ja infotehnoloogiaministri 16. detsembri 2022 a. määruse nr 101 „Eesti infoturbestandard“ (edaspidi *kehtiv määrus*) jõustumisega võeti vastu E-ITSi 2022. a versioon. Siinse eelnõuga võetakse vastu E-ITSi 2023. a versioon, milles on tehtud mitmesuguseid täiendusi ja lisandusi. Nende tegemisel lähtuti kasutajate tagasisidest, vajadusest ühtlustada (kõik) asjakohased dokumendid, uute meetmete ja moodulite lisamisest ning muutustest küberturvalisuse ohupildis. Lähtudes kasutusmugavusest ja praktilisest rakendamisest on eemaldatud meetmeid ja mooduleid, samuti neid, mis on aegunud. Lisaks tehti tehnilisi muudatusi (pealkirjade sõnastuste muutmine, viitamis- ja kirjavigade parandamine jne).

Määruse eelnõu ja seletuskirja koostas Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@mkm.ee) koos Riigi Infosüsteemi Ameti riigi infoturbe meetmete osakonnaga.

[1] Koostajad on Rahvusvaheline Standardiorganisatsioon (ingl International Organization for Standardization, ISO) ja Rahvusvaheline Elektrotehnikakomisjon (ingl International Electrotechnical Commission, IEC). Standardi 2017. a versiooni leiab ja seda on võimalik osta aadressilt https://www.evs.ee/et/evs-en-iso-iec-27001-2017 ning standardi 2023. a versiooni leiab aadressilt https://www.evs.ee/et/evs-en-iso-iec-27001-2023 (19.10.2023).

[2] E-ITSi portaali võrguleht. E-ITSi 2020. a versiooni lühijuhend: https://eits.ria.ee/et/versioon/2020vers1/juhendid/luehijuhend/ punkt 1 (19.10.2023).

Eelnõu ja seletuskirja kohta tegi õiguslikke ettepanekuid Majandus- ja Kommunikatsiooniministeeriumi õigusosakonna õigusnõunik Ragnar Kass (ragnar.kass@mkm.ee). Eelnõu ja seletuskirja keeletoimetas Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@mkm.ee) ja Justiitsministeeriumi õigusloome korralduse talituse toimetaja Airi Kapanen (airi.kapanen@mkm.ee).

E-ITS-i esimese versiooni (2020) ja sellega seotud dokumendid koostas KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti (edaspidi RIA) tellimusel ja Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine 2015–2023“ raames Euroopa Regionaalarengu Fondi rahastusel.[3]

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb neljast punktist, millega täiendatakse kehtivat määrust kolme lisaga, mis tervikuna moodustavad E-ITSi. Seletuskirjas selgitatakse ja analüüsitakse muudatusi, mida toob kaasa eelnõuga kehtestatav E-ITSi versioon (2023) võrreldes kehtiva määrusega kehtestatud versiooniga (2022).

Määruse volitusnormid on esitatud küberturvalisuse seaduse (KüTS) § 7 lõikes 5 ning sama lõike alusel antava Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (edaspidi *VV määrus*) § 3 lõikes 1. KüTS-i § 7 lõige 5 lisati seadusesse küberturvalisuse seaduse ja teiste seaduste muutmise seaduse eelnõu 531 SE (edaspidi *531 SE*) vastuvõtmise tulemusena.[4]

KüTS-i § 7 lõige 5 võimaldab Vabariigi Valitsusel või tema volitatud ministril kehtestada määrusega samas paragrahvis sätestatud kohustuste täitmise ning võrgu- ja infosüsteemide (edaspidi *süsteem*) küberturvalisuse tagamiseks:
1) infoturbe halduse nõuded, üldnimetusega Eesti infoturbestandard;
2) turvameetmete üldnõuded;
3) süsteemide turvameetmete erinõuded ja nende kohaldamise ulatuse.

VV määruse § 3 lõike 1 kohaselt kehtestab E-ITSi üleriigilise küberturvalisuse tagamise korraldamise eest vastutav minister määrusega. Eelnõu koostamise ajal on E-ITSi kehtestajaks majandus- ja infotehnoloogiaminister.[5] Lisaks Riigi Teatajale avaldab RIA E-ITSi sisu vastavas portaalis.[6]

Eelnõu 531 SE seletuskirjas (seaduseelnõu § 1 punkti 10 selgitused lk-del 14–15) on siinse eelnõuga kehtestatava määruse kohta selgitatud:
„Eelnõu lisaks olev kavandatav Vabariigi Valitsuse määrus annab üleriigilise küberturvalisuse tagamise korraldamise eest vastutavale ministrile (kelleks eelnõu koostamise hetkel on ettevõtlus- ja infotehnoloogiaminister) volituse kehtestada E-ITS (kui dokument ise) määrusega. Selleks sätestatakse eelnõu punktiga ka edasivolituse võimalus. E-ITS-i

[3] Lisainfo: https://ria.ee/infouhiskonna-teadlikkuse-tostmine-2015-2023 (22.11.2023).
[4] Riigikogu võrguleht. Küberturvalisuse seaduse ja teiste seaduste muutmise seadus 531 SE (29.11.2022); Riigi Teatajas avaldatud 05.08.2022, RT I, 06.08.2022, 2 (19.10.2023).
[5] Kuni 18. juulini 2022 ametis olnud Vabariigi Valitsuse 51. koosseisus oli üleriigilise küberturvalisuse tagamise korraldamise eest vastutava ministri nimetuseks „ettevõtlus- ja infotehnoloogiaminister“, kuid 18. juulil 2022 ametisse astunud Vabariigi Valitsuse 52. koosseisus on selle teema eest vastutava ministri nimetus „majandus- ja infotehnoloogiaminister“.
[6] E-ITSi portaal asub aadressil https://eits.ria.ee/ (19.10.2023).

kehtestamine on otstarbekam läbi viia edasivolituse alusel ministri määrusega, sest praktikas võimaldab ministri määruse kehtestamine vastavalt vajadusele dokumenti ajakohastada tulenevalt pidevalt muutuvast IKT raamistikust. See siiski ei tähenda, et teised osapooled (sh ministeeriumid jt asutused) ei saaks osaleda ning kaasa rääkida E-ITS-i sisu uuendamisel ja sisustamisel. Seaduseelnõus ei kasutata sõnastust „valdkonna eest vastutav minister", sest tulevikus võib tekkida vajadus kavandatavas Vabariigi Valitsuse määruses sätestada edasivolitust võimaldav norm erinevate valitsusalade ministritele, ning sellises olukorras valdkonna täpsustamata jätmine seaduseelnõus võib tekitada õigusselgusetust, et milline minister millise valdkonna eest vastutab. E-ITS kehtestamine käskkirjaga ei ole võimalik, kuivõrd E-ITS-i kehtestamine ei ole käsitletav üksikjuhtumi reguleerimisena. [….]

Vabariigi Valitsusele on ette nähtud võimalus määruse andmist edasi volitada kogu volitusnormi ulatuses. Jääb Vabariigi Valitsuse otsustada, kas volitatakse, ning kui jah, siis mis ulatuses käesolevas volitusnormis sätestatud nõuete kehtestamist ministrile edasi volitatakse.

Edasivolituse eesmärk on ministeeriumi valitsemisalade valdkondade korraldamise võimaldamine. Volitusnormi esimeses kahes lõikes tähendab see avaliku sektori digiarengu ja üleriigilise küberturvalisuse tagamise juhtimise, korraldamise ja järelevalve võimaldamist ning kolmandas lõikes ka iga valitsusala korraldamise võimaldamist, kui reguleerimisobjektiks on konkreetsele valitsusalale iseloomulike süsteemide pidamine.

Edasivolituse ulatuse samastamine volitusnormiga on vajalik seetõttu, et iga volitus võib hõlmata eriliigilisi regulatsioone, mis lähtuvalt oma eripärast peaksid olema reguleeritud Vabariigi Valitse tasandil või ministri määrusega. Näiteks, kui Vabariigi Valitsus kehtestaks määrusega turvameetmete üldnõude, siis tehnilisemad nõuded selle sisustamisel tuleks välja töötada ning koostada küberturvalisuse tagamise korraldamise valitsemisalas. Täiendavalt tuleneb selline edasivolituse ulatuse vajadus ka tehnoloogilise arenguga järjepidamise vajadusest. Täpsem edasivolituse defineerimine näiteks konkreetsete süsteemide või tehnoloogiate osas võib kiiresti infotehnilisel maastikul aeguda."

E-ITS on dokumentide kogum, mida on vaja pidevalt ajakohastada ja täiendada. Majandus- ja Kommunikatsiooniministeeriumi (edaspidi MKM) valitsemisala asutus RIA korraldab E-ITSi täiendamist ning uuendamist, võttes selle aluseks varasema rakendamise praktikat ning muutusi infotehnoloogilises maailmapildis ja õigusraamistikes. Uuendamine toimub iga aasta sügisel (teostab RIA, kuid määruse lisa(d) asendab või täiendab MKM).

E-ITSi portaalis on 2020. a versioonis (pole ametlikult määrusega kinnitatud) avaldatud E-ITSi lühijuhend, mille peatükkides 1, 3, 3.1 ja 3.2 on selgitatud E-ITSi olemust ja sisu.[7] Järgmised tekstid on väljavõtted nendest peatükkidest:

„1. Käsitlusala

Lühijuhend annab esmase ülevaate Eesti infoturbestandardist (E-ITS). Eesti infoturbe-standardi siht on arendada ning edendada Eesti avaliku sektori asutuste ja erafirmade infoturbe taset. Seni on samal otstarbel kasutusel olnud ISKE (infosüsteemide turvameetmete süsteem = infosüsteemide kolmeastmeline etalonturve).

[7] E-ITS-i portaali võrguleht. E-ITS-i 2020. a versiooni dokument „Lühijuhend": https://eits.ria.ee/et/versioon/2020vers1/juhendid/luehijuhend/ (19.10.2023).

E-ITS-i eesmärk on esitada eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks, mis ühtlasi vastaks standardile ISO/IEC 27001 (27001). E-ITS esitab etalonturbe rakendamise süsteemi, mis aitab organisatsioonil saavutada tema vajadustega sobivat infoturbe taset.

Organisatsiooni juhtkond ise otsustab, milliseid objekte ja protsesse on tarvis kaitsta. Etalonturve seab kaitstavad objektid ja protsessid vastavusse etalonturbe kataloogi tüüpmoodulitega. Etalonturbe kataloogis leiduvad tüüpmoodulid kirjeldavad tüüpilisi ohte ja neile vastavaid, riskianalüüsi põhjal valitud turvameetmeid. Turvameetmete rakendamine vähendab infoturbeohtude realiseerumise tõenäosust. Etalonturve võimaldab organisatsioonil taaskasutada infoturbe parimaid praktikaid ning seeläbi kokku hoida infoturbe rakendamisele kuluvaid vahendeid.

Standard põhineb Saksa etalonturbe süsteemil BSI IT-Grundschutz (BSIG) ja standardil EVS-ISO/IEC 27001:2014 „INFOTEHNOLOOGIA. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded" (27001).

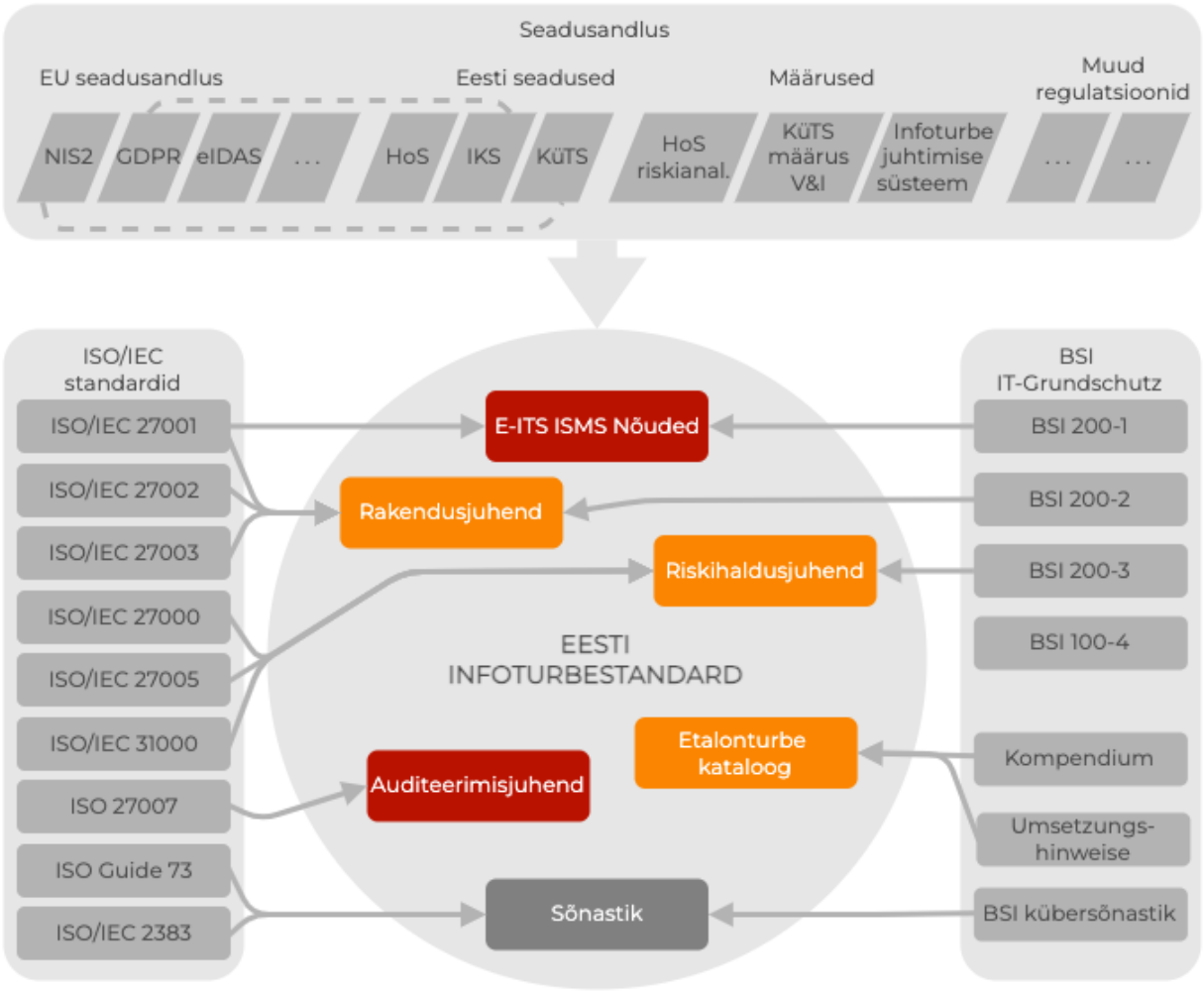
[---]

3. Infoturbe korraldamine E-ITSi alusel

E-ITS esitab infoturbe korraldamise parimad teadaolevad viisid. Standardi omanik on Riigi Infosüsteemi Amet. Standard tugineb seadusandlusele. E-ITSi ökosüsteemi oluliseks osaks on audiitorite kogukond, kes hakkab tuvastama organisatsioonide infoturbehalduse süsteemide vastavust standardi nõuetega.

Joonis 1 selgitab E-ITS olulisimate dokumentide suhtestumist Eestis kehtivate seaduste ja üldtuntud infoturbestandarditega.[8]

[8] Eelnõu koostaja märkus: E-ITSi 2020. a versiooni lühijuhendis on see joonis 2, kuid siinses eelnõus on tegemist esimese joonisega, mistõttu on seletuskirjas märgitud joonise numbriks 1. Võrreldes E-ITSi 2020. a versioonis esitatud joonisega on siinsel joonisel järgmised muudatused: 1) E-ITSi mullist on eemaldatud lahter „Üleminekujuhend" ja 2) paremal asuvas Saksa etalonturbe süsteemi BSI IT-Grundschutz tulbas on nelja alumise alamtulba asetust muudetud, kuid joonise põhisisu on jäänud samaks.



Joonis 1. E-ITSi võtmedokumentide suhtestumine oluliste mõjutajatega

E-ITS seob ühtsesse tervikusse järgmised turbeprintsiibid, -tehnoloogiad ja kontrollimehhanismid:

- *riskihaldus, lähtumine võimalikust kahjust, kahju vältimine. Kui tuvastati ohud, mida etalonturve hallata ei suuda, suunab E-ITS kasutaja vahetu riskihalduse protseduuri juurde;*
- *infoturbe halduse süsteem (*ingl *ISMS – **I**nformation **S**ecurity **M**anagement **S**ystem) muutuste avastamiseks ja infoturbe jätkusuutlikkuse tagamiseks;*
- *etalonturve – alusohtude tõrjumiseks riskianalüüsi tulemusel leitud tüüpsed meetmed, mis on mugavalt pakendatud ja rakendajale kasutusvalmis;*
- *auditeerimine ja sertifitseerimine – infoturbekohuslasele on väline vastavusaudit kohustuslik, sertifitseerimine standardi ISO/IEC 27001 suhtes on vabatahtlik ning asendab vastavusauditit.*

3.1. Eesti infoturbestandardi põhimõtted

E-ITS eeldab, et organisatsioon käsitleb infoturvet läbi äriprotsesside prisma. Toimiva infoturbe eeldusena peab organisatsioon olema teadlik oma eesmärkidest, põhikirjalistest

ülesannetest jms ning suutma kirjeldada oma toimimise valdkondi läbi äriprotsesside [, mille tulemusel saab organisatsioon pakkuda oma äritegevuse eesmärkidest tulenevaid tooteid või teenuseid].[9] *Infoturbe ülesanne organisatsioonis on säilitada äriprotsesside käigus töödeldava teabe turvalisus. Infoturbe konkreetsed eesmärgid on seejuures vastavuses organisatsiooni tegevuse eesmärkidega.*

Infoturve on pidevalt toimiv protsess, mitte ühekordne tegevus. Infoturve lähtub organisatsiooni eesmärkidest ja selle olulistest äriprotsessidest. Infoturbe tehnilised elemendid saab vajadusel sisse osta, kuid täpne arusaam organisatsiooni äriprotsessidest, nende tähtsusest ning kogu tegevuse eesmärkidest on ainult organisatsiooni juhtkonnal. See paneb juhtkonnale erilised ootused teadlikkuse, otsuste ja vastutuse osas.

Infoturve on tippjuhi vastutusalas, sest tippjuht näeb organisatsiooni tervikuna ning mõistab, mis võib äriprotsesse ohustada. Tippjuht teeb infoturbeprotsesse otseselt mõjutavad otsused turbeks vajalike ressursside jaotamise ning riskide aktsepteerimise kohta.

Infoturbe protsessi käivitamisele eelneb juhtkonna poolne kohustumus – avaldus, millega juhtkond võtab vastutuse infoturbe elluviimise eest organisatsioonis ning mille toel näitab ta edaspidi eeskuju kõigile töötajatele. Infoturve kaitseb organisatsiooni ohtude eest üksnes juhul, kui ta on loomuliku osana integreeritud äriprotsessidesse. Infoturbe nõuetega peavad kursis olema ning neid oma töös arvestama kõik töötajad.

Infoturve vajab pidevat uuendamist, sest ohud muutuvad ja teisenevad ajas. Infoturbe jätkusuutlikkuse tagamiseks näeb E-ITS ette, et organisatsioonis rakendatakse infoturbe halduse süsteem. Infoturbe seis organisatsioonis vajab pidevat parandamist, kavakindlat juhtimist ja jätkusuutlikku haldust selleks, et

- *mõista organisatsiooni tööprotseduure ja avastada neis ebaturvalisi kohti;*
- *täita seaduste ja standardite nõuded;*
- *seista vastu pidevalt teisenevatele küberohtudele.*

E-ITSi aluspõhimõtteks on riskihaldus. Et vältida kahju, mida ohud realiseerudes äriprotsessile võivad tekitada, peab organisatsioon oma riskid arvele võtma ja neid haldama. Standard on riskihalduse teinud kättesaadavaks ja mugavaks ka väikesele organisatsioonile.

E-ITSi turbemeetodiks on etalonturve [koos riskihaldusega].[10] *See tähendab, et tüüpjuhtude riskianalüüs on juba ette kestkselt ära tehtud standardi koostaja poolt. Riskide vähendamiseks pakutakse standardi rakendajale valmis tüüpmeetmed, mis paiknevad etalonturbe kataloogis. [Osale, kus tüüpseid varasid pole või kaitsetarve suur või väga suur, tuleb teha lisaks veel eraldi riskide analüüs.]*[11]

<u>3.2. Kasu E-ITSi rakendamisest</u>

E-ITSi rakendamine organisatsioonis toob kaasa infoturbekulutuste optimeerimise ning mitmed kaasnevad eelised.

- *Eesti avaliku sektori kõigi asutuste infoturve on ühtlaselt kõrgel tasemel (üks kõigi, kõik ühe eest), mis omakorda toetab e-riigi turvalist toimimist.*

[9] Eelnõu koostaja märkus: nurksulgudes olev tekst on lisatud siinse seletuskirja jaoks, kuid see ei asu E-ITSi 2020. a versiooni lühijuhendis.
[10] Vt eelmist allmärkust.
[11] Vt allmärkust 9.

- *Organisatsioon suudab kiiresti arenevas infoühiskonnas omi ülesandeid täita ja end globaalsete välisohtude eest kaitsta.*
- *Organisatsioon on halvimaks valmistunud. On tagatud organisatsiooni tegevuse jätkuvus. Läbi on mõeldud organisatsiooni ja selle töötajate kaitse küberohtude eest.*
- *Kui infoturve on hästi korraldatud, siis saab organisatsioon keskenduda oma põhitegevusele ning pole karta ootamatuid ründeid, sanktsioone ega trahve.*
- *Organisatsioon saavutab eelise ning parema maine omalaadsete organisatsioonide seas (olen naabrist parem).*
- *Organisatsioon saab oma turvalisust ning jätkusuutlikkust tõendada ka klientidele ja partneritele.*

Läbimõeldud ja jätkusuutlik infoturbeprotsess tagab seega organisatsiooni teenuste jätkuvuse ning hea maine. Infoturbe kõrge tase võib olla omakorda eelduseks rahastuse hankimisel projektidele (näiteks struktuurifondidest või hangetes).

Etalonturve võimaldab organisatsioonil taaskasutada infoturbe parimaid praktikaid ning seeläbi kokku hoida infoturbe rakendamisele kuluvaid vahendeid.".

Eelnõu esimese punktiga jäetakse kehtiva määruse lõikest 1 välja sõnad „käesoleva määruse lisas esitatud". Muudatus on seotud eelnõu ülejäänud punktidega, kuna muudetava lõike sõnastus sisustab, et E-ITS on kehtiva määruse puhul ühes lisas, kuid eelnõu tulemusel on määrusel mitu lisa. Kehtiva määruse lisas on eraldi esitatud sissejuhatav esileht, milles on märgitud E-ITSi ja selle sisudokumendid koos nende sisukordadega.

Eelnõu teise punktiga sisustatakse, millistest osadest koosneb E-ITS. Muudatuse tulemusena on määruse tasandil selgem loetelu, millised dokumendid on E-ITSi kui ühe terviku osad.

Kehtival määrusel on üks lisa nimetusega „Eesti infoturbestandard", mis omakorda sisaldab E-ITSi 2022. a versiooni järgmisi dokumente: (1) Infoturbe halduse süsteem. Nõuded; (2) rakendusjuhend; (3) etalonturbe kataloog; (4) auditeerimisjuhend.

Eelnõu tulemusena ei kehtestata võrreldes 2022. a versiooniga rakendusjuhendit, kuna selles olevad vajalikud osad on viidud eelnõu lisasse 1. Rakendusjuhend jääb edaspidi juhendi staatusega dokumendiks, mis on leitav E-ITSi portaalist. Samas portaalis on ka lisadokumendid, sh selgitavad juhendid, koolituste info, näidised, kogemuslood ja rubriik „Korduma kippuvad küsimused", mida siinses seletuskirjas ei hakata eraldi nimetama ega selgitama.

Versiooni nimi vastab lisade koostamise ja kinnitamise aastale. Edaspidi uuendatakse E-ITSi versiooni nii, et asendatakse määruse lisad.

Käesoleva määruse lisadeks saab E-ITSi 2023. a versioon, millega seotud dokumendid (osad) on järgmised:
1) nõuded infoturbe halduse süsteemile – asub eelnõu lisas 1;
2) etalonturbe kataloog – asub eelnõu lisas 2;
3) auditeerimisjuhend – asub eelnõu lisas 3.

Määrusega kehtestatava E-ITSi versiooni (2023) muutmise lugu võrreldes kehtiva määruse E-ITS versiooniga (2022) on leitav E-ITSi portaalist.[12] Muudatuste tegemisel lähtuti kasutajate tagasisidest, vajadusest ühtlustada (kõik) asjakohased dokumendid, uute meetmete ja moodulite lisandumisest ning küberturvalisuse ohupildi muutumist. Lähtudes kasutusmugavusest ja praktilisest rakendamisest on eemaldatud meetmeid ja mooduleid, samuti neid, mis on aegunud. E-ITSi rakendamise sisulises mõttes muudatusi ei ole tehtud.

Järgnevas tuuakse esile, mida on igas lisas muudetud.

Lisa 1 – nõuded infoturbe halduse süsteemile

Esimene muudatus on pealkirjas – kehtiva määruse lisas on selle siinse osa pealkirjaks „Infoturbe halduse süsteem. Nõuded“, ent siinse lisa pealkirja muudeti, et pealkirjas ei oleks punkti. Sel põhjusel tehti ka muudatused punktides 1.1 ja 10.2.

Muud muudatused:
- esitati selge seos, et E-ITS pole ainult etalonturve, vaid on lõimitud välise riskihaldusega (punktid 4, 6.7.5, 7 (tervikuna), 9);
- kaitsetarbe tähenduses täpsustati, et kaitsetarve on riskihalduse metoodika osa ja et kahjustsenaariumite ja skaala täpsustamine on organisatsiooni ülesanne (punktid 2 ja 7);
- lisatud termin *meetme teostatuse määr* (punkt 2);
- kustutatud üksiknõudena *infoturbeprotsessi algatamise dokumenteerimine*, selle asemel on loodud seos infoturbejuhi nimetamisega (punkt 5.1);
- E-ITSi ja ISO/IEC 27001 vahelise suhte täpsustamine ja kogu nõuete dokumendi ulatuses keskendumine vaid E-ITS-ile; ISO/IEC 27001 teemasid käsitletakse KüTSi tasandil, siin dokumendis iseloomustatakse vaid nendevahelist suhet (punkt 4 (täpsustatud koos lisaselgitusega), punkt 11.2 (kustutatud));
- toome märksõna „tippjuhtkond“ eraldi esile kui struktuuris kõige kõrgema juhtkonna rolli, kes infoturbe halduse eestvedamise ja toimimise eest vastutab (punktid 5 ja 5.1);
- varade ja sihtobjektide selgem kasutus paralleelselt, et neid saaks vajaduse korral eristada (enamasti on *varad* ja *sihtobjektid* kasutusel sünonüümidena, kuid definitsiooni alusel on võimalik äriprotsesside osad varad jätta kaitsealast välja ja sel juhul nad pole ka sihtobjektid, millele infoturvameetmeid rakendada) (punkt 6.2 ja kogu punkt 7);
- infoturvapoliitika väärtuste nimekirja kohandamine soovituslike kahjustsenaariumitega (punkt 6.1);
- infoturvapoliitika elementide joonise ja infoturbe eesmärkide olemuse täpsustamine kooskõlas ISMSi mooduliga (joonis 2 punktis 6.1);
- infoturvaeesmärkide kirjelduse lihtsustamine ja parem kooskõla etalonturbe kataloogi ISMS mooduliga (punkt 6.2);
- infoturbe komponentides selgem nõue vaid C-I-A osale (punkt 6.2);
- koolitusse lisatud eraldi nõue intsidendi käsitluseks (punkt 6.4);
- riskihaldusse lisatud kaitsetarbe määramise kohustus väljast tellitavatele teenustele (tarneahel) (punkt 7.1);

[12] E-ITSi portaali võrguleht. E-ITSi etalonturbe kataloogi 2023. aasta kavandi muutmise lugu: https://eits.ria.ee/et/versioon/2022/muutelugu/#eitsietalonturbekataloogi2023aastakavandimuutelugu1;
E-ITSi 2022. a versiooni pisiparandused (nendega on arvestatud 2023. a versioonis): https://eits.ria.ee/et/versioon/2022/muutelugu/versiooni-pisiparandused/;
uue versiooni kavandid: https://eits.ria.ee/et/versioon/2022/muutelugu/uue-versiooni-kavandid/ (kõik 19.10.2023).

- sihtobjekt riskihaldusse lülitamise kohustus, kui sellest sõltub samaaegselt mitu äriprotsessi (punkt 7.3);
- meetmete rakendamise täpsustamine kooskõlas auditijuhendiga (punkt 8);
- sõltumatu läbivaatuse puhul on sõnaselgelt esile toodud, et selleks ei pea olema audiitor, vaid võib olla ka pädev, kuid läbivaatusobjektist sõltumatu töötaja (punkt 10.2);
- jaotiste jooniste numeratsiooni muutused ja pisiparandused, mis sisu ei muuda, sh ka jaotiste pealkirjade loogiline struktuur (punkt 2, punktist 1.4 on joonis jäetud välja (asub standardis), punktid 4.1, 5, 5.1, 6, 6.1, 6.2, 7–10, 10.1);
- lisatud kohustusliku osa lõikude numeratsioon.

Lisa 2 – etalonturbe kataloog

ISMS. Turbehaldus

- muudatus moodulis ISMS.1 Turbehaldus
  - kirjelduses on muudetud viidet määruse lisa 1 pealkirjale;
  - lisateabes on asendatud Vabariigi Valitsuse määruse link.

ORP. Organisatsioon ja personal

- muudatused moodulis ORP.1 Infoturbe korraldus:
  - muudetud eesmärki ja vastutajaid;
  - täiendatud ohtu 2.3;
  - muudetud meetmeid ORP.1.M1, ORP.1.M4 ja ORP.1.M13;
  - lisatud uus meede ORP.1.M17 Nutitelefonide kaasas kandmise piiramine.
- muudatused moodulis ORP.2 Personal:
  - muudetud meedet ORP.2.M2;
- muudatused moodulis ORP.3 Infoturbe teadlikkuse tõstmine ja koolitus:
  - muudetud meetmeid: ORP.3.M1, ORP.3.M3 ja ORP.3.M8.

CON. Kontseptsioonid ja metoodikad

- muudatused moodulis CON.1 Krüptokontseptsioon:
  - muudetud piiranguid;
  - muudetud kõiki ohtusid;
  - muudetud lisamaterjale;
  - kustutatud järgmised meetmed: CON.1.M3, CON.1.M6, CON.1.M7, CON.1.M8, CON.1.M12, CON.1.M13 ja CON.1.M14;
  - lisatud järgmised meetmed: CON.1.M19 ja CON.1.M20;
  - muudetud järgmised meetmed: CON.1.M1, CON.1.M2, CON.1.M4, CON.1.M5, CON.1.M9, CON.1.M10, CON.1.M11, CON.1.M15, CON.1.M16, CON.1.M17 ja CON.1.M18;
- lisatud moodul CON.2 Isikuandmete kaitse;
- muudatused moodulis CON.6 Andmete kustutus ja hävitamine:
  - muudetud meedet CON.6.M11.

OPS. Käidutööd

- lisatud uus moodul OPS.1.1.1 IT-haldus.
- muudatused moodulis OPS.1.1.2 IT-süsteemide haldus:
  - muudetud mooduli nime, eesmärki, piiranguid, ohte ja elutsüklit;
  - eemaldatud meetmed: OPS.1.1.2.M3, OPS.1.1.2.M9, OPS.1.1.2.M10, OPS.1.1.2.M12, OPS.1.1.2.M14, OPS.1.1.2.M15 ja OPS.1.1.2.M20;

- lisatud meetmed: OPS.1.1.2.M21, OPS.1.1.2.M22, OPS.1.1.2.M23, OPS.1.1.2.M24, OPS.1.1.2.M25, OPS.1.1.2.M26, OPS.1.1.2.M27, OPS.1.1.2.M28, OPS.1.1.2.M29 ja OPS.1.1.2.M30;
- muudetud meetmed: OPS.1.1.2.M2, OPS.1.1.2.M5, OPS.1.1.2.M16 (K => S), OPS.1.1.2.M11, OPS.1.1.2.M17 ja OPS.1.1.2.M19.

- muudatused moodulis OPS.1.1.3 Paiga- ja muudatusehaldus:
  - muudetud punkti 1.3 Piirangud;
  - eemaldatud meede OPS.1.1.3.M16 Turvanõrkuste ja turvauuendite teabe seire;
  - muudetud meede OPS.1.1.3.M15 IT-süsteemide regulaarne uuendamine.
- muudatused moodulis OPS.1.1.5 Logimine:
  - lisatud Eesti meede OPS.1.1.5.ME1 Logide räsiaheldamine.
- muudatused moodulis OPS.1.1.7 Süsteemihaldus:
  - muudetud mooduli punkte 1.1 Eesmärk ja 1.3 Piirangud.
- muudatused moodulis OPS.1.2.5 Kaughooldus:
  - muudetud mooduli punkte 1.1 Eesmärk ja 1.3 Piirangud;
  - muudetud meetme nimi OPS.1.2.5.M10 Kaughooldustööriistade turvaline kasutamine;
  - muudetud meedet OPS.1.2.5.M14 Kaughoolduskliendi turvaline seadistus.
- kustutatud moodul OPS.2.1 Väljasttellimine.
- muudatused moodulis OPS.2.2 Pilvteenuste kasutamine:
  - muudetud meetmeid OPS.2.2.M1 ja OPS.2.2.M12;
  - lisateabest kustutatud aegunud juhend;
  - lisatud uus moodul OPS.2.3 Väljasttellimine;
  - kustutatud moodul OPS.3.1 Teenusandja infoturve;
  - lisatud uus moodul OPS.3.2 Teenuseandja infoturve.

APP. Rakendused

- muudatused moodulis APP.1.2 Veebibrauser:
  - muudetud APP.1.2.M9 ja APP.1.2.M13.
- muudatused moodulis APP.2.1 Kataloogiteenus üldiselt:
  - muudetud piiranguid ja ohte;
  - kustutatud meetmed APP.2.1.M4 ja APP.2.1.M7;
  - lisatud meetmed APP.2.1.M17 Kaitsevajadusega pääsuteabe turve, APP.2.1.M18 Kataloogiteenuse dubleerimine, APP.2.1.M19 Kataloogiteenuse anonüümse juurdepääsu haldus, APP.2.1.M20 Kataloogiteenuse dubleerimise turve, ja APP.2.1.M21 Kataloogiteenuse kõrgkäideldavuse tagamine;
  - muudetud meetmeid: APP.2.1.M1, APP.2.1.M2, APP.2.1.M8, APP.2.1.M9, APP.2.1.M11 ja APP.2.1.M14.
- muudatused moodulis APP.2.2 Active Directory Domain Services:
  - muudetud mooduli nimi;
  - muudetud piiranguid ja ohte;
  - kustutatud meetmed: APP.2.2.M2, APP.2.2.M10 ja APP.2.2.M14;
  - lisatud meetmed:
    APP.2.2.M16 AD DS kontode tugevdamine,
    APP.2.2.M17 AD metsa halduskontode kasutamise piiramine,
    APP.2.2.M18 AD arvutiobjektide domeeni lisamise piiramine,
    APP.2.2.M19 Virtualiseeritud domeenikontrollerite turvaline kasutamine,
    APP.2.2.M20 Organisatsiooniüksuste segmentimine,
    APP.2.2.M21 Mitmekihiline AD DS struktuurimudel,
    APP.2.2.M22 Halduskontode kasutuse ajaline piiramine,

APP.2.2.M23 Pääsuõiguste ja võimalike ründevektorite regulaarne analüüs;
  - muudetud meetmed: APP.2.2.M1, APP.2.2.M3, APP.2.2.M5, APP.2.2.M6, APP.2.2.M7, APP.2.2.M8, APP.2.2.M9, APP.2.2.M12 ja APP.2.2.M15;
  - lisatud lisamaterjale.
- muudatused moodulis APP.2.3 OpenLDAP:
  - muudetud piiranguid ja ohte;
  - muudetud meetmeid: APP.2.3.M6, APP.2.3.M9, APP.2.2.M10 ja APP.2.2.M11.
- muudatused moodulis APP.5.3 E-posti server ja klient üldiselt:
  - muudetud mooduli eesmärki;
  - muudetud meetmeid: APP.5.3.M2, APP.5.3.M6, APP.5.3.M9 ja APP.5.3.M10.
- pisimuudatused:
  - APP.3.2 piirangud;
  - APP.4.3 piirangud;
  - muudetud meedet APP.3.1.M4;
  - muudetud meedet APP.3.2.M12;
  - muudetud meedet APP.4.3.M1;
  - muudetud meedet APP.5.3.M7;
  - muudetud meedet APP.EE.1.M20.
- lisatud uus moodul: APP.5.4 Ühendatud side- ja koostöölahendused (UCC).

SYS. IT-süsteemid

- muudatused moodulis SYS.1.1 Server üldiselt:
  - muudetud piiranguid;
  - lisatud ohte;
  - lisatud meede SYS.1.1.M39 Serveri turvaseadete keskne haldus;
  - muudetud meetmeid SYS.1.1.M1, SYS.1.1.M6, SYS.1.1.M11 ja SYS.1.1.M16.
- muudatused moodulis SYS.1.6 Konteinerdus:
  - muudetud meedet SYS.1.6.M2;
  - lisatud uus moodul SYS.1.9 Terminaliserver;
  - lisatud uus moodul SYS.1.2.3 Windows Server.
- muudatused moodulis SYS.2.1 Klientarvuti üldiselt:
  - muudetud meetmeid SYS.2.1.M1 ja SYS.2.1.M11;
  - kustutatud meede SYS.2.1.M14.
- muudatused moodulis SYS.2.2.3 Windows kliendid:
  - moodul ümbernimetatud „SYS.2.2.3 Windows 10 ja Windows 11“;
  - muudetud eesmärki, piiranguid, vastutajaid, ohtusid;
  - muudetud meetmeid SYS.2.2.3.M1, SYS.2.2.3.M2, SYS.2.2.3.M4, SYS.2.2.3.M5, SYS.2.2.3.M13, SYS.2.2.3.M15, SYS.2.2.3.M16, SYS.2.2.3.M19, SYS.2.2.3.M21, SYS.2.2.3.M22, SYS.2.2.3.M23 ja SYS.2.2.3.M25;
  - lisatud meede SYS.2.2.3.M26 VSM (Virtual Secure Mode) kasutamine.
- muudatused moodulis SYS.2.3 Linuxi ja Unixi klient:
  - muudetud meetmeid SYS.2.3.M8 ja SYS.2.3.M14.
- muudatused moodulis SYS.4.3 Sardsüsteemid (*embedded systems*):
  - muudetud meetmeid SYS.4.3.M1, SYS.4.3.M2, SYS.4.3.M5 ja SYS.4.3.M11.
- muudatused moodulis SYS.4.5 Irdandmekandjad:
  - muudetud meetmed: SYS.4.5.M2, SYS.4.5.M4, SYS.4.5.M13 ja SYS.4.5.M15;
  - lisatud meede SYS.4.5.M17 Andmete pikaajaline säilitamine irdandmekandjal;
  - lisatud uus moodul SYS.EE.2 eID komponendid.

IND. Tööstuse IT

- muudatused moodulis IND.1 Käidu- ja protsessijuhtimissüsteemid:
  - muudetud meedet IND.1.M11 Turvaline hankimine ja süsteemiarendus;
- muudatused moodulis IND.3.2 Käidutehnoloogia komponentide kaughooldus;
  - 1.3 Piirangud;
  - 2.7 Kaughooldusla henduste ebaturvaline teostus;
  - muudetud meetmed: IND.3.2.M1, IND.3.2.M4, IND.3.2.M7 ja IND.3.2.M10.

NET. Võrgud ja side

- muudatused moodulis NET.1.1 Võrguarhitektuur ja lahendus:
  - muudetud meedet NET.1.1.M36.
- muudatused moodulis NET.2.1 Raadiokohtvõrgu käitamine:
  - muudetud meedet NET.2.1.M7;
  - lisatud uus moodul NET.3.4 Võrkupääsu reguleerimine (NAC).

INF. Taristu

- muudatused moodulis INF.1 Hoone üldiselt:
  - muudetud meedet INF.1.M9 Hoonete turbe programm.
- muudatused moodulis INF.2 Serveriruum ja andmekeskus:
  - muudetud meedet INF.2.M9 Tulekustutussüsteem ja kustutusvahendid.
- muudatused moodulis INF.6 Andmekandjate arhiiv:
  - muudetud meedet INF.6.M6.
- muudatused moodulis INF.10 Koosoleku-, ürituse- ja koolituseruumid:
  - kustutatud meede INF.10.M10 Mobiiltelefonide keeld.
- muudatused moodulis INF.11 Sõidukite IT-komponendid:
  - muudetud ohtu INF.11. oht 2.2;
  - meetmes INF.11.M2 kasutatakse sõna „autoriseerimine“ asemel „volitamine“.
- muudatused moodulis INF.13 Hoone tehniline haldus:
  - muudetud meede INF.13.M2 Vajalike pädevuste ja vastutajate määramine;
  - meetmes INF.13.M26 kasutatakse sõna „autoriseerimine“ asemel „volitamine“.
- muudatused moodulis INF.14 Hooneautomaatikasüsteemid:
  - muudetud meede INF.14 Hooneautomaatikasüsteemid ptk 1.3 Piirangud.

Lisa 3 – auditeerimisjuhend

Selles on muudetud jaotistes asuvate jooniste numeratsiooni ja tehtud pisiparandusi, mis sisu ei muuda, sh ka jaotiste pealkirjades.

- Auditeerimisjuhendis tehti muudatusi järgmistes peatükkides (nt viitamise parandused, ent ka muud pisiparandused, mis sisu ei muuda; vältimaks dubleerimist eemaldati terminid, mis on sisustatud siinse määruse lisas 1):
  - 1. Sissejuhatus
  - 2. Mõisted ja lühendid;
  - 3. E-ITSi auditi eesmärk;
  - 5. E-ITSi auditi eeldused;
  - 6. Auditi üldine korraldus;
  - 7. E-ITSi auditi tellimine;
  - 10. E-ITSi põhiaudit;
  - 11. E-ITSi vaheaudit;
  - 12. Lõpparuanne ja järeldusotsus;
  - 14. Seonduvad dokumendid.

- parandused Eesti Infosüsteemide Audiitorite Ühingult (edaspidi EISAÜ) saadud tagasiside põhjal (esitatud on viide peatükile või ala-punktile):
  - 3.1: täpsustati E-ITSi auditi eesmärki (lisatud vastavus dokumendile „Nõuded infoturbe halduse süsteemile“); „auditi edukas läbimine“ on asendatud parema arusaamise nimel „audiitori sõltumatu hinnanguga“;
  - 5.7: lisatud „ja plaanitavaid tegevusi“;
  - 10.4: rakendamist =>[13] rakendatust;
  - 10.10: turvalisus => infoturve; turvasertifikaat => turvameetmete rakendatust kinnitav sertifikaat;
  - 11.3.2: lisatud „kontrollitakse infoturbe meetmete rakendusplaani täitmist“;
  - 11.3.5: eemaldatud sõna „valimi“;
  - 14. Seonduvad dokumendid – lisatud viited EISAÜ IT-audiitorkontrolli eeskirjale ja eetikakoodeksile.

Eelnõu punktidega kolm ja neli tunnistatakse kehtetuks kehtiva määruse lisa (E-ITSi versioon 2022) ja kehtivat määrust täiendatakse eelnõu lisadega (E-ITSi 2023. a versiooniga). Eelnõu eelmiste punktide selgituste juures on selgitatud, miks on vaja kehtiva määruse üks lisa asendada mitme lisaga.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu ehk E-ITSi 2023. a versiooni kehtestamine ei ole seotud ega oma puutumust Euroopa Liidu õigusega. Euroopas on standardimine korraldatud vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) nr 1025/2012.[14] Selle määruse kohaselt on riiklik standard selline standard, mille on vastu võtnud riigi standardiorganisatsioon (Eesti puhul Eesti Standardimis- ja Akrediteerimiskeskus). Taoliste standardite puhul kohaldub toote nõuetele vastavuse seaduse[15] § 40. Samas pole E-ITSi standard määruse nr 1025/2012 ning toote nõuetele vastavuse seaduse tähenduses, vaid E-ITS on ühtsete nõuete kogum, mitte standardiorganisatsiooni kinnitatud dokument. Eestis on ka praegu juba standardiorganisatsiooni väliseid standardeid, mis on analoogselt kehtestatud määrusega.[16]

Seega on eelnõu kooskõlas Euroopa Liidu õigusega.

4. Määruse mõjud

Kuna eelnõu tulemusena E-ITSi sisu ja põhiolemus ei muutu, on siinses osas võimalik võrrelda ainult neid muudatusi, mis tehakse kehtiva määruse versiooni (2022) asendamisel siinse määruse lisades oleva versiooniga (2023).

---

[13] Sümbol => osutab pärast parandamist kasutatavale sõnale.

[14] Euroopa Parlamendi ja nõukogu määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ (19.10.2023).

[15] toote nõuetele vastavuse seadus, RT I, 03.02.2023, 11 (19.10.2023).

[16] Vt nt haridus- ja teadusministri 28.11.2008. a määrust nr 69 „Kutsestandardite koostamise, muutmise ja vormistamise kord“ (RTL 2008, 97, 1345), 19.06.2015. a määrust nr 27 „Täienduskoolituse standard“ (RT I, 11.11.2016, 2), 21.03.2007. a määrust nr 27 „Huviharidusstandard“ (RTL 2007, 27, 474) ning rahandusministri 13.12.2011. a määrust nr 57 „Siseaudiitori kutsetegevuse standardite kehtestamine“ (RT I, 21.04.2017, 13), (kõik 19.10.2023).

Ülevaatlikkuse huvides korratakse siinses tekstilõigus viiteid, mis olid ka kehtiva määruse seletuskirjas. Eelnõu 531 SE seletuskirjas (peatükk 6.1, lk-d 33–39) on analüüsitud E-ITSi kehtestamisega seotud mõjusid. Selles esitatud mõjude analüüs lähtus samadest mõjude liikidest, mis on nõutud hea õigusloome ja normitehnika eeskirja[17] § 65 lg 1 punkti 4 kohaselt. VV määruse eelnõu seletuskirjas (peatükk 5.1, lk-d 19–27) on sisuliselt korratud 531 SE mõjude analüüsi sisu ja teatavas osas on seda täiendatud. Kehtiva E-ITSi versiooni kehtestanud määruse seletuskirjas (lk 10) on samuti selgitatud kehtiva E-ITSi versiooniga seotud mõjusid.[18] Seetõttu eelmainitud analüüse käesolevas seletuskirjas ei korrata, kuid ka selles tehtud mõjude hindamine on teatavas ulatuses asjakohane ka E-ITSi 2023. a versiooni kehtestamisel.

Küberruumis tegutsevad E-ITSi rakendajad ühtemoodi nii Tallinnas, Narvas, kui ka Ruhnus ja nad on enamvähem sama ründevektoriga igalt poolt tabatavad. Seega, E-ITSis kui tervikus ei ole erandeid võimalik teha. Samas on E-ITS-i rakendamise ulatus ja maht paljuski seotud konkreetse E-ITS-i rakendaja põhitegevusega (näiteks tema osutatavad ülesanded või teenused), mille suhtes E-ITS-i rakendatakse. Sellest omakorda sõltub, mil määral on vaja teha muudatusi infoturbe halduse korralduses.

E-ITS võtab arvesse selle rakendajate küpsust meetmete rakendamisel ning meetmed on jagatud põhi-, standard- ja kõrgmeetmeteks.

- Kui tegu on organisatsioonidega, kus kaitsetarve on normaalne, ja varem pole infoturbega teadlikult tegeletud, siis esialgu vähendab põhiturbe rakendamine E-ITSi rakendamise koormust.
- Suurema kaitsetarbega organisatsioonidel on hädavajalik rakendada E-ITSi meetmeid vähemalt nende kaitseala osades, mille kohta kehtivad rangemad kaitsetarbe nõuded, valides nimetatud nõuetele vastavaid meetmeid ka standard- ja kõrgmeetmete hulgast.

Seejuures tuleb pidevalt lähtuda riskipõhisest mõtlemisest. Rakendamata meetmete suhtes on vajalik hinnata jääkriske kaitsetarbele. E-ITSi rakendamine aitab vähendada äririske, ent see pole eesmärk omaette.

E-ITSi 2023. a versiooni rakendamine nõuab mõningaid ressursse, kuid vajadus nende järele oleneb konkreetsest organisatsioonist, sh määratud kaitsetarbest ja sellest, kas tema suhtes on eelnõuga muudetud või lisanduvad meetmed üldse kohaldatavad. Nendesamade meetmete rakendamine omakorda aitab suurendada organisatsiooni küberturvalisuse taset ja toimepidevust ning võimaldab paremini hallata riske. Samuti on selle kõige tulemusena võimalik paremini tegeleda küberintsidentide haldusega, sh kohaste meetmete rakendamisel minimeerida võimalikke kahjulikke mõjusid nii enda organisatsioonile kui ka klientidele (kliendid kui inimesed või ettevõtjad ja asutused) ning teatavas ulatuses kogu ühiskonnale.

E-ITSi 2023. a versiooniga tutvumine võtab kindla aja, et uute või muudetud nõuetega tutvuda ja asjakohaste meetmete rakendamine ellu viia, st seada eesmärgiks asjakohaste meetmete rakendamine töösse panna ja ära teha. Samas, aegunud meetmed tuleb käibelt kõrvaldada. Selle kõige käigus tehtud tegevused ja kulud peaksid vähendama suurte kahjude tekkimise riski küberintsidentide korral.

Kuna E-ITSi 2023. a versiooni ehk määruse lisa 1 puhul pole muudetud sisulisi nõudeid, vaid nende esitamise vormi, et tagada lihtsam ja selgem arusaamine ja parem loetavus, seisneb

[17] Vabariigi Valitsuse 22. detsembri 2011. a määrus nr 180 „Hea õigusloome ja normitehnika eeskiri“, RT I, 29.12.2011, 228 (26.10.2023).
[18] E-ITSi 2022. a versiooni kehtestanud ministri määrus – leitav MKM-i avalikust dokumendiregistrist aadressil https://adr.rik.ee/mkm/dokument/13670130 (26.10.2023).

muudatuste mõju eelkõige selles, et dokument tuleb rakendajal uuesti läbi töötada ja veenduda, et kõigest on õigesti aru saadud. Uutel, tulevikus lisanduda võivatel rakendajatel peaks dokument olema tänu uuele versioonile paremini mõistetav. Kuna E-ITSi uues versioonis on punktid nummerdatud, on nõuete järgimisele parem viidata. Määruse lisas 2 tehtud muudatuste tõttu tuleb E-ITSi rakendajal ennekõike tutvuda uute meetmetega ja viia need ellu, sh vajaduse korral eemaldada vananenud meetmed, kui neid rohkem vaja ei lähe. Määruse lisa 3 puhul tuleb rakendajal see dokument uuesti läbi töötada, et oleks selge, millest lähtudes toimub auditeerimine. Kõigi kolme lisa puhul on abistavaks materjaliks nii E-ITS-i portaalis olev muuteloo info (vt allviidet 12) kui ka siinse seletuskirja 2. peatükis esile toodud muudatused.

4.1. Sotsiaalne, sealhulgas demograafiline mõju
E-ITSi meetmete ajakohastamine väldib aegunud meetmete rakendamist, järgib uut ohuolukorda ja sel on rakendajale pigem positiivne mõju, kuivõrd tal on teadmine, et tegeleb asjakohase, mitte vananenud standardiga.

4.2. Mõju riigi julgeolekule ja välissuhetele
E-ITSi meetmete regulaarne uuendamine tagab organisatsioonide infoturbe ajakohasena hoidmise ja parema toimetuleku äririskidega, mis on otseses sõltuvuses digitaalsetest vahenditest. E-ITS ja selle tegelik rakendamine organisatsioonides ning edusammude avalik kommunikeerimine toimib võimalikule ründajale heidutusmeetmena.

4.3. Mõju majandusele
E-ITSi meetmete (nii varem kehtestatud kui ka määrusega muudetud või lisanduvate meetmete) õige ja asjakohane rakendamine võib olulisel määral vähendada organisatsioonide võimalikku kahju intsidentide korral. Pikas perspektiivis annab standardiseeritud IT-haldus optimeerimisvõimalusi ja kokkuhoidu ning paremat planeerimisvõimet. Samas, uute meetmete rakendamise võib nõuda lisaressursse. Siinkohal on organisatsiooni otsus, kas potentsiaalse kahju ärahoidmine õigustab lisainvesteeringut nimetatud ressursidesse.

4.4. Mõju elu- ja looduskeskkonnale
Kui organisatsiooni ärieesmärgid mõjutavad elu- ja looduskeskkonda, võib E-ITSi meetmete õige ja asjakohane rakendamine olulisel määral vähendada organisatsioonide ärieesmärkide saavutamise võimalikku kahju intsidentide korral (nt elutähtsa teenuse osutajate korral).

4.5. Mõju regionaalarengule
Määrusega lisanduvad või muudetud nõuded on võrdsed kõigile E-ITSi rakendajatele.

4.6. Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele
Selgem infoturbe halduse korraldus toimib hästi koos teiste organisatsiooni juhtimissüsteemidega. Standardiseeritud süsteemi rakendamisel on positiivne mõju, kuna pikas perspektiivis optimeerib see töökorraldust, sest tegevusi ei tehta juhtumipõhiselt (*ad hoc*), vaid pigem plaani põhiselt konkreetse protsessina. Sellesse etappi aga jõuavad asutused, kui on saavutatud esmane infoturbe küpsus ja juhtkonna selge ja pidev eesvedu ja toetus.

Kokkuvõtteks, kõigi seletuskirja punktides 4.1–4.6 kirjeldatud mõjude puhul on nende ulatus väike, sagedus väike ja ebasoovitavate mõjude risk väike. Mõju pikas perspektiivis on pigem positiivne. Tegelik mõju lähtub organisatsioonist ja tema juhtimiskultuurist ning riskide haldusest. Seetõttu võib mõju organisatsiooniti ka erineda.

Käesoleva eelnõuga seni käsitlemata mõjusid ei kaasne.

5. Määruse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamise eeldatavad tulud

Kuna eelnõu tulemusena E-ITSi sisu ja põhiolemus ei muutu, siis on võimalik siinses osas võrrelda ainult neid muudatusi tegevustes, kuludes ja tuludes, mis toimuvad kehtivas määruses esitatud E-ITSi versiooni (2022) asendamisel siinse määruse lisades oleva versiooniga (2023).

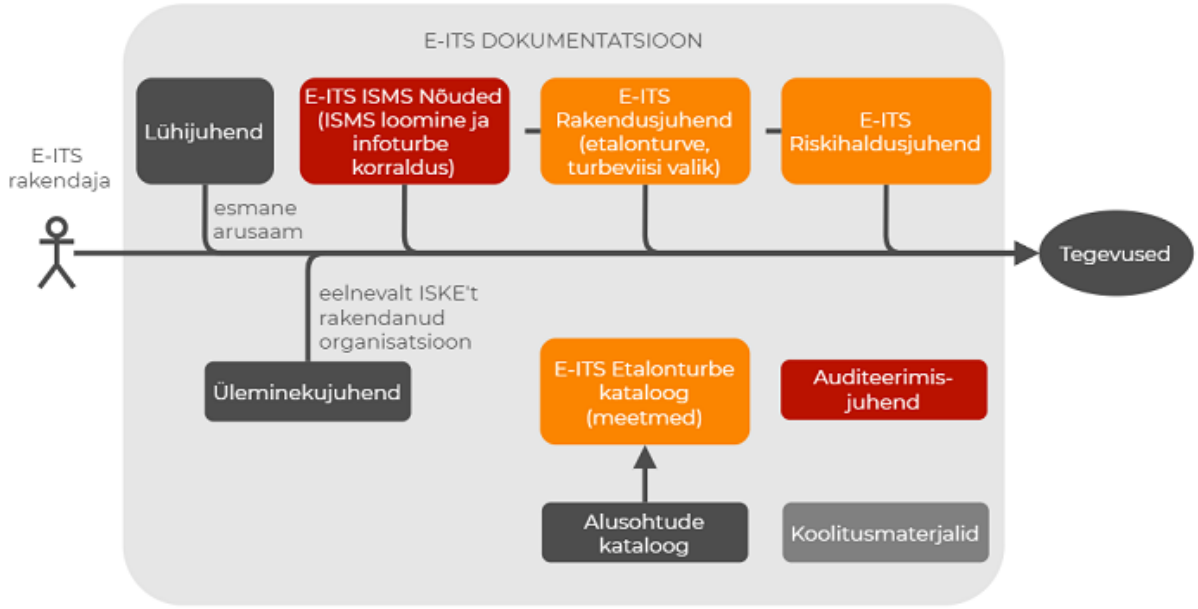
Ülevaatlikkuse huvides korratakse siinses tekstilõigus viiteid, mis olid ka kehtiva määruse seletuskirjas. Eelnõu 531 SE seletuskirjas (peatükk 7.1, lk-d 45–47) on analüüsitud neid riigi ja kohaliku omavalitsuse tegevusi, eeldatavaid kulusid ja tulusid, mis on seotud E-ITSi kehtestamisega. VV määruse eelnõu seletuskirjas (peatükk 6.1, lk-d 29–31) on korratud sisuliselt sama analüüsi, mis on 531 SE seletuskirjas, sh on teatavas osas seda ka täiendatud. Kehtiva E-ITSi versiooni kehtestanud määruse seletuskirjas (lk 10) on samamoodi selgitatud kehtiva E-ITSi versiooniga seotud mõjusid.[19] Seetõttu eelmainitud analüüse käesolevas seletuskirjas ei korrata, kuid neis tehtud mõjude hindamine on teatavas ulatuses asjakohane ka E-ITSi 2023. a versiooni kehtestamisel.

Tegevuste mõttes peab E-ITSi rakendaja hakkama tegelema E-ITSi uue versiooni rakendamisega ehk esmalt töötama läbi määrusega kehtestatava versiooni dokumendid. Selle töö puhul võib olla vajalik uurida nii E-ITS-i portaalis olevat muuteloo infot (vt allviidet 12) kui ka siinse seletuskirja 2. peatükki.

E-ITSi 2020. a versioonis olevas lühijuhendi 4. peatükis on esitatud joonis, kuidas E-ITSi kui terviku rakendamine ellu viia (siinses seletuskirjas joonis 2). Joonisel on ette näidatud soovitav liikumistee E-ITSi evitamisel ja dokumentidega tutvumisel. Punane värv tähistab kõrgema prioriteediga juhendmaterjale. Tollel joonisel esitatud pealkirjadele vastava sisu leiab siinse määrusega kehtestatava versiooni järgmistest lisadest:

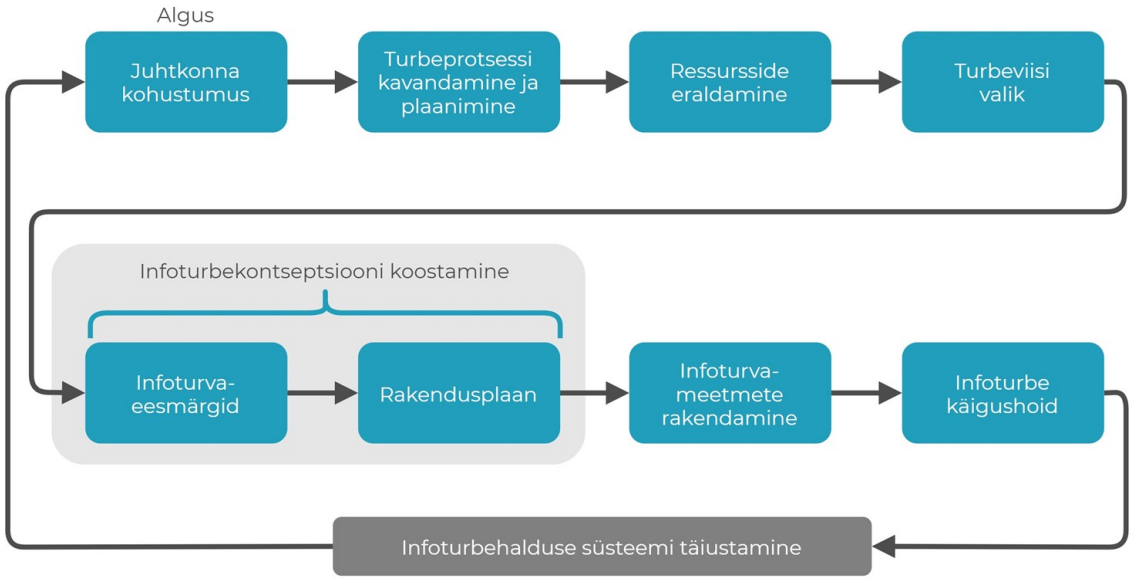
- „E-ITS ISMS Nõuded (ISMS loomine ja infoturbe korraldus)“ – lisa 1;
- „E-ITS Etalonturbe kataloog (meetmed) – lisa 2;
- „Auditeerimisjuhend“ – lisa 3.

[19] E-ITSi 2022. a versiooni kehtestanud ministri määrus – leitav MKM-i avalikust dokumendiregistrist: https://adr.rik.ee/mkm/dokument/13670130 (26.10.2023. a).



Joonis 2. E-ITSi juhendmaterjalidega tutvumise soovitatav järjestus[20]

Kehtiva määruse lisas olevas „Eesti infoturbestandard. Infoturbe halduse süsteem. Nõuded“ punktis 4.1 on esitatud joonis (tolles dokumendis numbriga 1) infoturbehalduse süsteemi protsesside ja sooritavate tegevuste kohta. Sama joonis asub ka käesoleva määruse lisa 1 punktis 4.1. Siinses seletuskirjas on see joonis 3. Siinse määrusega tehtavate muudatuste elluviimine toimubki sama protsessi järgides ehk alates sammust „Infoturbehalduse süsteemi täiustamine“ tegeletakse turbeprotsesside uuendamise kavandamise ja planeerimisega ning seejärel jätkatakse järgmiste sammudega.



Joonis 3. Infoturbehalduse süsteemi käivitamise ja uuendamise tegevused

[20] Eelnõu koostaja märkus: E-ITS-i 2020. a versiooni lühijuhendis on vastava joonise numbriks 5, kuid siinses eelnõus on tegemist teise joonisega, mistõttu on seletuskirjas märgitud joonise numbriks 2.

6. Määruse jõustumine

Määrus jõustub üldises korras.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitatakse kooskõlastamiseks eelnõude infosüsteemi kaudu kõikidele ministeeriumitele ning arvamuse avaldamiseks põhiseaduslikele institutsioonidele, avalik-õiguslikele juriidilistele isikutele, Andmekaitse Inspektsioonile, RIA-le, Keskkonnaministeeriumi Infotehnoloogiakeskusele, Registrite ja Infosüsteemide Keskusele, Riigi Info- ja Kommunikatsioonitehnoloogia Keskusele, Rahandusministeeriumi Infotehnoloogiakeskusele, Siseministeeriumi infotehnoloogia- ja arenduskeskusele, Tervise ja Heaolu Infosüsteemide Keskusele, Eesti Linnade ja Valdade Liidule, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule, Eesti Infosüsteemide Audiitorite Ühingule ning RIA vahendusel elutähtsa teenuse osutajatele ja olulise teenuse operaatoritele.