21.05.2026

Justiits- ja digiministri määruse „Eesti infoturbestandard“ eelnõu SELETUSKIRI

1. Sissejuhatus

1.1. Sisukokkuvõte

Eelnõukohase määrusega uuendatakse Eesti infoturbestandardit. Eesti infoturbestandardi (edaspidi *E-ITS*) siht on hoida ning edendada kübeturvalisuse seaduse subjektide ehk teenuseosutajate infoturvet. E-ITSis on esitatud nõuded, mis aitavad organisatsioonil saavutada oma vajadustega sobivat infoturbe taset, arvestades Eesti ja Euroopa Liidu õigusaktides sätestatut. Uuendatud E-ITS suurendab teenuseosutaja vastutust infoturbe eest ning vähendab riigipoolset keskset ettekirjutuste andmist. Muudatustega soovitakse edendada teenuseosutaja äriprotsessist lähtuvat infoturvet ja parandada nõuete arusaadavust. Nõuete detailsuse vähendamisega soovitakse anda nii teenuseosutajale kui ka riigile võimalus adekvaatsemalt ja kiiremalt reageerida uutele tehnoloogilistele lahendustele ja infoturvalisust ohustavatele sündmustele.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja ettevalmistamist ning koostamist on korraldanud Justiits- ja Digiministeeriumi riikliku küberturvalisuse talitus (riiklikkyber@justdigi.ee) koostöös Riigi Infosüsteemi Ametiga, lähtudes ameti ettepanekust. Vastutav ametnik on nimetatud talituse õigusnõunik Guido Pääsuke. Eelnõu ja seletuskirja on keeleliselt toimetanud Justiits- ja Digiministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse toimetaja Merike Koppel (merike.koppel@justdigi.ee).

1.3. Märkused

Eelnõu ei ole seotud ühegi teise menetluses oleva eelnõuga ega jõustunud seadusemuudatusega.

Eelnõu on kooskõlas Euroopa Parlamendi ja nõukogu 14. detsembri 2022. a direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (edaspidi *küberturvalisuse 2. direktiiv*), artikliga 21.

Eelnõukohase määrusega asendatakse ettevõtlus- ja infotehnoloogiaministri 16. detsembri 2022. a määrus nr 101 „Eesti infoturbestandard“ (RT I, 28.08.2025, 12) (edaspidi *määrus nr 101*).

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb 15 paragrahvist, mis on jaotatud nelja peatüki vahel järgmiselt:
1. peatükk – üldosa §-d 1 ja 2;
2. peatükk – infoturbe haldus §-d 3–9;
3. peatükk – seire §-d 10 ja 11;

4. peatükk – Eesti infoturbestandardi tugi ja rakendamine §-d 12–15.

E-ITS on osutunud tõhusaks abivahendiks Eesti turvalise digiühiskonna tagamisel ning aidanud kaasa IT-teadlikkuse kasvule. Määrusega nr 101 kehtestatud E-ITS on mahukas õigusakt, mis on tekitanud palju küsimusi selle rakendamise kohta, sealhulgas meetmete kohaldatavuse ja ulatuse kohta. Kehtivas määruses on meetmed põhjalikult rakendajatele lahti kirjutatud, mille tõttu on õigusloomeprotsess osutunud takistuseks kiirele reageerimisele uutele riskidele ning tehniliste lahenduste kasutuselevõtmisele. See tähendab, et mõned nõuded aeguvad kiiremini, kui neid kehtestada jõutakse. Praktikutelt saadud tagasisidest lähtuvalt on eelnõus võrreldes E-ITSi kehtiva versiooniga vähendatud soovitatavate meetmete, riski ulatuse ja infotehnoloogia (edaspidi *IT*) vahendite või neid toetava taristuga seotud ohtude, riskide ja vastumeetmete põhist ette kirjutamist. Eelnõukohase määrusega peaks turvameetmete rakendamine eeldatavasti muutuma arusaadavamaks, vajaduspõhiseks ning kohanduma paremini rakendaja äriprotsessidega.

Eesti infoturbestandardi uuendamisel peeti muu hulgas silmas järgmist:
i. Eesti avaliku korra ja ühiskonna toimimine ning turvalisusega seotud olulised valdkonnad on suurel määral seotud infotehnoloogiaga. Infotehnoloogial on ka üsna suur roll Eesti residentide igapäevategevustes. Mistahes süsteemid on mõjutatavad või pakuvad oma suure mõju tõttu huvi isikutele, kes võivad olla vaenulikud või pahatahtlikud nii ühiskonna kui ka indiviidi vastu. Seetõttu on vajalik üldine, koordineeritud ja pidev võrgu- ja infosüsteemide kaitse ning võimalike riskide hindamine ja maandamine.

ii. Infotehnoloogia ning küberkeskkond arenevad kiirelt, mis eeldab ka kiiret ning paindlikku reageerimist võimalikele või tuvastatud ohtudele.

iii. Küberturvalisuse 2. direktiivi artikli 21 lõike 1 esimese lõigu järgi tagavad liikmesriigid, et üliolulised ja olulised üksused võtavad asjakohased ja proportsionaalsed tehnilised, tegevuslikud ja korralduslikud meetmed, et juhtida riske, mis ohustavad nende üksuste tegevuses või teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust, ning et ennetada või minimeerida intsidentide mõju nende teenuste saajatele ja muudele teenustele.

iv. Küberturvalisuse seaduse (edaspidi *KüTS*) §-st 7 tulenevalt:
1. peab teenuseosutaja rakendama alaliselt asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ning korralduslikke turvameetmeid, et:
    1.1. hallata riske, mis ohustavad teenuseosutaja tegevuses või teenuse osutamisel kasutatava süsteemi turvalisust, sealhulgas koostab vastava riskianalüüsi;
    1.2. ennetada või minimeerida küberintsidendi mõju teenuseosutaja osutatava teenuse saajale ja muule teenusele;
    1.3. ennetada küberintsidenti või see tuvastada ja lahendada.
2. arvestatakse turvameetmete rakendamisel:
    2.1. teenuseosutaja vajadusi ja turvanõudeid;
    2.2. ajakohaseid ning asjakohasel juhul Euroopa ja rahvusvahelisi standardeid;
    2.3. turvameetmete rakendamise kulusid;
    2.4. turvameetmete rakendamise proportsionaalsust, mille hindamisel võetakse muu hulgas arvesse teenuseosutaja riskidele avatuse määra, teenuseosutaja suurust, küberintsidentide esinemise tõenäosust ja nende tõsidust, sealhulgas küberintsidentide ühiskondlikku ja majanduslikku mõju;
    2.5. ohte süsteemselt ja terviklikult hõlmavat lähenemisviisi, mille eesmärk on kaitsta süsteeme ja nende süsteemide füüsilist keskkonda küberintsidentide eest.

v. KüTSi § 7 lõike 5 kohaselt kehtestab Vabariigi Valitsus või tema volitatud minister määrusega eeltoodu tagamiseks muu hulgas:
1. infoturbe halduse nõuded üldnimetusega Eesti infoturbestandard;
2. turvameetmete üldnõuded.

vi. Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (edaspidi *määrus nr 121*) 3. peatükk sätestab turvameetmete nõuded. Määruse nr 121 § 3 annab üleriigilise küberturvalisuse tagamise korraldamise eest vastutavale ministrile volituse kehtestada Eesti infoturbestandard. Samas paragrahvis on osutatud ka teenuseosutajatele, kellele laieneb lisaks määruse nr 121 3. peatükis sätestatud turvameetmete nõuetele ka E-ITS. Siinjuures tasub toonitada, et E-ITS hõlmab ka esmaste turvameetmete puhul nõutut, mistõttu E-ITSi rakendades ei ole teenuseosutajal kohustust eristada esmaseid turvameetmeid ja E-ITSi rakendamisega kaasnevaid lisameetmeid.

vii. Arvestades eeltoodut on määruse eesmärk luua avalikku sektorit, avalikku korda ning ühiskonna toimimist olulisel määral mõjutavate teenuste osutamisel kasutatavate võrgu- ja infosüsteemide, sealhulgas neis töödeldava teabe kaitseks kasutatavate meetmete ühtne raamistik.

Arvestades eeltoodut, ei põhine eelnõukohase määruse jõustumisel kehtima hakkav E-ITS enam Saksa etalonturbe süsteemil BSI IT-Grundschutz (BSIG) ja standardil EVS-ISO/IEC 27001:2014 „INFOTEHNOLOOGIA. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded“ (27001). Uue E-ITSi puhul on arvestatud rakendajatelt saadud tagasisidega ning eesmärgiga vähendada rakendamisega kaasnevat koormust. Standardmeetmete kihi kaotamisega muutub asjakohaste meetmete väljaselgitamine ja rakendamine eeldatavalt kiiremaks. E-ITSi põhiosad on: äriprotsesside ja varade kaitsetarbe kaardistus; vastendamine; riskihaldus ja talitluspidevus, testimine ja kontroll. E-ITSi lahtisidumine eespool nimetatud dokumentidest loob parema võimaluse minna valdkonnaspetsiifiliselt regulatsioonilt üle üldisemale. Võrreldavusest loobumisega soovitakse parandada nõuete arusaadavust ka isiku jaoks, kes iga päev ei puutu kokku IT, võrgu- ja infosüsteemide haldusega ning sellest tulenevalt ka erialase sõnavaraga.

Eelnõu koostamisel on arvesse võetud Riigi Infosüsteemi Ametile ning Justiits- ja Digiministeeriumile laekunud tagasisidet E-ITSi kehtiva versiooni rakendamise kohta. E-ITSi muutmise kontseptsiooni on tutvustatud seletuskirja punktis 9.1 loetletud ministeeriumitele.

1. peatükk. Üldsätted
Paragrahvis 1 nähakse ette määruse üldsätted.

Lõikes 1 sätestatakse E-ITSi käsitlusala. E-ITS käsitleb võrgu- ja infosüsteemi infoturbe haldust ja infoturbe halduse meetmete auditeerimist. Võrreldes määrusega nr 101 E-ITSi käsitlusala ei muutu.

Lõikes 2 esitatakse viide nendele määruse nr 121 sätetele, kus on sätestatud teenuseosutajatele E-ITSi järgimise ulatus. E-ITS on kehtestatud Vabariigi Valitsuse antud volituse alusel ning Vabariigi Valitsusel on KüTSist tulenevalt õigus näha ette ka turvameetmete üldnõuded, mille puhul arvestatakse võrgu- ja infosüsteemide olulisuse ja mõjuga. Seetõttu on Vabariigi Valitsus määrusega nr 121 ka ette näinud erandid E-ITSi rakendamisel. E-ITSi meetmeid ei pea rakendama:

1. teenuseosutaja, kelle rakendatud turvameetmed vastavad rahvusvahelise standardiga ISO/IEC 27001 või Eesti standardiga EVS-EN ISO/IEC 27001 kehtestatud nõuetele ning seda kinnitav vastavussertifikaat on kehtiv ja esitatud Riigi Infosüsteemi Ametile. Tasub tähele panna, et see erand kehtib vaid osas, millele on eelnimetatud standardi kohane sertifikaat antud. Sertifikaadiga hõlmamata jäänu suhtes peab teenuseosutaja rakendama siiski E-ITSi;
2. teenuseosutaja, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aastane bilansimaht või aastakäive ei ületa 10 miljonit eurot, arvestades väikeettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta (ELT L 124, 20.05.2003, lk 36–41). Siinjuures ei ole oluline, kes on teenuseosutaja omanikud. See tähendab, et avaliku sektori osalus ei välista erandi tegemist. Kuna see erand on seotud ettevõtlusega, siis ei laiene see automaatselt avaliku sektori asutustele, kes võiks oma töötajate arvu ja eelarveaasta näitajatega kehtestatud kriteeriumite alusel erandi kohaldamisalasse kuuluda;
3. teenuseosutaja, kes on valla või linna ametiasutuse hallatav asutus ja osavalla või linnaosa ametiasutuse hallatav asutus, välja arvatud üldhariduskool, ja kellel on kalendriaasta jooksul keskmiselt alla 50 töötaja;
4. riigimuuseumist teenuseosutaja, kellel on kalendriaasta jooksul keskmiselt alla 50 töötaja;
5. kohaliku omavalitsuse üksuste liidust teenuseosutaja, kellel on kalendriaasta jooksul keskmiselt alla 50 töötaja.

Ülaltoodud erand ei kehti punktides 2–4 nimetatud teenuseosutajale, kui ta on avaliku teabe seaduse kohane andmekogu vastutav või volitatud töötleja, sest KüTSi § 3 lõike 4 punkti 1 järgi on andmekogu vastutav töötleja ja volitatud töötleja avaliku teabe seaduse tähenduses (vt § 43^1 ja § 43^4) oluline üksus. See tähendab, et tekkinud kohustus tuleneb erandina andmekogust endast, mitte teenuseosutaja tegevusvaldkonnast. Oluline on vahet teha, et andmekogu vastutav ja volitatud töötleja ei ole sama mis andmete vastutav või volitatud töötleja isikuandmete kaitse üldmääruse tähenduses.

Vabariigi Valitsus on lisaks E-ITSi rakendamise kohustusest vabastamisele ette näinud ka E-ITSi osalise rakendamise võimaluse. Osalise rakendamise korral on jätkuvalt kohustuslik välise isiku poolne infoturbe halduse meetmete auditeerimine. Vabariigi Valitsus on auditeerimiskohustusest vabastanud:

1. riigimuuseumi, avalik-õigusliku isiku muuseumi, valla või linna ametiasutuse, valla või linna ametiasutuse hallatava asutuse, osavalla või linnaosa ametiasutuse, osavalla või linnaosa ametiasutuse hallatava asutuse ning kohaliku omavalitsuse üksuste ühisameti ja -asutuse, kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga;
2. Haridus- ja Teadusministeeriumi hallatava asutusena tegutseva põhikooli ja gümnaasiumi, kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga avaliku teabe seaduse tähenduses.

Lõikes 3 esitatakse määruse kehtestamise eesmärk (vt seletuskirja p 2 sissejuhatavat osa).

Paragrahvis 2 esitatakse kolme määruses kasutatava termini tähendus: infoturbe halduse süsteem, infoturvameetmete rakendamise plaan (edaspidi ka *IMR*), organisatsioon ja äriprotsess (vt ka seletuskirja p 4 „Eelnõu terminoloogia“).

Organisatsiooni all mõistetakse kõiki KüTSi subjekte ehk teenuseosutajaid. Kuna infoturbe valdkonnas tähistatakse sõnaga „organisatsioon“ mistahes üksust (asutus, ettevõtja,

struktuuriüksus jne), mis infoturvameetmeid rakendab, siis kasutatakse eelnõus arusaadavuse huvides sama sõna.

2. peatükk. Infoturbe haldus

Paragrahvis 3 selgitatakse infoturbe halduse süsteemi olemust. Võrreldes määrusega nr 101 on välja jäetud infoturbe halduse süsteemi toimimist kirjeldav osa (määruse nr 101 lisa 1) ning haldussüsteemile olemuslikud olulisemad üksikasjad sätestatakse määruses endas.

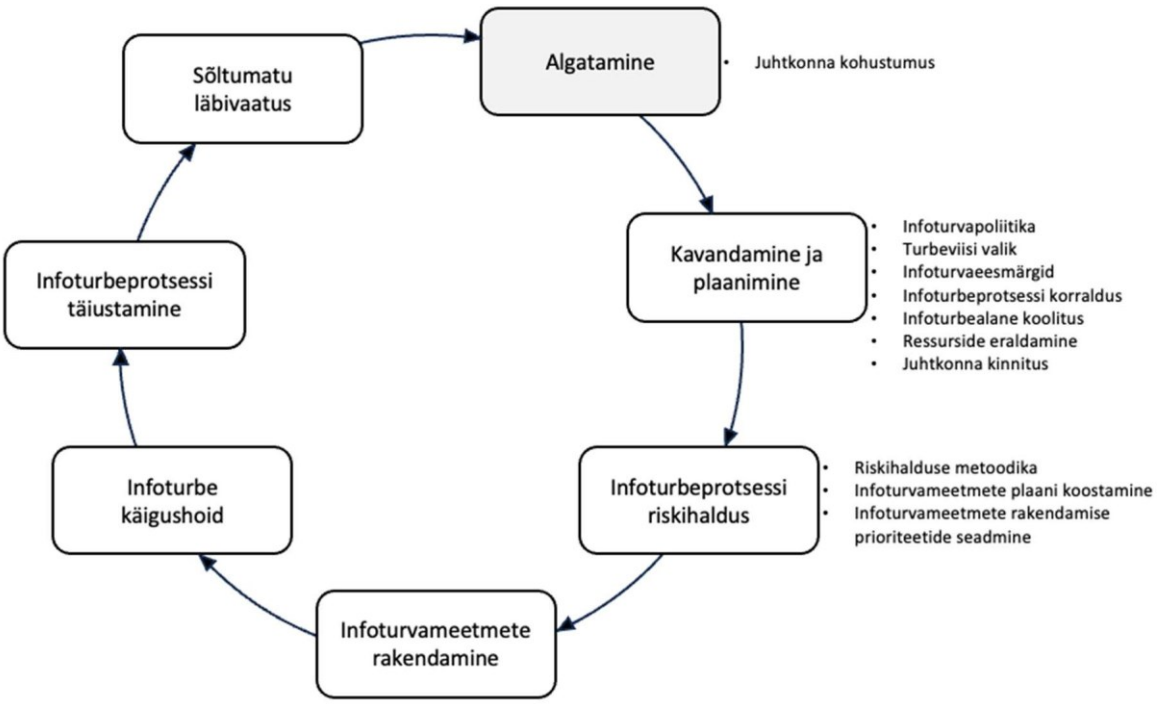
Lõikes 1 kirjeldatakse asjaolusid, mida organisatsioon peab infoturbe halduse süsteemi puhul arvesse võtma. Nendeks on organisatsiooni:

- tegevusvaldkond, eesmärgid, protsessid (sh äriprotsessid), protseduurid ja tavad;
- õigusaktidest ning lepingutest tulenevaid õigused ja kohustused;
- keskkond, kus tegutsetakse, ressursid (sh personal) ja vara.

Toimiva infoturbe halduse süsteemi ülesanne on tagada organisatsiooni jätkusuutlikkus ja kvaliteetne teenuste osutamine. Turve keskendub teabe ja äriprotsesside kaitsmisele, millest tuleneb vajadus kaitsta äriprotsesside toimimist tagavat infotöötlust ja ITd. Organisatsioon peab tuvastama teenuse osutamiseks vajalikud äriprotsessid, nendega seotud varad ning määrama kindlaks äriprotsessi ja vara kaitsetarbe, mille alusel saab riskihalduse jaoks kokku leppida riskikriteeriumid ja neile vastavad meetmed.

Infoturbe halduse süsteemi protsesse ja sooritatavaid tegevusi on kujutatud joonisel 1. Tegevusi võib sooritada vajadusel korraga. Infoturbe täiustamise käigus naastakse iga kord protsessi algusesse.

Joonis 1. Infoturbe halduse süsteemi elutsükkel



Allikas: Riigi Infosüsteemi Amet

Võrreldes E-ITSi kehtiva versiooniga on loobutud erinevatest skaaladest (nt kõrge, keskmine, madal), sest normiga ei ole võimalik piiritleda kõikvõimalikke olukordi ja lahendusi, mis võivad organisatsioonides esineda. Organisatsioonil võib olla erinevaid kohustusi, need võivad tuleneda erinevatest õigusaktidest. Neist mõnes on võib olla juba kirjeldatud ka riskihalduse nõudeid, mistõttu ei ole mõistlik E-ITSiga neid nõudeid sätestada. Seega jäetakse edaspidi organisatsiooni enda otsustada, kuidas riske hinnata ja millist skaalat kasutada.

Võrreldes kehtiva versiooniga on alles jäetud vaid kaitsemeetmed ja infoturbe halduse süsteemi raamistik ning loobutud on haldussüsteemi detailsest kirjeldamisest, küll aga on Riigi Infosüsteemi Ametile jäetud võimalus avaldada seni määruse nr 101 lisas 1 olnud teave samas ulatuses juhendmaterjalina veebilehel.

Lõikes 2 nimetatakse rollid, mis on vajalikud infohalduse süsteemi toimimiseks. Roll ei tähenda, et seda peab täitma sama ametinimetusega töötaja, vaid tegemist on tegevustega, millega organisatsioon peab arvestama. Nendeks rollideks on:

- äriüksuse juht – korraldab varade arvestuse, kaitsetarbe määramise ja kaitsetarbe saavutamiseks vajalike meetmete rakendamise regulaarse seire;
- infoturbejuht – koordineerib ja nõustab turvameetmete rakendamist, sealhulgas koolituste formaadi valimist;
- hankejuht – jälgib, et vara ja teenuste turvameetmed on kogu nende elutsükli ulatuses plaanitud uue vara ja teenuste hankimise etappi juba selle kavandamise käigus;
- kasutaja – järgib tema kasutusse antud vara kasutamise korda, läbib regulaarselt infoturbekoolitusi, reageerib intsidentidele kokkulepete kohaselt, sealhulgas korraldab küberintsidentidest teavitamist.

Hankejuhi all ei mõisteta eelnõus ostujuhti või riigihanke eest vastutajat. Hankejuhi ülesanne on kontrollida, kas turvameetmed on planeeritud kogu elutsüklis (nii teenuste kui ka varade puhul), enne kui mõni uus teenus kasutusele võetakse või võrgu- ja infosüsteemi turvalisuse tagamisega seotud tegevusi tehakse. Näiteks peab ta välja selgitama vajaduse tulekustutussüsteemi järele serveriruumis, nii et õnnetuse korral ei oleks tagatud mitte ainult tuleohutus, vaid ka teabe säilimine. Hankejuhi rollis ei pea olema üks töötaja, vaid seda rolli võib täita mitu töötajat.

Kasutaja rolli täidavad kõik organisatsioonis võrgu- ja infosüsteemi kasutavad töötajad. Kasutajatele võib ette näha erinevaid võrgu- ja infosüsteemile juurdepääsu ja teabe töötlemise õigusi.

Määruse nr 121 § 5 lõike 1 kohaselt peab organisatsioon kaardistama võrgu- ja infosüsteemid ning nendega seotud teenused või protsessid ja dokumenteerima süsteemidele rakendatavad turvameetmed ja riskianalüüsi. Sellest tulenevalt nähakse *lõikes 3* ette infoturbe halduse süsteemiga seotud teave, mis tuleb säilitada. Säilitamise kohustus nähakse ette osas, mis on seotud võrgu- ja infosüsteemi turvameetmete rakendamisega ning riskide ja nende vastumeetmete rakendamisega, seega tuleb säilitada järgmisi andmeid ja dokumente:

- infoturbe halduse süsteemi alusdokumendid ja otsuste kulg;
- infoturvasündmused ja organisatsiooni reaktsioon neile;
- infoturvameetmete rakendamise plaan ja selles sisalduvad riski aktsepteerimise otsused.

Määruse nr 121 § 5 lõike 2 kohaselt säilitatakse dokumentatsiooni vähemalt seitse aastat alates selle koostamisest.

Paragrahvis 4 sätestatakse organisatsiooni juhatuse roll infoturbe halduse süsteemi korraldamises. Organisatsiooni äriprotsesside toimimise eest vastutab juhatus, sellest tulenevalt vastutab juhatus ka äriprotsesse ohustavate sündmuste käsitlemise, sh infoturbe halduse süsteemi toimimise eest (*lõige 1*). Juhatuse kaasatus tagab infoturbe lõimituse kaitseala kõigisse protsessidesse ja infoturbe jätkusuutlikkuse ning juhatusel on õigus määrata prioriteete, kehtestada poliitikaid ja eraldada ressursse.

Juhatuse all tuleb lähtuvalt KüTSi §-st 6[1] mõista eraõigusliku juriidilise isiku või avalik-õigusliku isiku juhtorganit, kohaliku omavalitsuse üksuse täitevorganit (valla- või linnavalitsus), riigi ametiasutuse juhti, kohaliku omavalitsuse üksuse ametiasutuse juhti, valitsusasutuse hallatava asutuse juhti, valla või linna ametiasutuse hallatava asutuse juhti, sihtasutuse juhatust, riigi tulundusasutuse juhtimisorganit ja füüsilisest isikust ettevõtjat. Kui juhatus on mitmeliikmeline, siis on mõistlik, et põhivastutus pannakse kokkuleppel ühele liikmetest. Infoturbe halduse süsteemi rakendamise korraldamisel on juhatusel ka õigus jaotada ära rollid (vt ka § 3 lg 2 selgitus) ning vastutusalad konkreetsemalt (edasivolitamine, ülesannete kehtestamine jne). Juhatusel on õigus organisatsiooni tööd korraldava organina ka otsustada, milliseid rakendusplaanis kavandatud meetmete rakendamata jätmisest tulenevaid riske aktsepteeritakse ja milliseid mitte, arvestades võimalikku mõju äriprotsessi kaitsetarbele (*lõige 2*).

Selleks, et juhatus saaks täita talle antud ülesannet infoturbe halduse süsteemi korraldamisel, peab juhatusele olema tagatud regulaarne ja vajadusel operatiivne juurdepääs järgmisele teabele:

- riskid ning nende võimalik mõju ja kulu;
- toimunud küberintsidentide mõju äriprotsessidele;
- õigusaktidest ja lepingutest tulenevad nõuded ja nende muudatused;
- infoturbe hetkeseis ja infoturvameetmete rakendamise plaani täitmine.

Teabe liikumise protseduurid kehtestab organisatsioon ise (*lõige 3*).

Paragrahvi 5 *lõikes 1* käsitletakse infoturvapoliitikat. Infoturvapoliitika (inglise keeles *information security policy*) koosneb organisatsiooni väärtuste ja varade kaitse juhtpõhimõtetest. See sisaldab infoturbe põhimõtteid ja kohustumust: miks ja millistel põhimõtetel kaitstakse organisatsiooni varasid, sh andmeid ning võrgu- ja infosüsteeme küberohtude eest. Infoturvapoliitika määrab kindlaks infoturbe lähtealused, infoturbe üldised eesmärgid (inglise keeles *security goal*), sellega seotud rollid ja vastutusalad, turbe rakendamise korralduslikud alused, intsidentide käsitlemise ning turbeprotsessi hindamise ja täiustamise põhimõtted ning uuendamise regulaarsuse. Infoturvapoliitika alusel luuakse täpsemad alampoliitikad, eeskirjad, juhendid, protseduurireeglid ja tehnilised lahendused. Infoturvapoliitika ei pea olema koondatud vaid ühte dokumenti, kuid põhidokument peaks selguse huvides sisaldama viiteid seotud dokumentidele. Organisatsiooni selleteemaline tekst ei pea kohustuslikus korras kandma pealkirja „infoturvapoliitika“, vaid seda võib nimetada ka muud moodi või see võib ka olla muu dokumendi osa.

Joonis 2. Infoturvapoliitika põhilised elemendid

Allikas: Riigi Infosüsteemi Amet

Organisatsiooni kaitstavad väärtused tuletatakse üldisest keskkonnast ja organisatsiooni põhieesmärkidest. Põhieesmärgid tulenevad ettevõtte puhul ärieesmärkidest, avaliku sektori asutuse puhul põhikirjast või põhimäärusest. Organisatsiooni väärtustena võetakse arvesse vähemalt järgmist:
a) toimingute, sh teabekäitluse usaldatavus (käideldavus, terviklus, konfidentsiaalsus);
b) organisatsiooni sisemine ja väline maine;
c) investeeringud tehnoloogiasse, teabesse, tööprotsessidesse ja teadmusesse;
d) töödeldava informatsiooni väärtus ja kaitse vajadus, sh isikuandmed;
e) õigusaktide, eeskirjade, standardite ja lepingute nõuete täitmine;
f) inimeste füüsiline ja vaimne heaolu.
Organisatsiooni väärtused on aluseks kaitsetarbe määramisele.

Organisatsiooni infoturvapoliitika koostamisel tuleks arvestada:
a) organisatsiooni eesmärke ja strateegiat;
b) organisatsiooni kaitseala;
c) organisatsiooni struktuuri;
d) organisatsiooni olemasolevaid haldussüsteeme, nt kvaliteedihaldus, riskihaldus, keskkonnahaldus;
e) õigusalaseid raamtingimusi, sh kohalikud ja rahvusvahelised õigusaktid, valdkondlikud määrused;
f) klientide, tarnijate, partnerite ja muude huvipoolte nõudeid, sh lepingulisi;
g) tegevusala turvastandardeid ja -praktikaid.

Infoturvapoliitika kinnitab juhtkond. Infoturvapoliitika on soovitatav teha teatavaks töötajatele ning vajadusel teistele huvipooltele. Infoturvapoliitika tuleks vähemalt korra kalendriaastas või oluliste muudatuste korral üle vaadata ja vajadusel ajakohastada. *Lõikes 2* ette nähtud iga-aastase ülevaatamise kohustus on tingitud teadmisest, et IT-valdkond muutub kiirelt, mistõttu peaks organisatsioon vähemalt korra aastas mõtlema, kas infoturbe halduses tuleb midagi muuta või ei. Säte ei eelda, et iga aasta kinnitatakse uus infoturvapoliitika või selle muudatused. Muudatust ei ole vaja teha, kui on selge, et selle järele puudub vajadus.

Paragrahv 6. KüTSi § 7 lõikest 1 tulenevalt peab organisatsioon rakendama asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ning korralduslikke turvameetmeid, et:
1) hallata riske, mis ohustavad tema tegevuses või teenuse osutamisel kasutatava võrgu- ja infosüsteemi turvalisust, sealhulgas koostama vastava riskianalüüsi;
2) ennetada või minimeerida küberintsidendi mõju osutatava teenuse saajale ja muule teenusele;

3) ennetada küberintsidenti või see tuvastada ja lahendada.
See tähendab, et organisatsioonis peab olema toimiv riskihaldus.

Organisatsioon otsustab ise oma vara ja teabe (isikuandmed ja ärisaladus, sh tundlikud tehnoloogiad ja muu intellektuaalomand) kaitsmise vajaduse ja meetmed ohtudest avalduva riski alusel.

Mistahes meetmete rakendamisel jääb mingi risk alati alles ning organisatsioon peab otsustama, kas selline tuvastatud jääkrisk on aktsepteeritav või ei, st kas ta on nõus sellist riski taluma. Seejuures tuleb arvestada, et organisatsiooni riskitaluvus võib eri olukordades olla erinev. Riskihaldus hõlmab ka rohkemate kaitsemeetmete kavandamist tulevikus tekkida võiva riski maandamiseks, näiteks tehnoloogilist arengut silmas pidades. Ühtlasi tuleb kehtestada kahju vähendamise meetmed juhuks, kui vara või teavet ei ole enam võimalik kaitsta. Riskihalduse üldised etapid ja tegevused on esitatud tabelis 1.

Tabel 1. Riskihaldus

Riskihalduse etapp	Tegevus
Ohuhinnang	Millised ohud organisatsioonile avalduvad? Kelle või mille eest kaitstakse?
Riskihinnang	Millist kahju vara või teabe kahjustamine põhjustab? Millisel tasemel tuleks vara või teavet kaitsta?
Kaitsemeetmed	Millised peavad olema kaitsemeetmed üldiselt? Millised peavad olema kaitsemeetmed konkreetsel juhul?
Jääkrisk	Millised riskid jäävad pärast meetmete rakendamist alles? Kas maandamata risk on aktsepteeritav?
Lisameetmed	Kuidas tulevikus tekkida võivaid riske maandada? Millised kahju vähendamise meetmed on vajalikud?
Protsessi kordamine	Kas ohu- või riskihinnang on muutunud või muutub tulevikus? Milliseid uusi kaitsemeetmeid tuleb kasutusele võtta või kavandada?

Allikas: Justiits- ja Digiministeerium

Lõikes 1 sätestatakse, et enne riskihaldusmetoodika koostamist tuleks organisatsioonis võtta arvele varad (sh IT-vara) ja määrata kindlaks nende kaitseala. Kaitseala tuleb kindlaks määrata ning vajaduse korral ajakohastada ka jooksvalt soetatava vara puhul.

Lõike 2 järgi seotakse turvariskihaldus äririskide halduse protsessiga. Riskihaldusmetoodika peab sisaldama vähemalt järgmist:

- äriprotsessidele mõju avaldavate ohtude tuvastamine, arvestades teabe konfidentsiaalsust, autentsust, terviklust, käideldavust;
- vara ja protsessi vastendamine infoturbekataloogi moodulitega;
- infoturvameetmete rakendamise plaani täitmise otsused, sealhulgas riskide hindamine.

Organisatsiooni riskihaldusmetoodika peab tagama protsessi korratavuse ja võrreldavuse, võimaldades ülevaadet rakendatud meetmete seisust ning infoturvariskide haldamisest tervikuna.

Mistahes riskihinnang hakkab aeguma kohe pärast selle koostamist, mistõttu on riskihaldus pidev protsess. Seega peab organisatsioon regulaarselt uuesti läbi mõtlema, milliste ohtude eest, millisel määral ja milliste kaitsemeetmetega end ja oma teavet kaitsta.

Paragrahvis 7 kirjeldatakse infoturbekataloogi olemust. Infoturbekataloog on organisatsiooni kahjustada võivate ohtude kaitseks võetavate meetmete loend. Infoturbekataloogi moodulid on jaotatud protsessimooduliteks ja süsteemimooduliteks. Organisatsioon määrab igale kaitstavale varale või varade koondile turvameetmed. Infoturbekataloog on esitatud määruse lisas. Võrreldes kehtiva E-ITSi määrusega on märgatavalt vähendatud kataloogi detailsust, jättes sellega organisatsioonidele suurema vabaduse asjakohaste ja efektiivsete meetmete valimisel ning organisatsiooni tegevusest lähtuvate riskide kirjeldamisel.

Paragrahvis 8 käsitletakse infoturvameetmete rakendamise plaani. Infoturvameetmete rakendamise plaan (edaspidi ka *IMR*) on ühest või mitmest dokumendist koosnev juhend, kus kirjeldatakse, kuidas organisatsioonis teavet ja vara kaitsta ning võimalikke riske ennetada. IMRis esitatakse kokkulepitud turvameetmed ja rollid ning käitumisjuhised erinevateks olukordadeks.

Lõiked 1–6. IMRi koostatakse infoturbekataloogi abil, valides välja asjakohased osad ning kirjeldades kaitsemeetmeid. Organisatsioon võib riskihalduse põhjal lisada uusi meetmeid. Erinevalt E-ITSi kehtivast versioonist töötab organisatsioon välja oma meetmed ja hindab nende rakendamist ning mõju ise ilma määrusepoolse ettekirjutuseta. See võimaldab organisatsioonil välja töötada sobivaima meetmete komplekti, mis vastab organisatsiooni kaitsevajadustele. Kasutatavad protsessimoodulid ja süsteemimoodulid lõimitakse organisatsiooni infoturbe haldusse. Kaitseala varasid vastendatakse süsteemimoodulitega ja luuakse neile turvameetmete komplektid. Protsessimoodulite meetmed lõimitakse organisatsiooni igapäevasesse töökorraldusse.

Organisatsioon määrab meetmete rakendamise prioriteedid kaitsetarbe, turbeviisi, meetmete ja varade omavahelise sõltuvuse, vara elutsükli ja infoturbe eesmärkide alusel. Riski kaalutlemise tulemusel lisanduvaid riskikäsitlusmeetmeid kirjeldatakse IMRis. IMRi pidev haldus on riskihalduse protsessi osa. Ülevaade IMRist ja meetmete rakendamise hetkeseisust on osa juhtkonnale regulaarselt esitatavatest aruannetest.

Kui üksiku meetme rakendamata jätmisest tulenev risk ei ületa organisatsioonis kehtivat riskitaluvuspiiri või on risk maandatud alternatiivsete või kompenseerivate turvameetmetega, on lubatav jätta infoturbekataloogi meede rakendamata ja sellest tulenevat riski aktsepteerida. Riski aktsepteerimise otsused dokumenteeritakse IMRis ja vaadatakse regulaarselt üle.

Lõigetes 7–9 on võrreldes E-ITSi kehtiva versiooniga selgemalt sätestatud organisatsiooni kohustus hinnata ka sõltuvust välistest isikutest teenuse osutamisel või äriprotsessides (organisatsiooniväline tarneahel). Ka sellisel juhul peab organisatsioon võtma kasutusele mõistlikud meetmed, et olla teadlik tarneahelaga seotud riskidest. Näiteks veendumaks, et ka tarnija rakendab turvameetmeid, võib küsida asjakohase sertifikaadi olemasolu või enesehindamise tulemusi. Kui välise isiku puhul ei ole selge, milliseid meetmeid ta rakendab või kas tema teenust on hinnatud, siis tasub organisatsioonil kaaluda välise isiku vahetust või

kasutatava teenuse puhul rohkemate riskimeetmete rakendamist, sh teenuse kasutusulatuse piiramist.

Paragrahvis 9 nähakse ette personali turvameetmete rakendamise alase koolitamise vajadus. Organisatsioon peab kooskõlas infoturvapoliitika eesmärkidega tagama kõigi töötajate, sh juhatuse liikmete infoturbealase koolitamise ja teadmiste täiendamise. Koolitusel lähtutakse töötaja ülesannetest ja seotusest rakendatavate turvameetmetega. Regulaarsete infoturvet käsitlevate koolituste eesmärk on motiveerida töötajaid järgima infoturvanõudeid, käsitlema teavet ja käsitsema töövahendeid korrektselt, vältima riskikäitumist ja asjakohaselt reageerima mistahes intsidentidele, sealhulgas teadma, kuidas intsidente ennetada ja avastada.
Koolitus ei pea olema loengupõhine, lubatud on kasutada ka muid meetodeid, näiteks perioodiliste testide tegemist. Koolitus ei pea olema kogu personalile samasugune, vaid koolitamisel võib lähtuda töötaja rollist, seotusest võrgu- ja infosüsteemi ning selle kaitsega jne.

3. peatükk. Seire
Paragrahv 10. Eelnõu koostamise käigus vaadati üle määruse nr 101 lisas sätestatud auditeerimiseeskiri.
Võrreldes E-ITSi kehtiva versiooniga ei ole enam auditi osana sätestatud eelauditit, vaheauditit ja järelauditit. Nimetatud osade asemel nähakse eelnõus (*lõige 1*) ette organisatsioonisisene hindamine. Organisatsioonisisene hindamine on organisatsiooni pidev kontroll, mille käigus hinnatakse, kas organisatsioonis on:
1) kindlaks määratud äriprotsessid;
2) kaardistatud äriprotsessidega seotud varad;
3) tuvastatud välised infoturvanõuded, sealhulgas õigusaktid ja lepingud;
4) määratud kaitsetarve;
5) vastendatud infoturbekataloogi moodulid kaitseala varaga;
6) kehtestatud riskihaldusmetoodika;
7) koostatud infoturvameetmete rakendamise plaan;
8) rakendatud ja seiratud infoturvameetmeid vastavalt infoturvameetmete rakendamise plaanis esitatud tähtaegadele;
9) kõrvaldatud auditite ja hindamiste käigus tuvastatud puudused.

Järelauditi asemel peab organisatsioon auditi lõpparuandest tulenevalt kavandama parandusmeetmete rakendamise, määrama vastutajad ja tähtajad. Parandusmeetmete rakendamist ja infoturvameetmete rakendamise plaani ajakohastamist koordineerib infoturbe eest vastutav isik. Organisatsioonisisese hindamise käigus hinnatakse kavandatud meetmete rakendamist ja tulemuslikkust.

Lõige 2. Organisatsioonisisest hindamist võib teha organisatsiooniga töö- või teenistussuhtes olev isik või organisatsioonivälise isik. Muudatus võimaldab organisatsioonil lähtuda oma võimalustest ja vajadustest. Näiteks võib organisatsioon kasutada hindamiseks siseaudiitorit või kui organisatsiooni suurus või ülesehitus ei võimalda hindajat palgal hoida, siis on võimalik ka teenust sisse osta. Sealhulgas ei ole välistatud, et hindamist tehakse kahasse kahe või enama organisatsiooniga, kes on oma olemuselt seotud. Oluline on, et hindaja ise ei ole turvameetmete rakendaja, st on selle suhtes erapooletu.

Lõikes 3 sätestatakse, et organisatsioonisisese hindamise käigus tuvastatud puudused ning eelmise auditi järel kavandatud parandusmeetmed peaksid olema vastavalt kas kõrvaldatud või rakendatud. Sealhulgas arvatakse selle hulka ka riskide põhjendatud aktsepteerimist. Välise

isiku hinnang annab organisatsiooni klientidele ja partneritele teavet organisatsiooni infoturbe halduse süsteemi jätkusuutlikkuse ja infoturvalisuse ohtudele vastupanuvõime kohta. Näiteks rahvusvahelise standardi ISO/IEC 27001 järgimine eeldab auditeerimist, mille tulemusel väljastatakse vastav sertifikaat. Selle sertifikaadi olemasolu võivad eeldada võimalikud koostööpartnerid enne koostöö alustamist. Samas võib sertifikaat kehtida vaid kindla teenuse või tegevuse kohta.

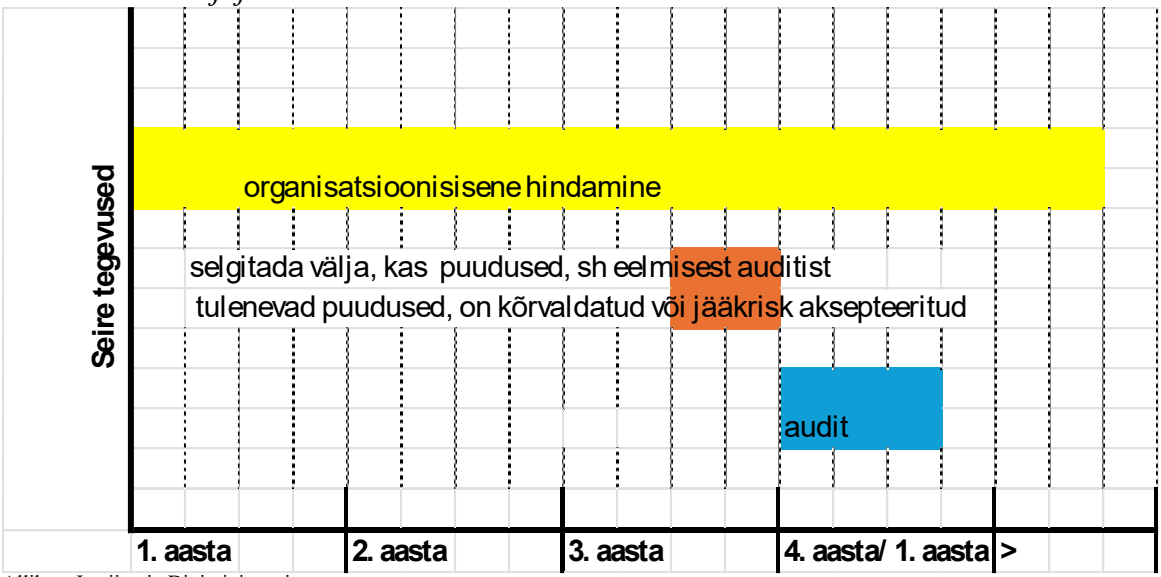
Paragrahvis 11 kirjeldatakse auditeerimise eesmärki, mis seni oli nimetatud kehtiva E-ITSi määruse lisas. Auditeerimine on osa turvameetmete rakendamise protsessist, mille käigus väline isik annab sõltumatu hinnangu tehtule ja kirjeldab avastatud puudujääke.

Auditi võib teha koos teise organisatsiooniga. Ühisaudit või teise organisatsiooni nimel auditi tellimine on ennekõike asjakohane juhul, kui eri organisatsioonide info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) taristu haldamine ja majutamine on üle antud kesksele organisatsioonile. Samas ei ole välistatud ka muud võimalused ühishanget teha. Küll aga peab auditi lõpparuanne sisaldama teavet iga auditi subjekti kohta. IKT-taristu haldamine ja majutamine kolmanda organisatsiooni kaudu ei mõjuta auditi subjekti kohustust E-ITSi järgida, mille täitmist audit kontrollib.

Organisatsioonipoolset auditi tellimist, auditiga kaasnevaid kohustusi, auditi kvaliteedi hindamist ning audiitoripoolset auditi kavandamist, tegemist ja selle kohta aruande koostamist on kirjeldatud auditeerimiseeskirjas, mis kehtestatakse määruse lisana.

Peatükis kirjeldatud tegevuste ajajoon on esitatud joonisel 3.

Joonis 3. Seire ajajoon



Allikas: Justiits- ja Digiministeerium

4. peatükk. Eesti infoturbestandardi tugi ja rakendamine

Eelnõuga kavandatakse märgatavalt vähendada määruse nr 101 regulatiivset osa, suurendades seeläbi info- ja võrgusüsteemide turvameetmete rakendamise paindlikkust ning parandades ka efektiivust, võimaldades organisatsioonil ise valida ja kujundada asjakohaseid turvameetmeid. Eri organisatsioonid vajavad siiski endiselt tuge ja nõu meetmete rakendamisel võrgu- ja infosüsteemide kaitseks. Selleks nähakse **paragrahvis 12** ette riigi tugitegevused E-ITSi

rakendamisel. Küberturvalisuse valdkonnas teeb riiklikku ja haldusjärelevalvet Riigi Infosüsteemi Amet. Eelnõukohases määruses sätestatakse, et E-ITSi rakendamise toetamiseks ja ühtlustamiseks loob amet asjakohase veebilehe või rakenduse. Veebilehe loomise nõue ei ole uus, sest ka kehtiva E-ITSi rakendamise toetamiseks on Riigi Infosüsteemi Amet loonud rakendamist toetava veebikeskkonna.[1] Veebilehel saab amet avaldada ajakohaseid juhiseid turvameetmete rakendamiseks või selgitada, kuidas, miks ja millele tähelepanu pöörata. Veebileht toetab määrust, kuid sel ei ole iseseisvat õigusjõudu. Seal avaldatud teave toetab organisatsioone, kuid samas jääb igale organisatsioonile vabadus rakendada soovitatust erinevat meedet või võtta kasutusel mõni teine organisatsiooni äriprotsessidega sobivam meede või jätta meede üldse rakendamata, kui selleks puudub vajadus. Veebileht võimaldab Riigi Infosüsteemi Ametil kiiremini teavitada organisatsioone uutest ohtudest ja riskidest ning pakkuda uusi tehnoloogilisi lahendusi jne.

Eelnõukohane määrus sätestab ka E-ITSi järgimist toetavate rakenduste kasutusele võtmise võimaluse. Kavandatav rakendus peaks parandama eelkõige väiksemate organisatsioonide võimekust omada ülevaadet oma võrgu- ja infosüsteemide kaitsega seotud riskidest ning puudujääkidest, sest erinevalt suurtest organisatsioonidest puudub väiksemates organisatsioonides sageli ainult infoturbega tegelev töötaja (infoturbejuht) või ostetakse infoturbeteenust sisse. Näiteks Riigi Infosüsteemi Amet arendab Eesti infoturbestandardi järgimiseks tugirakendust, mis aitab rakendajal luua vajaduspõhist turvameetmete rakendamise plaani, seejuures vähendada vigu meetmete valimisel, ja suunab rakendaja kohe meetmeid rakendama.[2]

Paragrahv 13. Eelnõukohase määrusega on ette nähtud E-ITSi kehtiva versiooni kehtetuks tunnistamine, mistõttu nähakse ette kolmeaastane üleminekuperiood. Perioodi pikkuse määramisel on arvestatud senise auditeerimise välbaga. Eelnõukohase määruse jõustumise korral ei ole ühelgi organisatsioonil kohustust alustada turvameetmete ülevaatamist või jätta pooleli juba toimuv audit. Eelnõukohase määrusega väheneb asjaomaste sätete hulk, kuid ei muudeta vajadust kaitsta võrgu- ja infosüsteeme. Seega on kehiva määruse alusel tehtud audit asjakohane ka pärast uue määruse kehtima hakkamist. Turvameetmete rakendamine ja riskide hindamine on pidev protsess, seega on ka organisatsioonipoolne meetmete kohandamine pidev protsess.

Paragrahvis 14 nähakse ette määruse nr 101 (RT I, 28.08.2025, 12) kehtetuks tunnistamine eelnõukohase määruse jõustumisel. Määrus jõustub **paragrahvi 15** kohaselt 1. augustil 2026 (vt ka seletuskirja p 7 „Määruse jõustumine“).

Eelnõul on kaks lisa:
lisa 1 „Infoturbekataloog“,
lisa 2 „Auditeerimiseeskiri“.

3. Eelnõu terminoloogia

Eelnõukohases määruses esitatakse nelja määruses kasutatava termini määratlus:
infoturbe halduse süsteem – riskide hindamisel, käsitlemisel ja aktsepteerimisel põhinev teenuseosutaja süsteemse kaitsmise ning infoturbe rajamise, teostamise, seire, läbivaatamise ja täiustamise süstemaatilise käsitlemise viis;

[1] https://eits.ria.ee/
[2] https://eits.ria.ee/et/abimaterjalid/tugirakendus

infoturvameetmete rakendamise plaan – organisatsioonikeskne struktureeritud ühest või mitmest dokumendist koosnev juhend turvameetmete haldamiseks;
organisatsioon – teenuseosutaja küberturvalisuse seaduse tähenduses;
äriprotsess – organisatsiooni tegevuse osa, mingi eesmärgi saavutamiseks rakendatavate inimeste, aja, finants- ja töövahendite (edaspidi koos *ressursid*), tegevuste, toimingute või protseduuride kogum, mille tulemusel valmib toode või teenus.

4. Eelnõu vastavus Euroopa Liidu õigusele

Määrus vastab Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv), artiklile 21. Eelnõu ei ole seotud Euroopa Liidu õiguse ülevõtmisega.

5. Määruse mõjud

Eelnõukohane määrus mõjutab majanduskeskkonda ning riigivalitsemist.

Eelnõukohase määruse jõustumisel väheneb olulisel määral nende võrgu- ja infosüsteemide infoturvet kirjeldavate sätete hulk, mille arvestamist või arvestamata jätmist peab põhjendama.

Mõjuvaldkond: halduskoormus (majanduslik), mõju kohaliku omavalitsuse korraldusele ja finantseerimisele ning keskvalitsuse korraldusele (riigivalitsemine)

Mõju sihtrühm: KüTSi subjektid, kellel on määrusest nr 121 tulenev kohustus rakendada E-ITSi.

Avalduv mõju ja mõju olulisus
Eelnõukohase määruse jõustumisel keskendub E-ITS senisest enam turvameetmete vormikohasuse asemel nende ajakohasusele, mille tulemusena muutub organisatsioonide küberturbe korraldamine efektiivsemaks ning vajaduspõhisemaks. Organisatsioonidel on edaspidi paremad võimalused keskenduda asja- ja ajakohaste meetmete rakendamisele.
Pikemas perspektiivis peaks eelnõukohase määruse rakendamine vähendama organisatsioonide haldus- või töökoormust, sest uue määrusega vähendatakse välise auditi kasutamise kohustuse ulatust ning ettekirjutavate normide hulka.

Järeldus mõju olulisuse kohta: eelnõukohase määruse jõustumisel suureneb paindlikkus võrgu- ja infosüsteemide turvameetmete valimisel ja rakendamisel. See võimaldab kiiremini reageerida tehnoloogiamuutustele ja võimalikele kaasnevatele riskidele. Muudatus toetab eeldatavalt efektiivsemalt digiühiskonna toimimist. Seega määruse üldine mõju on positiivne, kuid üksiku organisatsiooni seisukohast siiski väike, sest ei eelda vahetult uusi tegevusi ega sea ka uusi kohustusi.

6. Määruse rakendamisega seotud riigi ja kohaliku omavalitsuse tegevused, eeldatavad kulud ja tulud

Eelnõukohase määrusega ei kehtestata organisatsioonidele uusi kohustusi, küll aga võib see tänu auditeerimisprotsessi muudatustele veidi vähendada kulu. Eelnõukohase määruse jõustumisega ei kaasne riigi ja kohaliku omavalitsuse üksuse eelarvele lisakulu ega -tulu.

7. Määruse jõustumine

Määrus jõustub 1. augustil 2026. Jõustumisaja kehtestamisel on arvestatud Riigi Infosüsteemi Ameti vajadust vaadata üle haldus- ja riikliku järelevalvega seotud dokumentatsioon ning avaandmed ning viia need muudatustega kooskõlla. Riigi Infosüsteemi Amet peab ka ajakohastama oma veebilehel oleva teabe ning tegema selle kättesaadavaks rakendajatele.

8. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

9.1. Eelnõu esitakse eelnõude infosüsteemi kaudu kooskõlastamiseks Haridus- ja Teadusministeeriumile, Kliimaministeeriumile, Kultuuriministeeriumile, Majandus- ja Kommunikatsiooniministeeriumile, Regionaal- ja Põllumajandusministeeriumile, Rahandusministeeriumile, Siseministeeriumile, Sotsiaalministeeriumile, Välisministeeriumile, Riigikantseleile ning Eesti Linnade ja Valdade Liidule.

9.2. Eelnõu saadetakse arvamuse avaldamiseks Riigikogu Kantseleile, Vabariigi Presidendi Kantseleile, Riigikohtule, Eesti Pangale, Finantsinspektsioonile, Riigi Infosüsteemi Ametile, Riigi Info- ja Kommunikatsioonitehnoloogia Keskusele, Andmekaitse Inspektsioonile ning Registrite ja Infosüsteemide Keskusele.

9.3. Eelnõu saadetakse arvamuse avaldamiseks Eesti Haiglate Liidule, Eesti Perearstide Seltsile, Eesti Vee-ettevõtete Liidule, Eesti Kiirabi Liidule, Ravimitootjate Liidule, Eesti Proviisorapteekide Liidule, Eesti Apteekrite Liidule, Eesti Elektritööstuse Liidule, Eesti Jõujaamade ja Kaugkütte Ühingule, Eesti Gaasiliidule, Eesti Transpordikütuste Ühingule, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule, Eesti Kaubandus-Tööstuskojale, Eesti Põllumajandus-Kaubanduskojale, Eesti Esmatasandi Tervisekeskuste Liidule ja Eesti Infosüsteemide Audiitorite Ühingule.