25.08.2026

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 küberturvalisuse 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 14 paragrahvist, mis on jaotatud nelja peatüki vahel järgmiselt:
1. peatükk – üldsätted, § 1;
2. peatükk – infoturbe haldus, §-d 2–8;
3. peatükk – seire, §-d 9 ja 10;

4. peatükk – Eesti infoturbestandardi tugi ja rakendamine, §-d 11–14.

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 infoturbestandardit uuendades peeti muu hulgas silmas järgmist:
i. Eesti avaliku korra ja ühiskonna toimimine ning turvalisusega seotud olulised valdkonnad on suurel määral seotud ITga. IT-l 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 jõustudes 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 ministeeriumitele (v.a Kaitseministeerium).

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.

Kuna infoturbe valdkonnas tähistatakse sõnaga „organisatsioon“ mistahes üksust (asutus, ettevõtja, struktuuriüksus jne), mis infoturvameetmeid rakendab, siis kasutatakse eelnõus arusaadavuse huvides sõnalühendina sama sõna, see tähendab, et eelnõukohases määruses viidatakse sõnaga *organisatsioon* KüTSi subjektile ehk teenuseosutajale.

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

Lõikes 4 määratletakse äriprotsessi mõiste.

Sõna *äriprotsess* on lisaks IT valdkonnale kasutusel ka planeerimisel, eelarvestamisel, kvaliteedijuhtimise, personalitöö jne valdkonnas. Kõnesolevas eelnõus on sellel laiem tähendus kui üldkeeles. Äriprotsess ei ole ka ettevõtlus äriseadustiku tähenduses. Äriprotsess on organisatsiooni (ettevõtja või riigi või kohaliku omavalitsuse asutus) organisatsiooni põhitegevuste või eesmärkide saavutamiseks vajalike tegevuste kogum, mille käigus kasutatakse aega, raha, töövahendeid ning inimeste tööpanust (edaspidi koos ressurss) teenuse, toote või muu väärtust loova tulemuse pakkumiseks. Avalik sektor pakub avalikku teenust ja igal asutusel on oma eesmärk, mille täitmiseks ta on loodud.

2. peatükk: infoturbe haldus

Paragrahvis 2 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.

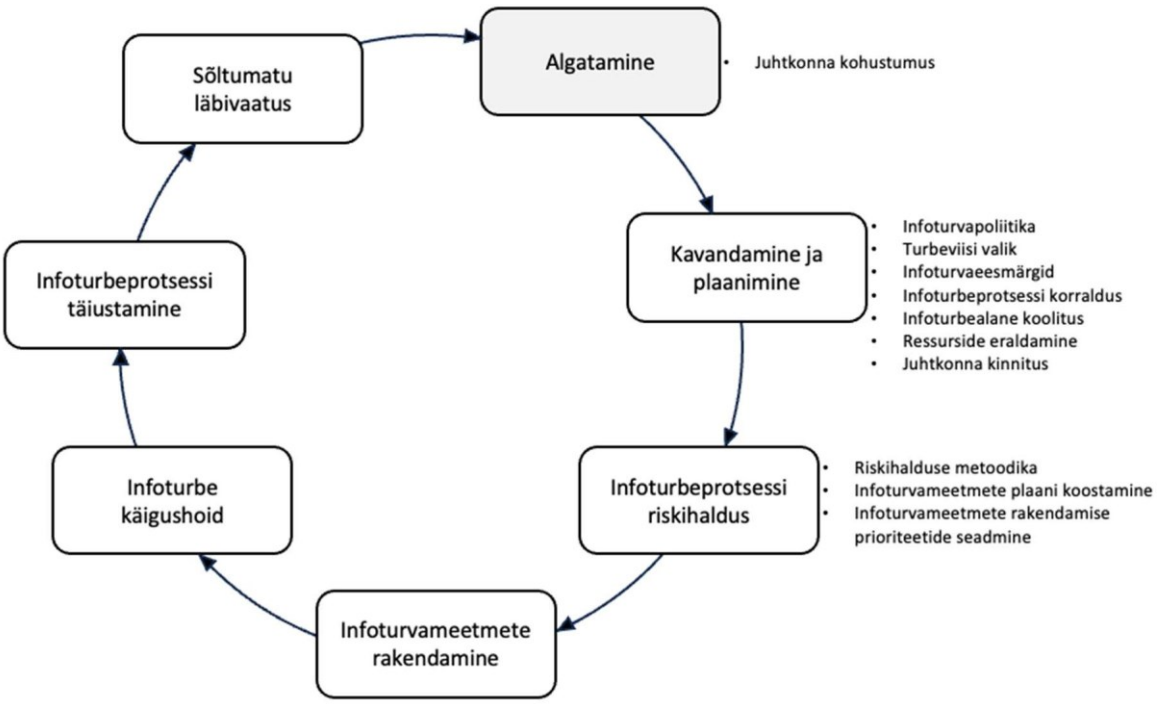
Infoturbe halduse süsteem on kokkuvõtvalt riskide hindamisel, käsitlemisel ja aktsepteerimisel põhinev teenuseosutaja süsteemse kaitsmise ning infoturbe rajamise, teostamise, seire, läbivaatamise ja täiustamise süstemaatilise käsitlemise viis.

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 olulisemad tegevused, millega peab arvestama toimiva infohalduse süsteemi üles ehitamisel ja töös hoidmisel. Ühegi tegevuse juures ei ole eeldatud, et seda peab ellu viima sama ametinimetusega töötaja, vaid tegemist on tegevustega, millega organisatsioon peab arvestama. Need tegevused on:

- vara kasutusele võtmine – vara kogu elutsükli ulatuses infoturbe riskide tuvastamine ja hindamine, turvameetmete planeerimine ja rakendamine sealhulgas meetmete planeerimine uue vara ja teenuste hankimise etapis või selle kavandamise käigus;
- vara kasutamine – kasutusse antud vara kasutamise korra järgimine, infoturbekoolituste regulaarne läbimine, intsidentidele kokkuleppekohane reageerimine, sealhulgas küberintsidentidest teavitamine;
- vara haldamine – kaitsetarbe määramise korraldamine ja kaitsetarbe saavutamiseks vajalike meetmete rakendamise regulaarne seire;
- andmekaitse – organisatsiooni andmete või organisatsioonile usaldatud andmete kaitse korraldamine.

Siinjuures olgu öeldud, et andmekaitse ei tähenda kõnesolevas eelnõus vaid isikuandmete kaitset. Igal organisatsioonil on andmed (teave), mis vajavad kaitset juba selleks, et organisatsioon toimiks ja saavutaks oma eesmärgid. Näiteks ärisaladus, asutusesiseseks kasutamiseks mõeldud teave või mistahes muu teave, mille kolmandatele isikutele kättesaadavaks tegemine võib kahjustada organisatsiooni või temast kõrgemal seisva institutsiooni huve. Organisatsioonile teiste isikute usaldatud teabe või muu õiguspäraselt kogutud teabe, sh isikuandmete kaitse tagamine on iseenesestmõistetav. Seega on andmekaitsel eelnõukohases määruses laiem tähendus kui vaid isikuandmete kaitse. Andmekaitsega samas tähenduses on valdkonnas kasutatud ka sõna *teabekaitse*.

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 riskikäsitlusviisid.

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

Paragrahvis 3 sätestatakse organisatsiooni juhatuse roll infoturbe halduse süsteemi toimimise 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 liikmele. Infoturbe halduse süsteemi rakendamise korraldamisel on juhatusel ka õigus jaotada ära infoturbe halduse süsteemi toimimiseks vajalikud tegevused (vt ka § 2 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*).

Küberturvalisuse 2. direktiivi preambuli põhjenduse 137 kohaselt on direktiivi eesmärk ka tagada kõrgel tasemel vastutus küberturvalisuse riskijuhtimismeetmete rakendamise ja teatamiskohustuse täitmise eest elutähtsate ja oluliste üksuste tasandil. Seepärast peaksid elutähtsate ja oluliste üksuste juhtorganid kiitma küberturvalisuse riskijuhtimismeetmed heaks ja jälgima nende rakendamist. Sellest tulenevalt on eelnõukohases määruses toonitatud organisatsiooni juhatuse vastutust. KüTSi § 6[1] lg 1 kohustab samas määrama vähemalt ühe juhatuse liikme, kes kiidab heaks turvameetmed, jälgib nende rakendamist ja vastutab selle eest. See isik või isikud on organisatsiooni sees peamised valdkonna koordineerijad, võimaldades teistel juhatuse liikmetel keskenduda muudele valdkondadele organisatsiooni juhtimisel. Kuid sellega ei võeta juhatuselt õigusaktidega ettenähtud kollektiivset vastutust, millele viitab ka sama paragrahvi lõige 3, sätestades: *Kui teenuseosutaja ei määra käesoleva paragrahvi lõikes 1 nimetatud juhatuse liiget, kohaldatakse käesolevas paragrahvis sätestatud kohustusi kõigile juhatuse liikmetele.*

Paragrahvi 4 *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, autentsus);
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, lepingute ja standardite järgimisel dokumendis esitatud 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 5. 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 peab organisatsioonis tuvastama äriprotsessile olulised varad (sh IT-vara) ja määrama kindlaks nende kaitseala. Kaitseala tuleb kindlaks määrata ning vajaduse korral ajakohastada ka jooksvalt soetatava vara puhul.

Sätte eesmärk on selgemalt ära märkida, et kaitsealasse kuuluvad kaitstavad äriprotsessid ja nendega seotud varad. Kaitsealast võib välja jätta näiteks selliste teenustega seotud äriprotsessid, mida ei rakendata KüTSi § 3 lõigetes 2–5 nimetatud tegevusaladel. Samuti võib välja jätta äriprotsessidega mitte seotud varad (nt kontoris asuvad muusika- ja spordiseadmed). Välja jätmise eelduseks on, et need kaitsealasse mitte kuuluvad varad ei ohusta KüTSi § 3 lõigetes 2–5 nimetatud tegevusaladega seotud varasid.

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

- äriprotsessidele mõju avaldavate riskide tuvastamine ja hindamine, 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.

Konsolideeritud teenuste (nt ministeeriumite valitsemisalade IT-majad) puhul võib organisatsioon meetmete väljatöötamise ja rakendamise jätta teenusepakkuja kohustuseks – see tähendab, et ka nendest teenustest lähtuvate meetmetega seotud riskihalduse saab delegeerida teenusepakkujale (vt ka paragrahvi 10 selgitused).

Paragrahvis 6 kirjeldatakse infoturbekataloogi olemust. Infoturbekataloog on organisatsiooni kahjustada võivate ohtude kaitseks võetavate meetmete loend moodulite kaupa. 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 7 käsitletakse infoturvameetmete rakendamise plaani. Infoturvameetmete rakendamise plaan (edaspidi ka *IMR*) on ühest või mitmest dokumendist koosnev kava, milles kirjeldatakse, kuidas organisatsioonis teavet ja vara kaitsta ning võimalikke riske ennetada. IMRis esitatakse kokkulepitud turvameetmed ja vastutajad ning käitumisjuhised erinevateks olukordadeks. IMRi võib hallata riskiregistris.

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 (organisatsioonivälise 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.

Eelnõukohane määrus ei näe ette, et tegemist peab olema lõpliku riski (jääkriski) aktsepteerimisega. Küll võib lugeda tegevuskava olemasolu soovitavate meetmete rakendamiseks riskide aktsepteerimisel, näidates tegevuskavas ära, kuidas toimub riski järkjärguline maandamine, mille kaudu saavutatakse kas riski minimeerimine või tase, mille puhul jääkrisk on aktsepteeritav.

Paragrahvis 8 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 9. Eelnõu koostamise käigus vaadati üle määruse nr 101 lisas sätestatud auditeerimiseeskiri.
Võrreldes E-ITSi kehtiva versiooniga ei ole enam auditi osana sätestatud eelauditit, vaheauditit ega 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) tuvastatud ja hinnatud äriprotsessidele mõju avaldavad riskid;
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.

Eelnõukohase määrusega ei piirata organisatsiooni võimalust soovi korral audiitorettevõttelt auditi järeldusotsuse auditileidude kõrvaldamisel uue järeldusotsuse tegemist tellida (nö järelaudit), kui leidude puhul on asjakohased meetmed rakendatud. See võimaldab

organisatsioonil vältida seda, et kuni järgmise korralise auditini kehtib järeldusotsus koos kõrge riskitasemega leidudega. Ka selline järeldusotsus tuleks esitada järelevalveasutusele.

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.

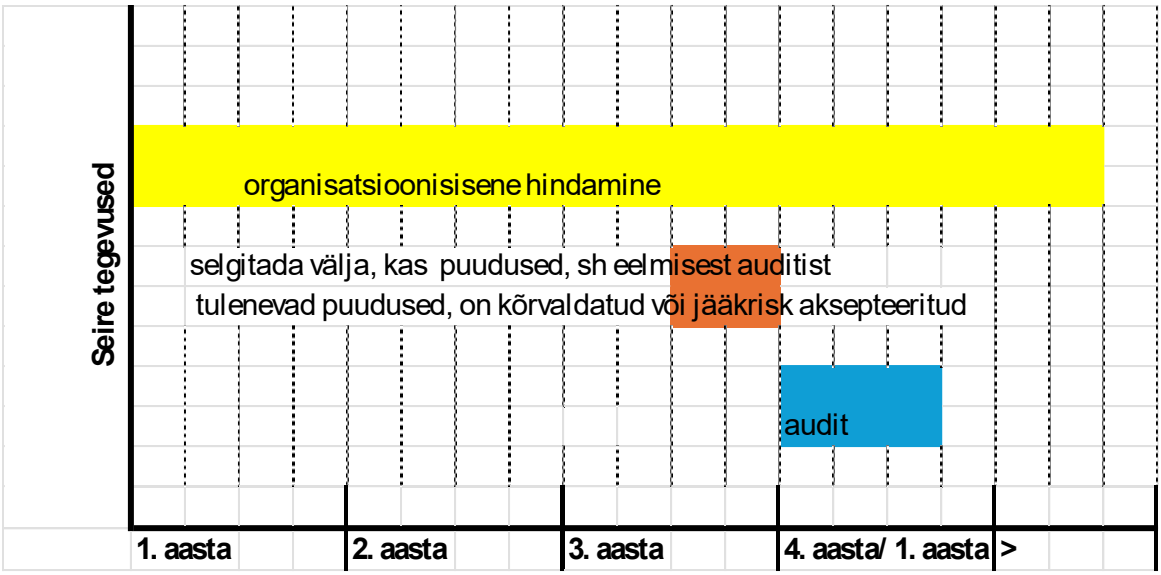
Lõikes 3 sätestatakse, et organisatsioonisisese hindamise käigus tuvastatud puudused ning eelmise auditi järel kavandatud parandusmeetmed peaksid olema vastavalt kas kõrvaldatud või rakendatud ning riskid aktsepteeritud. Sealhulgas arvatakse selle hulka ka infoturvameetmete rakendamata jätmisest tulenevate riskide põhjendatud aktsepteerimine (vt ka § 7 lõigete 7–9 selgitus). 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 10 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. Konsolideeritud teenuste puhul, kui turvameetmete väljatöötamine ja rakendamine on jäetud teenuseosutaja kohustuseks saab organisatsioon kontrollide meetmete täitmist kontrollida teenuseosutaja vastavusauditi kaudu.

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. Auditeerimiseeskiri on eelkõige mõeldud reguleerima määruse nr 121 § 4 lõigetes 1 ja 1^1 sätestatud auditi tegemist, piiramata samas organisatsiooni vabadust kasutada eeskirja organisatsiooni vajadustest lähtuvalt osaliste auditite tegemisel.

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 nende efektiivsust, 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 11** 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, 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]

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

Paragrahv 12. Eelnõukohase määrusega tunnistatakse kehtetuks E-ITSi kehtiv versioon, mistõttu nähakse ette üleminekuperiood. Turvameetmete rakendamine ja riskide hindamine on pidev protsess, seega on ka organisatsioonipoolne meetmete kohandamine pidev protsess ning nende uuendamisel on soovitatav järgida juba eelnõukohases määruses sätestatut. Dokumentatsiooni ülevaatamiseks, sealhulgas auditi eelduseks oleva organisatsiooni hindamise korraldamiseks nähakse ette kolmeaastane periood. Perioodi pikkuse määramisel on arvestatud senise auditeerimise välbaga, mis on sätestatud määruses nr 121. Kuna dokumentide ülevaatamine ja uuendamine toimub organisatsioonisisese hindamise käigus, on üleminekuperiood piisav. Eelnõukohase määruse jõustumise korral ei ole ühelgi organisatsioonil kohustust alustada kohe turvameetmete ülevaatamist või jätta pooleli juba toimuv audit või koostada uusi dokumente. Eelnõukohase määrusega väheneb asjaomaste sätete hulk, kuid ei muudeta vajadust kaitsta võrgu- ja infosüsteeme. Seega on kehtiva määruse alusel tehtud audit ja rakendatud turvameetmed asjakohased ka pärast uue määruse kehtima hakkamist.

Paragrahvis 13 nähakse ette määruse nr 101 (RT I, 28.08.2025, 12) kehtetuks tunnistamine eelnõukohase määruse jõustumisel. Määrus jõustub **paragrahvi 14** kohaselt 1. septembril 2026 (vt ka seletuskirja p 7 „Määruse jõustumine“).

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

3. Eelnõu terminoloogia

Eelnõukohases määruses esitatakse ühe kasutatava termini määratlus:
äriprotsess – organisatsiooni põhitegevuste või eesmärkide saavutamiseks vajalike tegevuste kogum, mille käigus kasutatakse aega, raha, töövahendeid ning inimeste teenuse, toote või muu väärtust loova tulemuse pakkumiseks.

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, riigivalitsemist ning infotehnoloogiat ja infoühiskonda.

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

5.1. 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 turvameetmete vormikohasuse asemel senisest enam 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.

5.2. Mõjuvaldkond: küberkeskkond ja küberhügieen (infotehnoloogia ja infoühiskond)

Mõju sihtrühm: ühiskonna toimimise seisukohast ülioluliste ja oluliste teenuste kasutajad (Eestis resideeruvad juriidilised ja füüsilised isikud).

Avalduv mõju ja mõju olulisus
Eelnõukohase määrusega vähendatakse keskselt ettekirjutatud regulatsiooni, jättes samaks üldised eesmärgid küberkeskkonna ja küberhügieeni osas. Ettekirjutatud regulatsiooni vähendamise tulemusel peaks muutuma ülioluliste ja oluliste teenuseosutajate võrgu- ja infosüsteemide kaitse senisest paindlikumaks ja looma võimalused kiiremaks reageerimiseks süsteeme ohustavatele sündmustele ja riskidele.

Järeldus mõju olulisuse kohta: eelnõukohase määruse jõustumisega kaasnev muudatus toetab turvalisuse küberkeskkonna toimimist ülioluliste ja oluliste teenuste osutamisel, tagades kasutajatele seeläbi nende teenuste jätkuva kättesaadavuse vähemalt senisel tasemel. Seega määruse üldine mõju on positiivne, kuid kasutaja seisukohast siiski oluline.

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. septembril 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

8.1. Eelnõu esitati eelnõude infosüsteemi kaudu kooskõlastamiseks ministeeriumitele, Riigikantseleile ning Eesti Linnade ja Valdade Liidule.

8.2. Eelnõu saadeti 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.

8.3. Eelnõu saadeti 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.

8.4. Eelnõu kooskõlastasid märkusteta Kultuuriministeerium ja Välisministeerium.

8.5. Eelnõu toetasid Finantsinspektsioon ja Riigikogu Kantselei.

8.6. Eelnõu kohta esitasid märkusi Kliimaministeerium, Rahandusministeerium, Majandus- ja Kommunikatsiooniministeerium, Siseministeerium, Sotsiaalministeerium, Eesti Linnade ja Valdade Liit, Andmekaitse Inspektsioon, Registrite ja Infosüsteemide Keskus, Riigi Info- ja Kommunikatsioonitehnoloogia Keskus, Eesti Haiglate Liit, Eesti Infosüsteemide Audiitorite Ühing, Eesti Kaubandus-Tööstuskoda, Eesti Vee-ettevõtete Liit ja Eesti Energia AS. Märkustega arvestamise tabel on esitatud seletuskirja lisas.

Märkuste tabel

	Märkus	Märkusega arvestamine
	Kliimaministeerium 29.06.2026 e-kiri	
1.	**Riskide aktsepteerimine (§ 8 lg 6)** Praegune sõnastus võib jätta mulje, et kui riski maandamistegevus kavandatakse kaugemale tulevikku kui järgmine regulaarne riskide ülevaatus, tuleb risk igal juhul aktsepteerida. Praktikas võivad suure organisatsiooni taristuprojektid kesta üle aasta, kuid see ei tähenda, et risk oleks sisuliselt tingimusteta aktsepteeritud. Palume täpsustada, et üle ühe aasta kestva maandamistegevuse puhul ei loeta riski automaatselt lõplikult aktsepteerituks, vaid risk peab olema käsitletud riskihalduses koos põhjendatud maandamiskava, ajutiste kompenseerivate meetmete, vastutaja ja tähtajaga. Kui jääkriski otsustatakse taluda kuni maandamistegevuse elluviimiseni, peab otsus olema dokumenteeritud ja regulaarselt üle vaadatud.	**Antud selgitus** Eelnõukohase määruse teksti § 7 lg 7 mõtte kohaselt (end § 8 lg 7), tuleks meetme rakendamise tähtaeg kehtestamisel lugeda aktsepteeritud riskiks. Säte ei näe ette, et tegemist peab olema lõpliku riski (jääkriski) aktsepteerimisega. Küll on ka tegevuskava soovitavate meetmete rakendamiseks riskide aktsepteerimine, samal ajal näidates ära kuidas toimub riski järk-järguline maandamine, mille kaudu saavutatakse kas riski minimaliseerimine või saavutatakse tase, millel jääkrisk on aktsepteeritav.
2.	**Organisatsioonisisese hindamise puuduste kõrvaldamine enne auditit (§ 10 lg 3 ja lisa 2 p 5.1)** Kehtiv sõnastus on liiga absoluutne, sest ka madala riskiga formaalne puudus võib takistada auditi alustamist. Palume kaaluda sõnastust, mille kohaselt võib auditeerimist alustada juhul, kui kõrvaldamata puudused on madala riskitasemega või nende kohta on kinnitatud põhjendatud	**Arvestatud** Määruse teksti ja lisa täiendatud viitega, et ka infoturvameetmete rakendamata jätmisest tulenevad riskid peavad olema aktsepteeritud.

	Märkus	Märkusega arvestamine
	parandusplaan ning need ei mõjuta oluliselt auditi teostatavust ega tulemuste usaldusväärsust.	
3.	**Audiitorettevõttele seatavad infoturbenõuded (lisa 2 p 4.8 ja 4.9)** Audiitor saab auditi käigus ligipääsu võrguskeemidele, logidele, õiguste näidetele, dokumentatsioonile ning potentsiaalselt tundlikule IT- ja OT-teabele. Praegused nõuded piirduvad peamiselt konfidentsiaalsuse, sõltumatuse ja parimate tavadega. Teeme ettepaneku kehtestada audiitorettevõttele minimaalsed infoturbenõuded või nõuda audiitorettevõttelt infoturbestandardile vastavust.	**Antud selgitus** Määrusega ei ole lubatud Eesti infoturbestandardi (edaspidi *E-ITS*) järgimise kohustuse panemist ettevõtjale, kellel seadusest tulenevalt vastav kohustus puudub. Küll on organisatsioonil, kellel on Eesti infoturbestandardi järgmise auditeerimise kohustus võimalik auditeerimise teenuse hankimisel või ostmisel lisada tingimustesse audiitorettevõtte minimaalsed infoturbenõuded või nõuda audiitorettevõttelt infoturbestandardile vastavuse kinnitust.
4.	**Teenusepakkujate infoturbe hindamine (lisa 2 p 5.10)** Paljudel praktilistel, eriti väiksematel või OT-teenusepakkujatel ei pruugi olla ISO/SOC/E-ITS sertifikaati ega selle rakendamise kohustust. Kui hindamine tugineb üksnes sertifikaatidele ja vastavusauditite, võib see muuta teenuste sisseostmise mõnes sektoris ebamõistlikult keeruliseks või kalliks. Palume lisada, et teenusepakkuja hindamisel võib arvesse võtta ka lepingulisi infoturbenõudeid, kliendi tehtud riskihinnangut ja kompenseerivaid meetmeid.	**Arvestatud** Lisa punkti 5.10. täiendatud ettepanekust lähtuvalt. *Hinnangu kujundamisel võib arvesse võtta ka lepingulisi infoturbenõudeid, organisatsioon koostatud riskihinnangut teenuseandja teenuse kohta ja riskihinnangust lähtuvate meetmete rakendamist.*
5.	**Kõrge riskiga leidude kõrvaldamise tähtaeg (lisa 2 p 7.3)** Kõrge riski maandamine võib suure organisatsiooni puhul eeldada hanget, arhitektuurimuudatust, eelarvet, tarnija arendust või OT-seisakute planeerimist. Seetõttu võib kuue kuu tähtaeg olla teatud juhtudel ebarealistlik. Palume lisada võimalus põhjendatud tähtaja pikendamiseks juhul, kui kõrge riski kõrvaldamine eeldab hanget, arhitektuurimuudatust, eelarveotsust, tarnija arendust või tehnoloogilist seisakut ning kui auditeeritav on rakendanud	**Arvestatud** Punkti 7.3 täiendatud lausega: *Kui auditeeritaval ei õnnestu kuue kuu jooksul seda riski kõrvaldada, koostab ta riski käsitlemise plaani, milles kirjeldab riski vähendamiseks rakendatud meetmeid ja riski kõrvaldamiseks rakendatavaid ajutisi meetmed ning määrab plaani rakendamise eest vastutaja.* Lisa täiendatud uue punktiga 7.5.

	Märkus	Märkusega arvestamine
	ajutised maandamismeetmed, kinnitanud tegevusplaani, määranud vastutaja ja teavitanud sellest järelevalveasutust.	*7.5. Punktis 7.3 sätestatud tegevusplaani koostamisest teavitab auditeeritav järelevalve asutust 14 päeva jooksul tegevusplaani koostamisest, kuid mitte hiljem kui kuue kuu möödumisest auditi järeldusotsuse ja auditi lõpparuande saamisest arvates.*
6.	**Auditi käsitlusala määratlemine (lisa 2 p 3.1)** Eelnõu lisa punkt kohaselt määrab auditeeritav auditit tellides või hankides käsitlusala. Siin on oht, et käsitlusala määratakse liiga kitsalt ning audit ei kata organisatsiooni olulisemaid riske. Palume täpsustada, et auditi käsitlusala ei tohi olla määratud viisil, mis jätab põhjendamatult välja organisatsiooni olulised või kriitilised äriprotsessid, nende toimimiseks vajalikud varad, tegevuskohad, välised teenusepakkujad või kõrgema kaitsetarbega süsteemid. Audiitor peab hindama käsitlusala piisavust ning märkima olulised piirangud auditi lõpparuandes ja vajaduse korral järeldusotsuses.	**Arvestatud sisuliselt** Punkti täiendatud lausega: *Käsitlusala peab hõlmama vähemalt küberturvalisuse seaduse § 3 lõigetes 2–5 nimetatud tegevusaladega seotud võrgu- ja infosüsteeme.* Viitamine eelmärk on tagada, et auditi tehakse vähemalt võrgu- ja infosüsteemide osas, mis on seotud teenustega, mille osutamise kaudu on organisatsioon KüTS subjekt. Samas juhime tähelepanu, et auditeerimiseeskiri on eelkõige mõeldud kasutamiseks eelnõukohases määruses sätestatud infoturbehalduse meetmete audit tellimiseks või hankimiseks, auditi tegemiseks. Eelnõukohase määrusega ei ole piiratud organisatsiooni vabadust tellida samu põhimõtteid järgides iseseisvaid auditeid või osalisi auditeid.
7.	**Auditi lõpparuande kaitse (lisa 2 p 6.18)** Kui auditi järeldusotsuses on üks või mitu kõrge tasemega riski, tuleb järelevalveasutusele esitada ka auditi lõpparuanne. See võib sisaldada väga tundlikku teavet. Palume määruses selgemalt välja tuua, kuidas auditi lõpparuannet kaitstakse, märgistatakse, edastatakse ja säilitatakse, kui see sisaldab juurdepääsupiiranguga või muud tundlikku teavet, sh infot süsteemiarhitektuuri, turvanõrkuste, logide, õiguste või OT/IT keskkonna kohta.	**Antud selgitus** Riigi Infosüsteemi Amet tagab dokumendi kaitse lähtuvalt organisatsiooni poolt ettenähtud kaitsetasemele. Kui organisatsioon on märkinud järeldusotsuse ärisaladuseks või asutusesiseseks kasutamiseks mõeldud teabeks, peab Riigi Infosüsteemi Amet tagama ka teabe sellisel kujul hoidmise ning kaitse jne.

	Märkus	Märkusega arvestamine
8.	**OT kohaldamisala täpsustamine** E-ITS 2026 määratleb OT jaoks SYS.7 mooduli, kuid ei täpsusta, et OT keskkonnale võivad kohalduda ka muud moodulid (nt võrk, tarneahel, intsidentide käsitlus). Ettepanek: Täpsustada, et OT-le tuleb rakendada kõiki asjakohaseid mooduleid.	**Jäetud arvestamata** Soovime vältida määruses liigset detailsust arvestades tehnoloogia kiiret arengut. Täpsemaid ajakohaseid juhiseid on kavas avaldada Riigi Infosüsteemi Ameti veebilehel.
9.	**OT kaughoolduse nõuete konkretiseerimine** SYS.7.6 nõuab turvalist kaughooldust, kuid miinimumnõuded puuduvad. Ettepanek: Lisada nõuded (MFA, ajutised ligipääsud, logimine, eraldatud kanalid).	**Jäetud arvestamata** Soovime vältida määruses liigset detailsust arvestades tehnoloogia kiiret arengut. Täpsemaid ajakohaseid juhiseid on kavas avaldada Riigi Infosüsteemi Ameti veebilehel.
10.	**Riskihindamise skaalade kaotamine** Ühtsete skaalade kaotamine vähendab võrreldavust organisatsioonide vahel. Ettepanek: Luua soovituslik riiklik metoodika ja minimaalne skaala.	**Antud selgitus** Riigi Infosüsteemi Ametil on jooksvalt kavandatud veebilehel avaldada riskihindamist abistavaid rakendusi ehk nö tööriistu.
11.	**CIA vs OT (Safety)** CIA mudel ei kata piisavalt OT ohutusriske. Ettepanek: Lisada Safety eraldi kaitstava väärtusena.	**Jäetud arvestamata** Soovime vältida määruses liigset detailsust arvestades tehnoloogia kiiret arengut. Täpsemaid ajakohaseid juhiseid on kavas avaldada Riigi Infosüsteemi Ameti veebilehel.
12.	**Infoturbepoliitika OT käsitlus** Poliitikad on sageli IT-kesksed ja ei kata OT-d piisavalt. Ettepanek: Nõuda OT käsitlemist poliitikas.	**Jäetud arvestamata** Soovime vältida määruses liigset detailsust arvestades tehnoloogia kiiret arengut. Täpsemaid ajakohaseid juhiseid on kavas avaldada Riigi Infosüsteemi Ameti veebilehel.
13.	**Ühtne riskihaldusmetoodika**	**Antud selgitus**

	Märkus	Märkusega arvestamine
	Ilma ühtse metoodikata puudub võrreldavus. Ettepanek: kehtestada ühine metoodika.	Eelnõu § 11 näeb ette E-ITS rakendamisel Riigi Infosüsteemi Ameti poolsed tugitegevused. Tugitegevustena on ära näidatud veebilehe loomine, millel avaldatakse juhendmaterjale E-ITS rakendamise toetamiseks ja ühtlustamiseks Vaata ka Siseministeeriumi märkusele nr 1 ja Riigi Info- ja Kommunikatsioonitehnoloogia Keskuse märkusele nr 3 antud vastust.
14.	**Juhendmaterjalide vajadus** Vähenenud detailsus võib tekitada tõlgendamisprobleeme. Ettepanek: RIA peaks avaldama standardiseeritud juhised ja näidised.	**Antud selgitus** Eelnõu § 11 näeb ette E-ITS rakendamise Riigi Infosüsteemi Ameti poolsed tugitegevused. Vaata ka Eesti Infosüsteemide Audiitorite Ühingu märkusele nr 1 antud vastust.
Majandus- ja Kommunikatsiooniministeerium 10.06.2026 e-kiri		
	Majandus- ja kommunikatsiooniministeerium edastab Eesti Standardimis- ja Akrediteerimiskeskuse tähelepanekul kommentaari seoses EIS-s kommenteerimisel oleva eelnõuga „Eesti infoturbestandard“ (EIS-i toimik JDM/26-608) Kommentaar puudutab **eelnõu seletuskirja.** Seletuskirja **§ 5 lõike 1** selgituses (lk 8) on välja toodud, et organisatsiooni väärtustena tuleks kindlasti arvesse võtta ka õigusaktide, eeskirjade, standardite ja lepingute nõuete täitmist.	**Arvestatud**

	Märkus	Märkusega arvestamine
	Mainitud sõnastusest tuleneb üldine standardite järgimise kohustus. Kuna standardite järgimine on üldjuhul vabatahtlik, siis teeme ettepaneku sõnastada standardite nõuete täitmise osa soovituslikuna, nt ühe võimaliku sõnastusena: *e) õigusaktide, eeskirjade, lepingute ja standardite järgimisel standardite nõuete täitmine*	
	Rahandusministeerium 08.07.2026 kiri nr 1.1-11/2256-2	
1.	Eelnõu § 4 kasutab mõistet „organisatsiooni juhatus“, kuigi määrus kohaldub küberturvalisuse seaduse tähenduses teenuseosutajatele, kelle hulka kuuluvad ka riigiasutused, kohaliku omavalitsuse üksused ja muud organisatsioonivormid, millel klassikaline juhatus puudub. Kuigi seletuskirjas on selgitatud, et juhatuse all peetakse silmas organisatsiooni kõrgeimat juhtimistasandit (nt asutuse juht, täitevorgan vms), ei tulene see üheselt määruse tekstist. Teeme ettepaneku täpsustada § 4 sõnastust, kasutades neutraalsemat terminit, nt „organisatsiooni kõrgeim juhtimistasand“, või defineerida „juhatus“ § 2 terminina selliselt, et see hõlmab kõiki küberturvalisuse seaduse subjektide juhtimisvorme.	**Jäetud arvestamata** Eelnõu arvestab küberturvalisuse seadusega (edaspidi *KüTS*). Näiteks nimetatud seaduse § 6^1 sätestab juhatuse liikme kohustused.
2.	Eelnõus kasutatud mõistete valik ei ole piisavalt ühtne ja pigem on segadust tekitav. Kuigi § 3 lõike 2 kohaselt kasutatakse mõistet „infoturbejuht“, ei kasutata seda mõistet järjepidevalt ei eelnõus tervikuna ega seletuskirjas, kus on kasutatud ka teistsugust väljendust „infoturbe eest vastutav isik“. Samuti jääb ebaselgeks, miks on valitud just mõiste „hankejuht“, kuigi seletuskirjas on	**Arvestatud sisuliselt** Rollid asendatud tegevustega, mida on vaja arvestada infoturbe halduse süsteemi toimimisel. Lisatud andmekaitse. Andmekaitse hõlmab organisatsiooni kui ka organisatsioonile usaldatud

	Märkus	Märkusega arvestamine
	selgitatud, et vastavaid ülesandeid võivad täita erinevad rollid jääb ikkagi ebaselgeks, miks on vajalik eraldiseisva mõiste kasutamine eelnõus. Palume eelnõus kasutatud mõisted tervikuna üle vaadata ning tagada nende ühtne ja põhjendatud kasutus. Mõistete valikul tuleb lähtuda kehtivast terminoloogiast ning vältida olukorda, kus sama sisu kirjeldamiseks kasutatakse erinevaid või sisult ebaselgeid mõisteid.	andmete kaitse kavandamist ja korraldamist. Muu hulgas hõlmab ka isikuandmete kaitset organisatsiooni poolt, kes neid töötleb.
3.	Eelnõu § 8 lõike 8 eesmärk on toetada organisatsiooni kohustust hinnata organisatsioonivälise tarneahelaga seotud riske (§ 8 lg 7). Kehtiv sõnastus annab organisatsioonile õiguse nõuda teenusepakkujalt tõendusmaterjali, kuid ei rõhuta piisavalt, et hinnangu andmiseks peab organisatsioonil olema ligipääs asjakohasele ja piisavale teabele. Teeme ettepaneku sõnastada säte järgmiselt: (8) Organisatsioonivälise tarneahela kaitse vajaduse hindamiseks on organisatsioonil õigus nõuda väliselt osapoolelt kaitsetarbele vastavate turvameetmete rakendamist tõendavat teavet, sealhulgas seirearuandeid, asjakohase käsitlusalaga auditi järeldusotsuseid, turvasertifikaate, enesehindamise tulemusi või muud asjakohast teavet.	**Jäetud arvestamata** Eelnõukohase määrusega sätestatakse nõuded vaid KüTS subjektidele, sh teenuseosutajatele (organisatsioonid). Teenuseosutaja lepingulistele või muudele partneritele ei ole võimalik määrusega kohustusi kehtestada. Teenuseosutaja ja tema lepinguliste partnerite (st väliste teenuste osutajatega) suhe põhineb vastastikustel lepingutel (sh tüüplepingud), milles sätestatakse muuhulgas ka teenuseosutaja võimalused saada teavet osutatava teenuse kohta.
4.	Määruse lisa 2 punkt 2.4 seab kaugtöö vormis tehtavatele auditiprotseduuridele 30 protsendi ülempiiri. Pilvteenuste, SaaS-lahenduste, hajustaristu ja väliste teenusepakkujate puhul ei pruugi füüsiline kohalkäik alati anda parimat tõendusväärtust. Mõnel juhul on kvaliteetsem tõendus kättesaadav hoopis turvalise kaugjuurdepääsu, ekraanijagamise, konfiguratsiooni läbivaatuse, logianalüüsi või dokumenteeritud kontrolljälje kaudu. Meie	**Arvestatud sisuliselt** Lisa 2 punkt 2.4. sõnastatud järgmiselt: *2.4. Auditi tegemine plaanitakse koostöös auditeeritava kontaktisikuga, kes tagab vajalike andmete ja isikute kättesaadavuse auditi ajal. Põhjendatud juhtudel ja eelneval kokkuleppel võib auditiprotseduure teha kaugtöö vormis, sellisel*

	Märkus	Märkusega arvestamine
	hinnangul peaks auditi vorm lähtuma tõendusmaterjali piisavusest, mitte jäigast protsendipiirist. Seega teeme ettepaneku asendada 30 protsendi piir riskipõhise käsitlusega. Võimalik sõnastus: „Auditiprotseduure võib teha kaugtöö vormis, kui auditi eesmärk, käsitlusala, riskid ja tõendusmaterjali laad seda võimaldavad ning audiitor saab kujundada piisava ja asjakohase hinnangu. Füüsiline paikvaatlus tehakse ulatuses, mis on vajalik füüsiliste, keskkonna- ja tegevuskohapõhiste kontrollide hindamiseks. Pilvteenuste, hajustaristu ja väliste teenusepakkujate kontrollimisel võib kasutada kaugprotseduure, kui need annavad piisava tõendusväärtuse. Kaugtöö vormis tehtud auditiprotseduurid, nende põhjendus ja piirangud kajastatakse auditiaruandes.“.	*juhul kajastatakse see fakt auditi lõpparuandes ja auditi järeldusotsuses koos kaugtöö vormis tehtud auditi käsitlusala kirjeldusega.*
	Lõpetuseks märgime, et on tervitatav, et eelnõuga lihtsustatakse nõudeid ning muudetakse neid erinevatele organisatsioonidele paremini rakendatavaks. Samas peame oluliseks, et Riigi Infosüsteemi Amet hoiaks ka edaspidi ajakohasena ja kättesaadavana E-ITS rakendamist toetavad juhendmaterjalid, sealhulgas etalonturbe kataloogi moodulites esitatud detailsema käsitluse, mis hõlmab turvameetmete kirjeldusi, tüüpilisi ohte ning soovituslikke lahendusi.	**Võetud teadmiseks**
	Siseministeerium 14.07.2026 kiri nr 1-7/160-6	
1.	**E-ITS lahti sidumine ISO standardist** Seletuskirjas rõhutatakse E-ITSi lihtsustamist ja nõuete arusaadavuse parandamist. Samas toob ISO standardist eemaldumine kaasa ühe rahvusvaheliselt tunnustatud	**Antud selgitus** Eelnõukohase määruse koostamisel on arvesse võetud, et organisatsioonidel säilib võimalus kasutada rahvusvahelist

	Märkus	Märkusega arvestamine
	võrdlusraamistiku kadumise. See võib praktikas muuta nõuete tõlgendamise ja rakendamise keerukamaks, mitte lihtsamaks. Selgema arusaadavuse tagamiseks ning koostöö hõlbustamiseks (sh rahvusvaheliste partnerite, audiitorite ja teenuseosutajatega) oleks otstarbekas lisada E-ITSi ja ISO/IEC 27001 põhimõtete vaheline vastendamine või suunav juhendmaterjal. Samuti võib vastavustabeli või juhendite puudumine kaasa tuua organisatsioonides dubleerivat tööd, näiteks: nõuete tõlgendamisel, turvameetmete valikul ja rakendamisel, teenuslepingute tingimuste kujundamisel.	standardit ISO/IEC 27001 või Eesti standardit EVS-EN ISO/IEC 27001. Seetõttu ei ole mõistlik kehtestada samasisulist nõuet riigi poolt. E-ITSi kehtiva versiooni rakendamine on paljudele organisatsioonidele osutunud koormavaks, sealhulgas on tõstnud esile küsimusi selle rakendamise kohta ja meetmete kohaldatavuse ning ulatuse kohta. Samuti on senine ISO standardiga seotus loonud olukorra, kus nõuded aeguvad kiiremine kui neid suudetakse ajakohastada ning õigusloome protsess on osutunud ka takistuseks ennetava vaate rakendamisel. Eelnõukohase määrusega seatakse esile eesmärgid ja põhimõtted, mida tuleb võrgu- ja infosüsteemi turvalisuse tagamisel silmas pidada. Samas vähendatakse ettekirjutatud meetmete hulka. Meetmete õigusaktiga reguleerimisel tuleb silmas pidada, et KüTS subjekte on ligikaudu 3000. See tähendab, et meetme kavandamisel (sh uuendamisel) tuleb arvestada kõigu nende võrgu- ja infosüsteemide eripäradega, muutes sellega meetme väljatöötamise aeganõudvaks ja hetkel kui meede kehtestatakse võib see juba mõne subjekti osas osutada piiravaks või ebaproportsionaalseks jne. Samas ei ole ka rahvusvahelist standardi ISO/IEC 27001 rakendamine olnud ühtlane, ehk standardit ei ole rakendatud organisatsiooni põhiselt vaid osadele teenustele. Küberturvalisuse 2. direktiivi ülevõtmisega nähti ette organisatsioonipõhine turvameetmete rakendamine. Küll ei ole jätkuvalt mõistlik nõuda organisatsioonipõhiselt ühtselt kõrgemate meetmete rakendamist ja auditeerimist. Seetõttu on lubatud KüTS subjektide organisatsiooniüleselt rakendada võrgu- ja infosüsteemide kaitseks erineval tasemel meetmeid, kuid kõik KüTS subjektid peavad turvameetmete rakendamisel alustama esmaste turvameetmete rakendamisest, millele vajadusel järgneb

	Märkus	Märkusega arvestamine
		osutatavtest teenustest tulenevate nõuete rakendamine. Arvestades ülaltoodut, ei ole üldine vastendamine asjakohane. Eelnõukohases määruses nähakse ette Riigi Infosüsteemi Ameti õigus avaldada veebilehel E-ITS rakendamist toetavaid juhiseid ja rakendusi. Selliste juhiste ja rakenduste kaasabil toimib ka nõuete rakendamise ühtlustumine ja ajakohane rakendamine.
2.	**Ohupilt ja dünaamiline küberturvalisuse keskkond** Tänapäevase kiiresti muutuva ohupildi kontekstis võiks standard käsitleda senisest selgemalt dünaamilist ohuteavet ja selle kasutamist. See hõlmab eelkõige: a. CERT-EE hoiatuste ja ohuhinnangute süsteemsemat kasutamist, b. tarkvara ja teenuste tarneahela küberturvalisuse riske (sealhulgas arvestades, et sertifikaadid üksi ei pruugi olla piisavad), c. pilveteenustega seotud spetsiifilisi riske, d. tehisintellekti kasutamisega kaasnevaid riske ja muutusi küberkeskkonnas. Kuigi eelnõu on tehnoloogianeutraalne, on tehisintellekti mõju küberdomeenis juba märkimisväärne ning selle käsitlemine vähemalt põhimõttelisel tasemel suurendaks regulatsiooni ajakohasust. Samuti võiks tugevamalt rõhutada organisatsioonide vahelise koostöö rolli, sealhulgas koostööd CERT-EE-ga.	**Antud selgitus** Nõustume, et organisatsioonide vaheline koostöö ja asjaomaste institutsioonide avaldatud teabe kasutamine küberturbe korraldamisel on mõistlik ning ka ressursse kokkuhoidev. Samas jääme seisukohale, et puudub vajadus eelnõukohases määruses sellise tegevuse sätestamiseks. Organisatsioonil ja selle juhtkonnal on õigus leida neile sobiv lahend, arvestades eelnõus sätestatut. Riigi Infosüsteemi Amet teostab KüTS nõuete täitmise üle riiklikku- ja haldusjärelevalvet. Korrakaitseorgani üks ülesandeid on ka ohu ennetamine, mis hõlmab ka teavitustegevust ja ohuhinnangute andmist. Riigi Infosüsteemi Ameti põhimääruse kohaselt kuulub põhisülesannete hulka ka koolitamis- ja nõustamistegevus, ennetustöö ja avalikkuse ohtudest teavitamise korraldamine.
3.	**Auditeerimise tsükkel** Kehtivas määruses on kasutusel mõiste „audititsükkel“. Uues määruse eelnõus ei ole seda mõistet otseselt sätestatud ega piisavalt selgitatud. Kuigi seletuskirjas on auditeerimise loogika osaliselt esitatud skeemina, ei ole kolmeaastane tsükkel normatiivsel tasandil üheselt arusaadav. Selline ebamäärasus võib	**Antud selgitus** E-ITSi auditeerimise ajatsükkel on kindlaks määratud Vabariigi Valitsuse 9.12.2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 4 lõigetes 1 (üldreeglina kolm aastat) ja 1^1 (elutähtsa teenuse osutajate puhul peab esmakordselt

	Märkus	Märkusega arvestamine
	praktikas kaasa tuua erinevaid tõlgendusi. Ettepanek on sätestada audititsükkel selges ja üheselt mõistetavas vormis kas määruses või auditeerimiseeskirjas.	tegema hädaolukorra seaduse § 38 lõike 1^3 punktis 3 sätestatud korras määratud tähtaja jooksul).
4.	**Eelnõus nimetatud rollid** Eelnõu § 3 lõige 2 sätestab, et infoturbe halduse süsteemi toimimiseks tuleb määrata sealsamas punktides 1-4 nimetatud rollid, milleks on „hankejuht“, „infoturbejuht“, „kasutaja“ ja „äriüksuse juht“. Rollidega külgnevalt on eelnõu seletuskirja lk 6 kolmandas ja neljandas lõigus selgitatud, et „Roll ei tähenda, et seda peab täitma sama ametinimetusega töötaja, vaid tegemist on tegevustega, millega organisatsioon peab arvestama.“ ning „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.“. SIM nõustub seletuskirjas toodud käsitlusega, et eelnõus nimetatud roll ei peaks tähendama, et seda peab täitma sama ametinimetusega töötaja. SIM mõistab eelnõuga taotletavat eesmärki selliselt, et infoturbe süsteemi toimimise tagamiseks on eeskätt tähtis, et organisatsioon on siseselt läbi mõelnud ja paika pannud, kes antud organisatsioonis täidab rollide juures kirjeldatud tegevusi. Hetkel see eelnõu tekstist selliselt välja ei tule vaid üksnes seletuskirjast. Ühtlasi leiame, et eelnõu § 3 lõike 2 punktis 1 kirjeldatud tegevuste eest vastutavale rollile antud nimetus „hankejuht“ on rollile määratud tegevusi silmas pidades eksitav.	**Arvestatud** Rollid asendatud tegevustega, mida on vaja arvestada infoturbe halduse süsteemi toimimisel. Lisatud andmekaitse. Andmekaitse hõlmab organisatsiooni kui ka organisatsioonile usaldatud andmete kaitse kavandamist ja korraldamist. Muu hulgas hõlmab ka isikuandmete kaitset organisatsiooni poolt, kes neid töötleb.

	Märkus	Märkusega arvestamine
	Kuigi seletuskirjas on toodud, et eelnõus ei mõisteta rolli „hankejuht“ all ostujuhti või riigihanke eest vastutajat, siis märgime, et tavapäraselt seostub avalikus sektoris sõnaga „hankejuht“ just riigihangete valdkonna töötaja ehk riigihanke menetluste läbiviija. Ülaltoodust lähtuvalt palume üle vaadata, kas piisab kui eelnõus jätta välja rollide nimetused ja sätestada organisatsioonile üksnes kohustus siseselt määrata, kes täidab eelnõu § 3 lõike 2 punktides 1-4 toodud tegevusi. Või alternatiivselt, üle vaadata eelnõus kasutatud rollide nimetused ning seejuures tagada, et ka eelnõust endast tuleb välja, et roll ei tähenda, et seda peab täitma sama ametinimetusega töötaja.	
5.	**Isikuandmete kaitse käsitluse täpsustamine** Eelnõu lisas 1 on eraldi protsessimoodulina ette nähtud GRC.4 „Isikuandmete kaitse“, kuid määruse normatiivses osas ei ole selgitatud, kuidas see moodul suhestub infoturbe halduse süsteemiga ning isikuandmete kaitset reguleerivatest õigusaktidest tulenevate kohustustega. Erinevate tõlgenduste vältimiseks võiks seletuskirjas või juhendmaterjalis selgitada, et GRC.4 eesmärk ei ole luua organisatsioonis eraldiseisvat andmekaitse juhtimissüsteemi, vaid toetada Euroopa Parlamendi ja nõukogu määrusest (EL) 2016/679 (IKÜM) tulenevate kohustuste täitmist tehniliste ja korralduslike meetmete rakendamisel ning andmekaitse lõimimisel organisatsiooni üldisesse riskijuhtimisse.	**Arvestatud sisuliselt** Seletuskirjas selgitatud andmekaitse alast tegevust.
	Riskihaldus ja andmekaitsealane mõjuhinnang Eelnõus käsitletakse infoturberiskide hindamist, kuid ei selgitata selle seost IKÜM artikli 35 kohase andmekaitsealase mõjuhinnanguga. Seletuskirjas võiks selgitada infoturberiskide hindamise ja andmekaitsealase mõjuhinnangu omavahelist seost.	**Antud selgitus** Eelnõukohases määruses ei nähta ette, et andmekaitse on vaid isikuandmete kaitse. Igal organisatsioonil on andmeid (teavet), mis vajab kaitsmist juba organisatsiooni oma eesmärkide

	Märkus	Märkusega arvestamine
	Praktikas viiakse mõlemad hinnangud sageli läbi sama projekti või infosüsteemi arendamise käigus. Juhised nende omavaheliseks sidumiseks aitaksid vältida dubleerimist ning toetaksid terviklikku riskijuhtimist. Samal ajal võiks selgitada ka nende hinnangute erinevat eesmärki ja fookust, et oleks arusaadav, millised riskid ja asjaolud kuuluvad infoturbe riskihindamise ning millised andmekaitsealase mõjuhinnangu käsitlusalasse.	kaitsmiseks. Näiteks ärisaladus, asutusesiseseks kasutamiseks mõeldud teave või mistahes muu teave, mille kolmandatele isikutele kättesaadavaks tegemine võib kahjustada organisatsiooni või tema kõrgemal seisva institutsiooni huve. Muidugi tuleb mõelda kuidas kaitsta organisatsioonile teiste isikute poolt usaldatud teavet või muud õiguspäraselt kogutud teavet, sh isikuandmeid. Seega andmekaitse on eelnõukohases määruses laiem kui vaid isikuandmete kaitse. Küll ei ole keelatud mõne muu õigusliku kohustuse raames tehtud hinnangut taaskasutada organisatsiooni riskihindamises.
7.	**Muud täpsustavad kommentaarid** Määruse seletuskirja lk 6 alguses olev lõik „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“ on segane ja mitmeti mõistetav, kuna ei saa üheselt aru kas see lõik käib ainult riskihindamise kohta või ka kaitsetarbe hindamise kohta? Kui ainult riskide kohta, siis kuidas siduda kaitsetarbe hindamine asutuse enda rakendatud riskikäsitlusega? Kuidas hinnata kaitsetarbe mõju riskikäsitluses. Lisanduvas juhendis võiks olla need lahti seletatud koos soovitusliku riskikäsitlusega.	**Võetud teadmiseks**
	Määruse väljasttellimise ja nõuetega on küsimus, kuidas lähtuda E-ITSi meetmest „*OPS.2.1.M7.a Infoturbe meetmete rakendatust*	**Antud selgitus**

	Märkus	Märkusega arvestamine
	tõendab teenuseandja välise audiitori poolt väljastatud E-ITS auditi järeldusotsusega või akrediteeritud“ kui E-ITS ei põhine enam ISO vastavusel. Kuidas sellest punktist lähtuda, et partneri asutuses olevast ISO-st piisab. Kuidas on tagatud tellija E-ITS-ist lähtuvate nõuete katmine, kui teenuseandja lähtub oma asutuses ISO rakendamisel enda asutuse vajadustest ja teenuslepetes ei reguleerita seetõttu piisavalt täpselt tellija nõudeid. Praktikas võib tekkida olukord, kus teenuseandja rakendab ISO standardit oma organisatsiooni vajadustest lähtudes, kuid teenuslepingutes ei ole tellija spetsiifilised E-ITSi nõuded piisava täpsusega sätestatud. Ettepanek on täpsustada kuidas peab tellija tagama E-ITS-i nõuete katvuse (all)hanke- ja lepingulistes suhetes.	Märkus edastatud Riigi Infosüsteemi Ametile veebilehel oleva teabe ülevaatamiseks. Eelnõukohase määruse lisa 1 OPS 2.1. Väljasttellimine üldiselt kohaselt peab organisatsioon esitama meetmed väljasttellitava teenuse turvaeesmärkide saavutamise tagamiseks kogu allhanke kestel. Ehk organisatsioon peab olema eelnevalt läbimõelnud, millist teavet ta allhankijalt vajab ning kuidas ta reageerib allhankest tulenevatele riskidele. Näiteks kui avalikus sektoris tegutsev organisatsioon on riigihankes sätestanud, et pakkuja peab teenuse pakkumisel ja kogu teenuse kasutamise perioodil omama teenuse osas rahvusvahelist standardi ISO/IEC 27001 või Eesti standardi EVS-EN ISO/IEC 27001 sertifikaati, siis sertifikaadi olemasolu saab juba lugeda üheks meetmeks.
	Sotsiaalministeerium 26.06.2026 kiri nr 1.2-3/1355-6	
1.	**Meetmete struktuuri muutus ja mõju auditeerimistsüklile** Eelnõuga muudetakse senise E-ITSi meetmete struktuuri olulisel määral. Kuigi toetame eesmärki muuta standard paindlikumaks ja riskipõhisemaks, võib muudatus praktikas tähendada, et olemasolevaid rakendusplaane, vastendusi ja auditeerimise ettevalmistusi ei ole võimalik uue mudeliga üks-ühele seostada. Seetõttu võib paljudel organisatsioonidel tekkida vajadus teha järgmise auditi eel sisuliselt uuesti kogu vastendamise ja infoturvameetmete rakendamise plaani koostamise töö. Palume kaaluda vana ja uue meetmestruktuuri ametliku vastavustabeli koostamist, pikema üleminekuperioodi sätestamist ning võimalust lugeda olemasolevad vastendused ja põhjendused	**Arvestatud osaliselt** Riigi Infosüsteemi Amet avaldab E-ITS rakendamist toetavad raames juhendmaterjalid oma veebilehel. § 12 (end 13) tekst sõnastatud järgmiselt: *(1) Enne käesoleva määruse jõustumist Eesti infoturbestandardi järgimiseks rakendatud turvameetmed, mis ei ole vastuolus määrusega, kehtivad kuni nende rakendamise lõppemiseni või ajakohastamiseni.* *(2) Enne käesoleva määruse jõustumist Eesti infoturbestandardi järgimiseks koostatud dokumentatsioon kehtib kuni kolm aastat määruse jõustumisest.*

	Märkus	Märkusega arvestamine
	teatud ulatuses ülekantuks. See aitaks vältida ebaproportsionaalset topelttööd ning suunaks organisatsioonide ressursi tegeliku infoturbe parandamisele.	*(3) Lõikes 2 sätestatud dokumentatsiooni uuendamisel määruses sätestatud korras enne lõikes 2 sätestatud tähtaja möödumist kehtib dokumentatsioon ettenähtud korra kohaselt.* Justiits- ja Digiministeerium arvestab Vabariigi Valitsuse poolt kehtestatud audititsüklit seetõttu ei toeta ülemineku aja muutmist.
2.	**Auditeerimise üleminekusätete täpsustamine** Eelnõu üleminekusätted näevad ette üleminekuperioodi olemasolevate dokumentide kasutamiseks, kuid eelnõust ei selgu piisavalt, kuidas viiakse üleminekuajal läbi auditeid. Praktikas on oluline, et nii organisatsioonidele kui ka audiitoritele oleks selge, millises ulatuses võib tugineda kehtiva E-ITSi alusel koostatud dokumentatsioonile, millal muutub uue struktuuri täielik rakendamine auditi eelduseks ning kuidas välditakse olukorda, kus organisatsioonid peavad samaaegselt haldama nii vana kui ka uut raamistikku. Palume täiendada eelnõu või auditeerimisega seotud juhiseid selliselt, et üleminekuajal kohaldatavad nõuded oleksid üheselt arusaadavad nii rakendajatele kui ka audiitoritele.	**Antud selgitus** Võrgu- ja infosüsteemide auditeerimise kohustus, sh tähtaeg tuleneb Vabariigi Valitsuse 9.12.2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“§ 3 lõikes 1. Selle kohaselt tuleb auditeerida iga kolme aasta järel. Seega nt aastal 2025 tehtud auditi korral ei ole vaja eelnõu kohase määruse jõustumisel teha uut auditit enne 2028. aastat.
3.	**Dokumenteerimiskohustuste proportsionaalsus** Toetame eelnõu eesmärki vähendada bürokraatiat ja suurendada organisatsioonide paindlikkust. Samas võivad § 3 lõikes 3 sätestatud dokumenteerimis- ja säilitamisnõuded mõnes osas tekitada täiendavat halduskoormust ilma selge lisandväärtuseta. Eelkõige vajab täiendavat põhjendamist infoturvasündmustele organisatsiooni reaktsiooni säilitamise kohustus ning infoturvameetmete rakendamise plaani säilitamise kohustus ulatuses, milles see ei ole vajalik juhtimise, tõendamise või õigusliku vastutuse seisukohast.	**Võetud teadmiseks** Eelnõu koostajate hinnangul ei kaasne eelnõukohase määruse jõustumisel uut bürokraatiat ja dokumenteerimise kohustust

	Märkus	Märkusega arvestamine
	Leiame, et säilitada tuleks eelkõige sellist teavet, millel on selge juhtimis-, tõendamis- või õiguslik väärtus. Vastasel juhul võib dokumenteerimiskohustus kujuneda sisuliselt auditi tarbeks loodavaks lisakoormuseks, mis ei pruugi parandada organisatsiooni tegelikku infoturvet.	
4.	**Mõiste „äriprotsess“ sobivus avalikus sektoris** Eelnõu keskne mõiste on „äriprotsess“. Avalikus sektoris on aga laialdaselt kasutusel teenusepõhine juhtimis- ja eelarvestamisloogika. Tegevuspõhise riigieelarve metoodika kohaselt on asutused kaardistanud teenused, sidunud kulud teenustega ning loonud teenuste loetelud ja teenuskaardid. Kui E-ITS nõuab lisaks eraldi „äriprotsesside“ kaardistamist ja kaitsetarbe määramist, võib see tekitada paralleelse kirjeldus- ja juhtimiskihi, mis on ressursimahukas, dubleeriv ning võib auditis põhjustada tõlgendusriski. Palume kaaluda eelnõus ja lisades mõiste „äriprotsess“ asendamist mõistega „teenus või protsess“ või „teenuse osutamise protsess“. Avaliku sektori asutuse puhul peaks olema selgelt lubatud tugineda olemasolevale teenuste loetelule, teenuskaartidele ja nendega seotud varadele. Sama muudatus tuleks teha läbivalt ka lisades, sealhulgas nendes kohtades, kus räägitakse näiteks pilvteenuse, X-tee turvaserveri või mobiilirakenduse seotusest äriprotsessiga.	**Antud selgitus** Sõna „äriprotsess“ on lisaks infotehnoloogia valdkonnale kasutusel ka planeerimisel eelarvestamisel, kvaliteedijuhtimise, personalitöö jne valdkonnas. Äriprotsessi sisu hõlmab rohkemalt kui selle kõnekeelne tähendus. Äriprotsess ei ole ettevõtlus äriseadustiku tähenduses. Äriprotsess on organisatsiooni (st nii ettevõtjate kui ka riigi või kohaliku omavalitsuse asutuste) põhitegevuste või eesmärkide saavutamiseks vajalike tegevuste kogum, mille käigus kasutatakse aega, raha, töövahendeid ning inimeste tööpanust teenuse, toote või muu väärtust loova tulemuse pakkumiseks. Avalik sektor ***pakub avalikku teenust*** ja igal asutusel on oma erinev eesmärk, mille osutamiseks ta on loodud.
5.	**Kaitsetarbe mõiste ja skaala täpsustamine** Kaitsetarve on E-ITSi rakendamise ja auditeerimise keskne mõiste, kuid eelnõu terminite hulgas seda ei defineerita. Samas sõltuvad kaitsetarbest meetmete valik, prioriteedid, tähtajad, tarneahela nõuded ja auditi valim. Kui kaitsetarbe mõiste ja skaala	**Antud selgitus** Infoturbe halduse süsteemi toimimist korraldab organisatsiooni juhatus, mis määrab ka kaitsetarbe, sh organisatsioonis

	Märkus	Märkusega arvestamine
	ei ole piisavalt ühesed, suureneb rakendajate ja audiitorite tõlgenduserinevus. Palume lisada eelnõu § 2 terminite hulka „kaitsetarve“ ning täpsustada kaitsetarbe määramise skaala või miinimumnõuded skaalale. Võimalik definitsioon oleks järgmine: kaitsetarve on teenuse, protsessi, teabe, andmete või vara kaitsevajadus, mis tuleneb konfidentsiaalsuse, tervikluse või käideldavuse rikkumise võimalikust mõjust organisatsiooni ülesannete täitmisele, teenuse osutamisele, isikute õigustele või avalikule huvile. Kui kaitsetarbe skaala jäetakse organisatsiooni otsustada, peaks riskihalduse metoodikas olema kohustuslikult kirjeldatud vähemalt kaitsetarbe määramise skaala, kriteeriumid, otsustaja ja dokumenteerimise viis. Lisaks palume täpsustada eelnõus äriprotsessile või teenusele määratava kaitsetarbe ning Vabariigi Valitsuse 9. detsembri 2022. a määruses nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ andmekogudele määratava turvaklassi omavahelist seost. Praegune paralleelne käsitlus võib rakendajates tekitada segadust, kuna eri asutused käsitlevad turvaklassi ja kaitsetarbe määramist oma infoturbeprotsessides erinevalt. Palume kaaluda, kas määruse tasandil tuleks turvaklass ja kaitsetarve omavahel võrdsustada või sätestada selgelt, et andmekogudele tuleb määrata eraldi kaitsetarve sõltumata teenuse või protsessi kaitsetarbest. Samuti tuleks hinnata, kas sellisel juhul on põhjendatud senise turvaklassi määramise kohustuse säilitamine või tuleks regulatsiooni vastavalt muuta. Peame oluliseks, et andmekogude kaitsetarve või turvaklass oleks määratud eraldi, et vältida olukorda, kus andmekogule rakendatakse automaatselt sama kaitsetarvet, mis on määratud teenusele või protsessile, mille varade hulka andmekogu kuulub.	rakendatavad tasemed. Keskne skaala ei ole otstarbekas, arvestades KüTS subjektide arvu.

	Märkus	Märkusega arvestamine
6.	**Riskihalduse regulatsiooni selgus ja auditeeritavus** Riskide hindamine on organisatsiooni juhtimise tööriist ning vastutus riskide juhtimise eest jääb organisatsioonile sõltumata kasutatavast metoodikast. Seetõttu peaks riskihalduse regulatsioon jääma piisavalt põhimõtteliseks ega tohiks liigselt ette kirjutada organisatsiooni sisemist töökorraldust. Samas peab riskihaldusmetoodika olema auditeeritav, korratav ja võrreldav. Praegune sõnastus ei pruugi anda piisavat selgust, millised miinimumelemendid peavad metoodikas olema, kes on riskiomanik, kes hindab riski ja kes võib riski aktsepteerida. See võib põhjustada olukorra, kus metoodika on formaalselt olemas, kuid auditis ei ole võimalik järjepidevalt hinnata riskide käsitlemise piisavust. Palume kaaluda § 6 täpsustamist selliselt, et õigusaktis oleks sätestatud üksnes vajalikud miinimumnõuded. Metoodika peaks sisaldama vähemalt riskikriteeriume, mõju ja tõenäosuse hindamise loogikat või muud põhjendatud hindamisviisi, riskitaluvuse piire, kaitsetarbe määramise seost riskihaldusega, riskiomaniku määramist ning riski aktsepteerimise otsustustaset. Täpsemad metoodilised ja korralduslikud juhised võiksid jääda juhendmaterjalidesse.	**Antud selgitus** Juhtkond kehtestab ise organisatsioonisisese metoodika. Kuna KüTS subjekte on ligikaudu 3100, ei ole mõistliku aja jooksul võrdlevat ja samas ajakohast skaalat võimallik koostada.
7.	**Riskide aktsepteerimise võimalus sisehindamise ja auditi kontekstis** Eelnõu § 10 lõike 3 kohaselt tuleb sisehindamise käigus tuvastatud puudused kõrvaldada auditeerimise alguseks. Samas on seletuskirjas nõuet selgitatud paindlikumalt, märkides, et puuduste kõrvaldamise või parandusmeetmete rakendamise hulka võib	**Arvestatud** Paragrahvi 9 (end § 10) lõige 3 sõnastatud järgmiselt: *(3) Lõikes 1 nimetatud hindamise käigus tuvastatud puudused tuleb kõrvaldada ja infoturvameetmete rakendamata jätmisest tulenevad riskid aktsepteerida auditeerimise alguseks.* Vaata ka Kliimaministeeriumi märkust nr 2.

	Märkus	Märkusega arvestamine
	kuuluda ka riskide põhjendatud aktsepteerimine. Sellest tulenevalt võib eelnõu sätte ja seletuskirja vahel tekkida sisuline ebaselgus. Õigusselguse tagamiseks palume täpsustada eelnõu ja auditeerimiseeskirja selliselt, et riskide põhjendatud aktsepteerimise võimalus kajastuks sõnaselgelt ka õigusakti tekstis. Kui organisatsioon on puudusega seotud riski hinnanud, põhjendanud, juhtkonna tasandil aktsepteerinud ning vajaduse korral näinud ette leevendavad või kompenseerivad meetmed, ei peaks sellist olukorda käsitama samamoodi nagu kõrvaldamata ja käsitlemata puudust. Võimalik sõnastus oleks järgmine: „Hindamise käigus tuvastatud puudused tuleb auditeerimise alguseks kõrvaldada või nende kohta peab olema dokumenteeritud riskikäsitluse otsus, sealhulgas põhjendatud jääkriski aktsepteerimine, kompenseeriv meede või kinnitatud tegevuskava.“	
8.	**Rollide paindlikum ja avalikule sektorile sobiv käsitlemine** Palume kaaluda § 3 lõikes 2 nimetatud rollide käsitlemist pigem täidetavate funktsioonidena, mitte eraldiseisvate ametikohtadena. Väiksemates organisatsioonides täidab üks inimene sageli mitut funktsiooni ning rollide formaalne nimetamine ei pruugi anda täiendavat turbeväärtust. Oluline on, et vastutus oleks selgelt määratud ja ülesanded täidetud. Eraldi palume kaaluda mõiste „äriüksuse juht“ asendamist avaliku sektori konteksti paremini sobiva mõistega. Riigiasutustes, hallatavates asutustes ja kohaliku omavalitsuse üksustes kasutatakse pigem mõisteid „asutuse juht“, „struktuuriüksuse juht“, „teenuse omanik“, „protsessi omanik“ või „vastutusala juht“. Kaitsetarbe määramisel peab olema selge, kes sisuliselt vastutab teenuse, protsessi, vara ja andmete kirjelduse õigsuse eest.	**Arvestatud sisuliselt** Rollid asendatud tegevustega, mida on vaja arvestada infoturbe halduse süsteemi toimimisel. Lisatud andmekaitse. Andmekaitse hõlmab organisatsiooni kui ka organisatsioonile usaldatud andmete kaitse kavandamist ja korraldamist. Muu hulgas hõlmab ka isikuandmete kaitset organisatsiooni poolt, kes neid töötleb.

	Märkus	Märkusega arvestamine
	Võimalik sõnastus oleks järgmine: „teenuse omanik või struktuuriüksuse juht – korraldab tema vastutusalas oleva teenuse või protsessi ja vara kaardistuse, kaitsetarbe määramise ning vajalike meetmete rakendamise regulaarse seire.“ Eelnõu § 3 lõikes 2 konkreetsete rollide määratlemine võib tekitada segadust ka seetõttu, et organisatsioonides on sarnaste ülesannetega rollid juba määratletud organisatsiooni struktuurist ja töökorraldusest lähtudes. Selguse huvides võiks rollide asemel reguleerida vajalikke tegevusi ja vastutusi, jättes organisatsioonile võimaluse otsustada, millise ametikoha või struktuuriüksuse kaudu neid ülesandeid täidetakse. Eraldi palume kaaluda mõiste „äriüksuse juht“ asendamist avaliku sektori konteksti paremini sobiva mõistega. Riigiasutustes, hallatavates asutustes ja kohaliku omavalitsuse üksustes kasutatakse pigem mõisteid „asutuse juht“, „struktuuriüksuse juht“, „teenuse omanik“, „protsessi omanik“ või „vastutusala juht“. Kaitsetarbe määramisel peab olema selge, kes sisuliselt vastutab teenuse, protsessi, vara ja andmete kirjelduse õigsuse eest. Võimalik sõnastus oleks järgmine: „teenuse omanik või struktuuriüksuse juht – korraldab tema vastutusalas oleva teenuse või protsessi ja vara kaardistuse, kaitsetarbe määramise ning vajalike meetmete rakendamise regulaarse seire.“	
9.	**Rollide ja vastutuse auditeeritavus** Eelnõus on nimetatud üksnes piiratud arv rolle, kuid puudub selge vastutuse jaotus selle kohta, kes kirjeldab teenuse või protsessi, kes määrab kaitsetarbe, kes kinnitab kaitsetarbe, kes nõustab infoturbe vaatest, kes rakendab tehnilised meetmed, kes aktsepteerib riski ja kes peab olema teavitatud. Auditis peab neid vastutusi olema võimalik tõendada.	**Antud selgitus** Infoturbe toimimist korraldab juhatus, kellel on õigus kehtestada organisatsioonisisene metoodika või volitada edasi metoodika kehtestamine ja võrreldavuse tagamine.

	Märkus	Märkusega arvestamine
	Palume lisada seletuskirja või rakendusjuhisesse minimaalne vastutusmudel, näiteks RACI-põhine mudel. E-ITSi puhul võiks miinimumnõue olla, et organisatsioonil on kaitsetarbe määramise, riskide aktsepteerimise ja infoturvameetmete rakendamise plaani täitmise kohta rollide ja vastutuste jaotus taasesitatavas vormis olemas. Samuti palume selgitada, kas senises E-ITS-is kasutatud rollid jäävad rakendamisel kehtima juhendmaterjali või rakenduspraktika tasandil või on need teadlikult infoturbe halduse süsteemi rollimudelist välja jäetud. Kui need rollid jäetakse määrusest välja, tuleks seletuskirjas või rakendusjuhises esitada vastavustabel seniste ja uute rollide vahel. Eriti vajab täpsustamist IT talituse, IT-juhi või IT-teenuse vastutaja roll, sest praktikas on see tehniliste meetmete rakendamise, IT-varade halduse, muudatuste, seire, logihalduse, varunduse ja tehniliste intsidentide lahendamise võtmeroll.	
10.	**Tarneahela nõuete proportsionaalsus** Toetame tarneahela riskide käsitlemise tugevdamist. Samas palume täpsustada, et väliselt osapoolelt nõutavad tõendid ja kinnitused peavad olema riskipõhised ja proportsionaalsed. Vastasel juhul võib tekkida olukord, kus väiksemate või standardsete teenuste puhul kujuneb tarnijate hindamise halduskoormus ebamõistlikult suureks võrreldes tegeliku riskiga. Palume täiendada eelnõu või seletuskirja selliselt, et tarneahela hindamisel lähtutakse teenuse olulisusest, töödeldavate andmete olemusest, sõltuvuse ulatusest ning võimalikust mõjust organisatsiooni teenustele ja protsessidele.	**Arvestatud** Seletuskirja täiendatud.
11.	**Sisehindaja erapooletus ja hindamise mõiste**	**Antud selgitus**

	Märkus	Märkusega arvestamine
	Seletuskirjas on rõhutatud, et sisehindaja peaks olema erapooletu ega tohiks olla hinnatavate turvameetmete vahetu rakendaja. Eelnõu § 10 tekstis seda põhimõtet sõnaselgelt ei sisaldu. Sisehindamise usaldusväärsuse tagamiseks palume lisada eelnõusse nõue, et hindamine peab olema korraldatud objektiivselt ning võimaluse korral viisil, mis väldib huvide konflikti. Lisaks märgime, et mõiste „organisatsioonisisene hindamine“ võib olla ebatäpne, kuna eelnõu järgi võib hindamist teha ka organisatsioonivälineisik. Palume kaaluda mõiste „organisatsiooni korraldatav hindamine“ kasutamist või täpsustada, et hindamise korraldab organisatsioon, kuid selle võib läbi viia sõltumatu sisemine või väline hindaja.	Seletuskirja täiendatud ettepanekust lähtuvalt. Säte, et organisatsioonisisest hindamist võib teha ka organisatsiooni väline isik on lisatud tagasisidest lähtuvalt. Nimelt ei pruugi väiksematel organisatsioonidel olla siseaudiitori või muud ametikohta, mis täidaks hindaja rolli. Seetõttu lisati säte, et seda tööd võib teha ka personali mitte kuuluv isik. Välise isiku kaasamine ei muuda tegevust olemuslikult organisatsiooni väliseks hindamiseks, sest isik lähtub töös etteantud nõuetest. Nii näiteks kui organisatsioon peab tagama töötajale asjakohased töötingimused, siis remonditeenuse sisse ostmine ei muuda seda kellegi teise kohustuseks.
12.	**Audiitorettevõtte rotatsiooninõue** Auditeerimiseeskirjas kavandatud piirang, mille kohaselt ei või sama audiitorettevõte teha sama asutuse auditit üle kahe korra järjest, võib Eesti piiratud IT-auditi turul takistada kvalifitseeritud pakkujate leidmist ja hangete läbiviimist. Eriti võib see mõjutada suuremaid või keerukamaid organisatsioone, kelle auditeerimine eeldab spetsiifilist valdkondlikku teadmist ja varasemat kogemust. Palume kaaluda rotatsiooninõude kehtestamist audiitorettevõtte asemel juhtivaudiitorile. Alternatiivina võiks kaaluda audiitorettevõtte rotatsiooniperioodi pikendamist või erandi sätestamist olukordadeks, kus turul puudub piisav arv kvalifitseeritud pakkujaid.	**Võetud teadmiseks**
13.	**Kõrge tasemega riskide kõrvaldamise tähtaeg** Auditeerimiseeskirja kohaselt tuleb kõrge tasemega riskid kõrvaldada kuue kuu jooksul alates auditi lõpparuande saamisest. Praktikas võib see tähtaeg osutuda ebapiisavaks juhtudel, kus	**Arvestatud sisuliselt** Paragrahvi 9 (end § 10) lõike 3 sõnastust muudetud järgmiselt:

	Märkus	Märkusega arvestamine
	puuduse kõrvaldamine eeldab näiteks uue tarkvaralahenduse hankimist, infosüsteemi ümberarendamist, arhitektuurimuudatusi või muid ajamahukaid tegevusi. Palume muuta nõuet paindlikumaks ning lisada võimalus, et objektiivsete takistuste korral võib kuuekuulise kõrvaldamiskohustuse asemel koostada juhtkonna kinnitatud riskide leevendamise tegevuskava. Tegevuskava peaks sisaldama realistlikke tähtaegu, ajutisi kompenseerivaid meetmeid ning vastutajaid. Selline lahendus võimaldaks kõrge tasemega riske sisuliselt juhtida ka olukorras, kus nende täielik kõrvaldamine ei ole kuue kuu jooksul objektiivselt võimalik.	*(3) Lõikes 1 nimetatud hindamise käigus tuvastatud puudused tuleb kõrvaldada ja infoturvameetmete rakendamata jätmisest tulenevad riskid aktsepteerida auditeerimise alguseks.*
14.	**Terminoloogia ja sõnastuse ühtlustamine** Palume eelnõus ja lisades terminoloogiat ühtlustada. Eelnõus kasutatakse läbivalt nii „infoturbe“ kui ka „infoturva-“ vorme, näiteks „infoturbe halduse süsteem“, „infoturbekataloog“, „infoturvameetmed“, „infoturvasündmus“, „infoturvapoliitika“, „infoturvaoht“ ja „infoturvaintsident“. Rakendaja jaoks ei pruugi olla selge, kas vormidel on sisuline tähenduserinevus või on tegemist üksnes keelelise liitsõnamoodustusega. Palume terminikasutus ühtlustada või lisada seletuskirja terminoloogiline märkus, et sisulist tähenduserinevust ei ole. Samuti palume kaaluda mõiste „organisatsiooni juhatus“ asendamist mõistega „organisatsiooni juhtorgan või asutuse juht“, kuna avaliku sektori asutustes ei pruugi „juhatus“ olla korrektne ega üheselt mõistetav mõiste. Mõiste „hankejuht“ võib avalikus sektoris seostuda eelkõige riigihanke või ostumenetlusega. Kuna seletuskirja järgi ei mõisteta selle all üksnes ostujuhti või riigihanke eest vastutajat, palume kaaluda täpsemat rollinimetust, näiteks „vara või teenuse	Eelnõule on koostöös valdkonna spetsialistidega tehtud keeletoimetus. Eelnõu läbib keeletoimetuse ka enne selle allkirjastamist määrusena.

	Märkus	Märkusega arvestamine
	kasutuselevõtu eest vastutav isik“ või „soetuse ja kasutuselevõtu turvanõuete eest vastutav roll“. Auditeerimiseeskirjas kasutatud mõiste „teenuseandja“ võib minna segi KüTS-i tähenduses teenuseosutaja või organisatsiooni mõistega. Kui mõeldakse välist IT-teenuse osutajat, pilvteenuse tarnijat või tarneahela osalist, palume kasutada läbivalt mõistet „väline teenuseosutaja“ või „tarneahela osaline“ ning eristada see selgelt KüTS-i tähenduses teenuseosutajast. Lisaks palume ühtlustada eelnõu ja seletuskiri autentsuse käsitlemise osas. Eelnõu § 6 nimetab konfidentsiaalsust, terviklust ja käideldavust, kuid seletuskirjas on samas kontekstis lisatud ka autentsus. Kui autentsus peab olema kohustuslik hindamiskriteerium, tuleks see lisada normiteksti. Kui kohustuslikuks jäävad konfidentsiaalsus, terviklus ja käideldavus, võiks autentsust käsitleda seletuskirjas näitliku lisakriteeriumina. Kokkuvõttes toetame Eesti infoturbestandardi uuendamise eesmärki, kuid peame oluliseks, et eelnõu rakendamine ei tooks kaasa ebaproportsionaalset üleminekukoormust ega liigset formaalset dokumenteerimist. Palume eelnõu ja sellega seotud auditeerimise regulatsiooni täiendada viisil, mis tagab õigusselguse, riskipõhisuse, proportsionaalsuse ning rakendajatele ja audiitoritele üheselt arusaadavad üleminekureeglid.	
	Andmekaitse Inspektsioon 02.06.2026 kiri nr 2.3-4/26/2161-2	
	Eelnõu § 3 lg-s 2 nimetatakse asutusesisesed rollid, mis on vajalikud infoturbe halduse süsteemi toimimiseks. Seletuskirjas selgitatakse, et roll ei tähenda, et seda peab täitma sama ametinimetusega töötja, vaid tegemist on tegevustega, millega	**Arvestatud sisuliselt** Rollid asendatud tegevustega, mida on vaja arvestada infoturbe halduse süsteemi toimimisel. Lisatud andmekaitse. Andmekaitse

	Märkus	Märkusega arvestamine
	organisatsioon peab arvestama. Inspektsioon teeb ettepaneku lisada rollide loetellu ka andmekaitsespetsialisti rolli, sest EITS meetmete komplekt (GRC.4 Isikuandmete kaitse) puudutab ka isikuandmete kaitset.	hõlmab organisatsiooni kui ka organisatsioonile usaldatud andmete kaitse kavandamist ja korraldamist. Muu hulgas hõlmab see ka isikuandmete kaitset organisatsiooni poolt, kes neid töötleb.
Registrite ja Infosüsteemide Keskus 25.06.2026 e-kiri		
1.	Eelnõukohase määruse paragrahvis 3 lõikes 2 nimetatakse rollid, mis on vajalikud infohalduse süsteemi toimimiseks. RIKi hinnangul jääb määruses arusaamatuks toodud rollide eesmärgipärasus. Eelnõu seletuskirjas on toodud, et roll ei tähenda, et seda peab täitma sama ametinimetusega töötaja, vaid tegemist on tegevustega, millega organisatsioon peab arvestama. Lähtudes seletuskirjas toodust võiks ka määruses olla tegemist pigem tegevustega, mille organisatsioon peab tagama, mitte rollipõhise jaotusega. Eeltoodust tulenevalt tuleks muuta ka eelnõukohase määruse paragrahvi 4 lõiget 2 punkti 1, mille kohaselt juhatus infoturbe halduse süsteemi toimimiseks määrab organisatsiooni sees rollid ja vastutajad, määramata rollide eest vastutab juhatus ise. Juhul kui paragrahvis 3 lõikes 2 nimetatakse tegevused, siis edastame paragrahvi 4 lõike 2 punkti 1 muudatusettepanekuna sõnastuse: „määrab organisatsiooni sees tegevustele vastutajad, määramata vastutajatega tegevuste eest vastutab juhatus;“. RIKi hinnangul välistaks tegevuse nimetamine olukorra, kus toodud rollides isikuid on raske määratleda või kasutakse rollinimetusi, millel on klassikalises mõistes hoopis teistsugused ülesanded.	**Arvestatud sisuliselt** Rollid asendatud tegevustega, mida on vaja arvestada infoturbe halduse süsteemi toimimisel.
2.	Eelnõukohase määruse paragrahvis 4 sätestatakse organisatsiooni juhatuse roll infoturbe halduse süsteemi korraldamises. Valitusasutused peavad infoturbe tagamisel	**Antud selgitus**

	Märkus	Märkusega arvestamine
	lähtuma Vabariigi Valitsuse 15.03.2012 määrusest nr 66 infoturbe juhtimise süsteem, kas Vabariigi Valitsuse määrus on plaanitud tulevikus kehtetuks muuta või ühtlustada määruste sõnastused.	Eelnõu koostamisel on arvestatud kooskõlaga viidatud Vabariigi Valitsuse määrusega. Eelnõukohase määruse infoturbe nõuded on üldisemad. Vabariigi Valitsuse määrus täpsustab infoturbe juhtimise nõudeid valitsusasutuste osas. Näiteks eelnõukohase määruses ei nähta ette infoturbe juhi ametikoha loomist, siis Vabariigi Valitsuse määrus sätestab, et valitsusasutus peab määrama infoturbe juhi. Nii samuti määrab nt Vabariigi Valitsus ministeeriumi ja hallatavate riigiasutuste infoturbe rakendamise eest vastutavaks ministeeriumi kantsleri, mis tähendab et ministeeriumite osas ei saa juhtkond teisiti otsustada jne.
3.	Eelnõukohase määruse paragrahvis 7 kirjeldatakse infoturbekataloogi olemust. Paragrahvis 7 lõikes 1 sätestatakse, et määruse lisas 1 sätestatud infoturbekataloog on organisatsiooni kahjustada võivate ohtude kaitseks võetavate meetmete loend. Määruse lisa 1 on moodulite loend, sellele vihjavad ka lisa 1 tabelite pealkirjad „Protsessimoodulid“ ja „Süsteemimoodulid“. Mooduli põhised meetmed asuvad E-ITS portaalis. Eeltoodust tulenevalt tuleks RIKi hinnangul asendada paragrahvis 7 lõikes 1 ja 2 sõna „meetmed“ sõnaga „moodulid“.	**Arvestatud sisuliselt**
4.	Eelnõukohase määruse paragrahvis 11 kirjeldatakse auditeerimise eesmärki, mis seni oli nimetatud kehtiva E-ITSi määruse lisas. Määrusest on välja jäetud auditeerimise ajatsükkel. Peatükis kirjeldatud tegevuste ajajoon on esitatud küll seletuskirjas, kuid selleks, et tegemist oleks kohustusega tegevusi teatud ajaperioodi jooksul teha peaks see olema sätestatud määruse tasandil. RIK esitab eeltoodust tulenevalt ettepaneku määrust täiendada tegevuste ajaperioodiga.	**Antud selgitus** E-ITSi auditeerimise ajatsükkel on kindlaks määratud Vabariigi Valitsuse 9.12.2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 4 lõigetes 1 (üldreeglina kolm aastat) ja 1^1 (elutähtsa teenuse osutajate puhul peab esmakordselt tegema hädaolukorra seaduse § 38 lõike 1^3 punktis 3 sätestatud korras määratud tähtaja jooksul).
5.	Eelnõukohase määruse lisas 2 „Auditeerimiseeskiri“ termini „teenuseandja“ selgituses kasutatakse mõistet „digielement“.	**Antud selgitus**

	Märkus	Märkusega arvestamine
	Mõiste „digielement“ on Eesti õigusruumis täiesti uus mõiste (lisaks ei ole mõistet ka AKITis), mistõttu jääb selgusetuks, kes on teenuseandja.	Lisas 2 on teenuseandja termini juures võetud eeskujuks Euroopa Parlamendi ja nõukogu 23.10.2024 määruse 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) artikkel 3 punkti 13 mõiste „tootja“. Küll on eelnõus asendatud parema arusaadavuse eesmärgil ja kehtivat Eesti infoturbestandardit arvestades küberkerkuse määruse sõna „tootja“ sõnaga „teenuseandja“. Seega tuleb digielemendi puhul lähtuda otsekohalduvast Euroopa Liidu määrusest.
6.	Eelnõukohase määruse lisas 2 „Auditeerimiseeskiri“ kasutatakse sõna „äriprotsess“ mitmuses (nt punktid 3.1., 5.5.1., 6.6.3., 6.6.4.). Määruse lisas 2 tuleks kasutada ainsust, mis hõlmaks olukordi, kus äriprotsesse on üks või mitu. Käesolevas sõnastuses tekib küsitavus, et kui orginatsioonil on ainult üks äriprotsess, siis kas sellisel juhul ei ole vajalik auditit läbi viia.	**Arvestatud**
7.	Eelnõukohase määruse lisas 2 „Auditeerimiseeskiri“ punktis 2.4. on sätestatud, et auditit tööde ei tohi kaugtöötundide osakaal ületada 30% kavandatud tundide koguarvust. Sedavõrd konkreetse protsendi paika panemise eesmärgipärasus jääb arusaamatuks ja soovitame sätestada pigem kohustus kohapealseks kontrolliks konkreetsete meetmete/moodulite osas – näiteks on arusaadav, miks füüsilise turbe kontrolli ei ole võimalik kaugtöö vormis teostada. Kaugtöötundide osakaalu määramine 30% ei ole eesmärgipärane olukordades, kus füüsilise turbe kontroll ei hõlma 30%. Punktis 2.4. on sätestatud, et põhjendatud juhtudel ja eelneval kokkuleppel võib auditiprotseduure teha kaugtöö vormis, sellisel juhul kajastatakse see fakt auditiaruandes, mistõttu peaks juba see lause tagama, et näiteks füüsilist turbe	**Arvestatud sisuliselt** Lisa 2 punkt 2.4 sõnastatud järgmiselt: *2.4. Auditi tegemine plaanitakse koostöös auditeeritava kontaktisikuga, kes tagab vajalike andmete ja isikute kättesaadavuse auditi ajal. Põhjendatud juhtudel ja eelneval kokkuleppel võib auditiprotseduure teha kaugtöö vormis, sellisel juhul kajastatakse see fakt auditi lõpparuandes ja auditi järeldusotsuses koos kaugtöö vormis tehtud auditi käsitlusala kirjeldusega.*

	Märkus	Märkusega arvestamine
	kontrolli ei teostata kaugtöö vormis ning konkreetse protsendi sätestamise vajadus puudub. Täiendavalt on punktis 5.8. toodud, et auditi tõendusmaterjali võib audiitorile kas väljastada, kohapeal näidata või selgitada intervjuu käigus, mis tähendab, et auditeeritav võib ise valida kolme variandi vahel. Kelle kohustus on seejuures järgida, et kaugtöötundide osakaal ei ületa 30%, kuna kui auditeeritav valib tõendusmaterjali väljastamise (enamus/suur hulk tõendusmaterjale on digitaalses vormis) või selgituste andmise intervjuu käigus, siis need viisid on teostavad samaväärselt kaugtöö vormis.	
8.	Eelnõukohase määruse lisa 2 punkti 3.5. kohaselt võib auditi tellida või hankida mitmele auditeeritavale korraga. Kui auditeeritavad tuginevad samale infoturbe halduse süsteemile (nt on neil ühine infoturbe organisatsioon, infoturvapoliitika ja infoturbe dokumentatsioon), võib ühe auditi käsitlusala laiendada mitmele auditeeritavale. Seejuures käsitletakse auditiaruandes ja järeldusotsustes vajaduse korral auditeeritavate erisusi. Eelnõukohase määruse paragrahvi 11 kohta öeldakse seletuskirjas, et auditi võib teha teise organisatsiooniga ning ühisauditi või teise organisatsiooni nimel auditi tellimine on ennekõike asjakohane juhul, kui eri organisatsioonide info- ja kommunikatsioonitehnoloogia taristu haldamine ja majutamine on üle antud kesksele organisatsioonile. Eelnõukohase määruse lisa 2 punkt 2 ja paragrahvi 11 kohta seletuskirjas öeldu ei katu, mistõttu tuleks sõnastused ühtlustada. Käesolevas sõnastuses jääb selgusetuks, millisel juhul on ühisauditi või teise organisatsiooni nimel auditi tellimine lubatud.	**Antud selgitus** Seletuskirjas on toodud üks näide, millal võib mõelda ühisauditile. Seletuskirjas on välja toodud ka, et võib esineda ka muid olukordi, kus organisatsioonid leiavad, et ühisauditi tegemine on mõistlik. Auditis tuleb näidata organisatsiooni põhiseid erisusi, kui need esinevad (nt kaitseala osas või siis osas kus on rakendatud erinevaid meetmeid). Lõpparuaruandest peab selguma millise organisatsiooni kohta milline otsus tehti.
9.	Eelnõukohase määruse lisas 2 „Auditeerimiseeskiri“ punktis 5.5.5. sätestatakse, et kontrollitavate meetmete valimisel lähtub audiitor varasemate infoturbe auditite leidudest ning läbivaatuste	**Antud selgitus**

	Märkus	Märkusega arvestamine
	aruannetes esitatud tähelepanekutest ja soovitustest. On selgusetu, millistest infoturbe auditite leidudest ning läbivaatuste aruannetes peab audiitor lähtuma. Kui tegemist on varasemate E-ITS auditite tega, siis audiitor saab lähtuda üksnes organisatsiooni lõppotsusest ning kui organisatsioon kasutab teisi teenusepakkujaid, siis sellisel juhul on audiitorile üksnes esitada teiste organisatsioonide järeldusotsuseid. RIKi hinnangul tuleks selgelt sätestada, millistest dokumentidest peab audiitor lähtuma, arvestades seejuures, millised dokumendid on konfidentsiaalsed või sisaldavad asutusesiseseks kasutamiseks mõeldud teavet.	Audiitor peab vajalikud allikmaterjalid auditeeritavalt küsima auditi käigus. Seejuures tuleb ka audiitoril endal teha riskihinnang tulenevalt keskkonnast. Teenuse andja turbe puhul lähtub audiitor lisa 2 punktis 5.10. sätestatust.
10.	Eelnõukohase määruse lisas 2 „Auditeerimiseeskiri“ punktis 5.10 sätestatakse, et auditeeritava teenuseandjate infoturbe hindamisel tugineb audiitor oma hinnangut kujundades teenuseandja (nt pilvteenuse tarnija) esitatud auditi käsitlusala hõlmavatele ja turvameetmete rakendatust kinnitavatele sertifikaatidele ning vastavusauditite aruannetele. Kas vastavusauditite aruannete all on mõeldud E-ITSi, sellisel juhul saab audiitor üksnes tugineda teenuseandja järeldusotsusele, kuna lõpparuanded on konfidentsiaalsed või sisaldavad asutusesiseseks kasutamiseks mõeldud teavet. Kui on mõeldud üldisemaid aruandeid, siis selguse loomiseks võiks lisada E-ITS auditite osa, milles on hindamisel üksnes võimalik tugineda järeldusotsustel.	**Arvestatud** Loetellu lisatud ka auditi järeldusotsus.
Riigi Info- ja Kommunikatsioonitehnoloogia Keskus 26.06.2026 kiri nr 8-1/26-184-2		
1.	Terminid Selguse huvides palume täpsustada määruse eelnõus kasutatavate terminite „kaitseala“ ja „käsitlusala“ omavahelist	**Antud selgitus**

	Märkus	Märkusega arvestamine
	seost ning vajadusel lisada vastavad definitsioonid mõistete loetellu (§ 2). Praegu kasutatakse mõistet „kaitseala“ määruse eelnõu sisutekstis mitmes sättes (nt § 6, § 8 ja § 10), kuid selle sisu ei ole eelnõus eraldi avatud. Samal ajal kasutatakse auditeerimiseeskirjas mõistet „auditi käsitlusala“, mis on auditeerimiseeskirjas (lisa 2) terminina avatud. Õigusselguse tagamiseks palume kaaluda määruse ja auditeerimiseeskirja mõistete kooskõlla viimist. See aitaks vähendada tõlgendusruumi ning toetaks ühtset praktikat moodulite valikul, riskihalduses ja auditi läbiviimisel.	Kaitseala on organisatsiooni enda määratletud infoturbe haldusele allutatud osa. Auditi käsitlusala on auditi ulatus, mis ei pruugi kaitsealaga kattuda. Kaitseala on organisatsiooni infoturbe halduse rakendamise käsitlusala. Organisatsioon liigitab kaitsealasse kaitstavad varad ehk sihtobjektid, mida turbeprotsess hakkab edaspidi kaitsma.
2.	Infoturbekataloog Praeguses sõnastuses viitab eelnõu § 7, et lisa 1 sisaldab meetmete loendit, kuid sisuliselt koosneb lisa 1 moodulite loetelust. Samuti ei ole lisas 1 ega määruse eelnõus otsest viidet sellele, kust leiab moodulite rakendamiseks mõeldud detailsemad meetmed. Selguse huvides palume täpsustada määruse lisa 1 ja E-ITS infoturbekataloogi veebilahenduses esitatud meetmete omavahelist seost. Õigusselguse ja rakendamise ühtsuse huvides palume kaaluda määruse ja seletuskirja sõnastuse kooskõlla viimist ning lisada selgitus, kas infoturbe meetmete rakendusplaan (IMR) peab lähtuma moodulitest üldtasandil või sisaldama konkreetseid meetmeid detailtasandil. Samuti aitaks täpsustus selgitada, mille alusel toimub auditi käigus vastavuse hindamine – kas moodulite eesmärkide täitmise või E-ITS veebikataloogis kirjeldatud meetmete rakendamise kaudu.	**Jäetud arvestamata**
3.	Kaitsetarbe määramise metoodika Selguse huvides palume täpsustada kaitsetarbe määramise põhimõtteid või viidata sobivale metoodilisele raamistikule.	**Antud selgitus**

	Märkus	Märkusega arvestamine
	Eelnõu näeb ette kaitsetarbe määramise kohustuse, kuid jätab organisatsioonile ulatusliku kaalutlusruumi selle osas, kuidas ja millise metoodika alusel see toimub. Ühtse rakenduspraktika toetamiseks võiks kaaluda vähemalt miinimumnõuete või lähteprintsiipide kirjeldamist, et tagada võrreldav ja põhjendatud lähenemine erinevates organisatsioonides.	Eelnõukohase määruse jõustumisel jätkab Riigi Infosüsteemi Amet oma veebilehel ajakohaste juhiste ja rakenduste esitamist, sh ka soovituslikke juhiseid kuidas määrata kaitsetarvet. Otsustusõigus jääb siiski organisatsioonile, arvestades organisatsiooni enda eripärasid ja tegevusest tulenevaid vajadusi. Organisatsioon peab oma vara hindamisel olema teadlik, mida ja mis määral soovib kaitsta (käideldavus, autentsus, terviklus ja konfidentsiaalsus). Eelnõu koostamisel ei peetud vajalikuks kindla skaalade kirjeldamist, kuivõrd senise praktika kohaselt paljusel juhtudel ei lähtutud kaitsevajadusest vaid olemasolevatest ressurssidest turvameetmete rakendamisel.
4.	Kohustuslikud rollid (§ 3 lg 2) Selguse huvides palume täpsustada eelnõu § 3 lõike 2 eesmärki ning viia määruse ja seletuskirja sõnastus omavahel paremini kooskõlla. Määruse sõnastusest võib järeldada, et organisatsioonil tuleb määrata konkreetsed rollid, samas kui seletuskirjas selgitatakse, et rollide all peetakse silmas eelkõige tegevusi või funktsioone, mida organisatsioon peab katma, sõltumata ametinimetusest. Õigusselguse huvides võiks täpsustada, kas normi eesmärk on formaalne rollide määratlemine või sisuline ülesannete täitmise tagamine. See aitaks vältida erinevaid tõlgendusi ning toetaks normi ühetaolist rakendamist.	**Arvestatud sisuliselt** Eelnõu § 2 lõike 2 (end § 3 lg 2) sõnastust muudetud. Viide rollidele asendatud infoturbe halduse toimimiseks vajalike tegevustega.
Eesti Linnade ja Valdade Liit 29.06.2026 kiri nr 2-3/138-2		
1.	Eelnõu seletuskirjas on kirjeldamata üleminekuprotsessid kehtivalt standardi versioonilt uuele. Kas uute nõuete rakendamiseks antakse üleminekuaeg või peab neile üle minema koheselt uue	**Arvestatud** Seletuskirja täiendatud.

	Märkus	Märkusega arvestamine
	standardi kehtima hakkamisel (eeldatavasti 1. augustil 2026), näiteks auditi läbiviimist puudutavate muudatuste osas? Palume seletuskirja vastavalt täiendada, sest pole piisavalt selge, kas organisatsioonid peavad samaaegselt täitma nii kehtivat kui uut standardit.	
2.	Ühtlasi juhime tähelepanu, et riskipõhine lähenemine eeldab organisatsioonidelt suuremat kompetentsi infoturberiskide hindamisel ning võib väiksematele omavalitsustele tuua täiendava töö- ja ressursikoormuse, eelkõige riskihindamise, dokumenteerimise ja infoturbe juhtimise korraldamise osas. Seetõttu peame oluliseks, et riik tagaks kohalikele omavalitsustele piisava metoodilise toe, juhendmaterjalid ja koolitused, et tagada eelnõu nõuete ühtlane ja kvaliteetne rakendamine.	**Võetud teadmiseks**
	Eesti Haiglate Liit 22.06.2026 kiri nr 232-2B	
1.	Eelnõu § 3 lg 2 sätestab kohustuse määrata infoturbe halduse süsteemis rollid (hankejuht, infoturbejuht, äriüksuse juht ja kasutaja). Selline rollipõhine lähenemine vajab meie hinnangul ümbervaatamist. Kuigi see lähenemine on sarnane ISO/IEC 27001 standardis kasutatavale praktikale, ei ole Eesti õigusloomes tavapärane sätestada organisatsioonisiseseid rolle normatiivse kohustusena. Määruse tasandil tuleks sõnastada asutuse kohustused ja vastutused infoturbe halduse süsteemi toimimise tagamiseks. Sellise detailsusastmega rollide lahti kirjeldamine tekitab praktikas märkimisväärseid probleeme, kuna need rollid on asutustes juba laiemalt või kitsamalt defineeritud ja juhul, kui ei ole juba defineeritud, siis määruse praegune sõnastus seab rollidele liiga suured piirangud. Teeme ettepaneku eemaldada paragrahv 3	**Arvestatud sisuliselt** Eelnõu § 2 lõike 2 (end § 3 lg 2) sõnastust muudetud. Viide rollidele asendatud infoturbe halduse toimimiseks vajalike tegevustega.

	Märkus	Märkusega arvestamine
	lõige 2 sellises sõnastuses, sest asutusesisesed rollid võivad olla praktikas väga erinevad. Teeme ettepaneku § 3 lõige 2 ümber sõnastada selliselt, et selles sätestataks asutuse kohustused ja vastutused, mitte konkreetsed organisatsioonisisesed rollid. Rollimõistet võiks kasutada üksnes kirjeldavas tähenduses.	
2.	Eelnõu § 3 lg 2 sätestab rollina hankejuhi. Praktikas on hankejuht sageli eraldiseisev ametikoht ning organisatsioonides kasutatakse paralleelselt ka muid nimetusi (nt hankespetsialist, hankejurist), mistõttu võib selline regulatsioon tekitada ebaselgust. Ettepanek: täpsustada sätte sõnastust selliselt, et välistada vastuolud organisatsioonides kehtivate ametikohtade süsteemiga ning sätestada kohustus rakendada infoturbe meetmeid hangete läbiviimisel asutuse hankekorra alusel, mitte rollipõhiselt.	**Arvestatud sisuliselt** Eelnõu § 2 lõike 2 (end § 3 lg 2) sõnastust muudetud. Viide rollidele asendatud infoturbe halduse toimimiseks vajalike tegevustega.
3.	Eelnõu § 3 lg 2 sätestab rollina kasutaja. Ettevõtluspraktikas ei käsitleta kasutajat iseseisva juhtimisfunktsioonina ning vastava rolli kehtestamine ei ole otstarbekas, kuna see hõlmab sisuliselt kõiki organisatsiooni töötajaid. **Ettepanek:** eemaldada § 3 lg 2-st kasutaja roll.	**Arvestatud sisuliselt** Eelnõu § 2 lõike 2 (end § 3 lg 2) sõnastust muudetud. Viide rollidele asendatud infoturbe halduse toimimiseks vajalike tegevustega.
4.	Eelnõu § 3 lg 2 sätestab rollidena infoturbejuhi ja äriüksuse juhi. Infoturbejuhi roll on eelnõu kohaselt kirjeldatud pigem nõustavana, samas kui äriüksuse juhile on omistatud ülesanded (nt kaitsemeetmete määramine ja rakendamise seire), mis kuuluvad oma olemuselt infoturbejuhi ning juhtorgani pädevusse tulenevalt küberturvalisuse seaduse § 6^1 lg-st 1. **Ettepanek:** täpsustada sätte sõnastust selliselt, et infoturbejuhi ja äriüksuse juhi ülesanded oleksid selgelt eristatavad ning kooskõlas küberturvalisuse seaduse § 6^1 lg-ga 1.	**Arvestatud sisuliselt** Äriüksuse juhi ja infoturbe juhi roll eelnõu tekstist välja jäetud

	Märkus	Märkusega arvestamine
5	Eelnõu § 4 lg 2 p 4 kohaselt on kogu juhatusele pandud vastutus aktsepteerida riske meetmete rakendamata jätmise korral. Nimetatud säte on vastuolus küberturvalisuse seaduse § 6[1] lg-ga 1, mille kohaselt on vastav kohustus määratud ühele juhatuse liikmele. **Ettepanek:** viia § 4 lg 2 p 4 kooskõlla küberturvalisuse seaduse § 6[1] lg-ga 1.	**Antud selgitus** Eelnõu ei ole vastuolus küberturvalisuse seaduse § 6[1] lg 1. Küberturvalisuse seaduse § 6[1] lg 1 eeldab, et vähemalt üks juhatuse määratakse isikuks, kes kiidab heaks turvameetmed, jälgib nende rakendamist ja vastutab selle eest. Samas viidatud seaduse paragrahvi lõige 3 sätestab järgmist: *(3) Kui teenuseosutaja ei määra käesoleva paragrahvi lõikes 1 nimetatud juhatuse liiget, kohaldatakse käesolevas paragrahvis sätestatud kohustusi kõigile juhatuse liikmetele.* Seega on seaduses sätestatud, et juhatus korraldab võrgu-ja infosüsteemide turvameetmete rakendamist, sh infoturbe halduse süsteemi toimimist. Ka ühe oma liikmete määramine peamiseks vastutajaks on osa korraldamisest.
6.	Eelnõu § 6 lg 1 („Riskihaldusmetoodika kasutuselevõtmise eeldus on organisatsiooni varade arvelevõtmine ja nende kaitseala kindlaksmääramine“) on esitatud kirjeldavas vormis ega vasta normitehnilistele nõuetele, kuna ei kehtesta otsest kohustust. **Ettepanek:** sõnastada § 6 lg 1 järgmiselt: „Organisatsioon peab võtma arvele varad ning määrama kindlaks kaitseala.“	**Arvestatud**
7.	Auditeerimiseeskirja peatüki 2 „Auditi üldine korraldus“ punkt 2.4 sisaldab sõnastust: „Kaugtöötunnid ei tohi ületada 30% audititööks kavandatud tundide koguarvust. Erandiks on auditeeritav, kes kasutab ainult virtuaalseid töökohti.“ Nimetatud piirang ei ole praktikas põhjendatud, kuivõrd see piirab auditeerimistoimingute, sealhulgas intervjuude läbiviimist kaugtöövahendite abil. Arvestades asjaolu, et auditeeritavad asutused (sh haiglad) paiknevad geograafiliselt üle Eesti ning auditeerivad ettevõtted	**Arvestatud sisuliselt** Lisa 2 punkt 2.4. sõnastatud järgmiselt: *2.4. Auditi tegemine plaanitakse koostöös auditeeritava kontaktisikuga, kes tagab vajalike andmete ja isikute kättesaadavuse auditi ajal. Põhjendatud juhtudel ja eelneval kokkuleppel võib auditiprotseduure teha kaugtöö vormis, sellisel juhul kajastatakse see fakt auditi lõpparuandes ja auditi*

	Märkus	Märkusega arvestamine
	asuvad valdavalt Tallinnas, toob nimetatud piirang kaasa põhjendamatult suure ajakulu ning märkimisväärse täiendava rahalise koormuse seoses transpordi- ja majutuskuludega. Sellest tulenevalt ei ole kehtestatud piirang proportsionaalne ega eesmärgipärane. **Ettepanek:** muuta punkti 2.4 sõnastust selliselt, et kaugtöö piirang ei hõlmaks auditi intervjuude läbiviimist virtuaalkoosolekute vormis	*järeldusotsuses koos kaugtöö vormis tehtud auditi käsitlusala kirjeldusega.*
	Eesti Infosüsteemide Audiitorite Ühing 26.06.2026 kiri 8-1/4143-1	
1.	**Turvameetmete sisu nihkumine siduvast õigusaktist mittesiduvasse juhendisse** Eelnõu lisa 1 (infoturbekataloog) on esitatud moodulite kaupa, kusjuures iga mooduli all on üksnes ühelauseline eesmärgikirjeldus (näiteks „NET.1.3. Raadiokohtvõrk: Esitada raadiokohtvõrgu rajamise ja turvalise käitamise juhised“). Sisulised turvameetmed kataloogist puuduvad. Eelnõu § 12 kohaselt võib Riigi Infosüsteemi Amet anda rakendamist toetavaid soovituslikke juhiseid. Senised E-ITS ja ISKE olid etalonturbe metoodikad, mille puhul oli suur osa meetmete väljatöötamise tööst kesksel te ette tehtud. Kui meetmete sisu nihkub siduvast määrusest RIA mittesiduvasse juhendmaterjali, tähendab see ühingu hinnangul kahte olulist probleemi: — Etalonturbe põhimõte säilib üksnes praktikas (veebilehel), kuid kaob õigusaktist endast. Juhendi olemasolu, ulatus ega ajakohasus ei ole õiguslikult tagatud, kuna § 12 sõnastus on „võib“. Riigi Eesti ettevõtlusmaastik koosneb valdavalt mikro- ja	**Antud selgitus** Eelnõukohase määrusega soovitakse asendada vastavusauditi riskipõhise auditile ja võimaldada organisatsioonidele vajaduspõhist paindlikkust. Riigi Infosüsteemi Ameti ülesanne on turvameetmete süsteemi arendamise ja rakendamise toetamine. Justiits- ja Digiministeerium ei pea vajalikuks Riigi Infosüsteemi Ametile meetmete avaldumise kataloogi avaldamist ja ajakohastamist järgmistel põhjustel: • kohustuslike meetmete kehtestamine eeldab asjakohaste osapoolte ja huvigruppide arvamuse ära kuulamist, mis muudab nende kehtestamise ajakulukaks. Senine praktika on näidanud, et nõuete kehtestamine jääb jalgu uute nõuete kehtestamise vajadusele. Seetõttu on soovituste koostamine kiirem meede võimalikele ohtudele reageerimisel jättes samas organisatsioonile tegevusvabaduse; • seadusega ei ole ministrile antud õigust edasi volitada Riigi Infosüsteemi Ametile turvameetmete kehtestamise õigust;

	Märkus	Märkusega arvestamine
	väikeettevõtjatest, kelle jaoks adekvaatsete meetmete iseseisev konstrueerimine eeldab pädevust, mida turul napib. — Tekib auditeeritavuse probleem. E-ITSi järgimise audit on oma olemuselt vastavusaudit — eelnõu § 11 lõike 1 kohaselt hinnatakse, kas rakendatud meetmed vastavad 2. peatüki nõuetele. Kui sisulised meetmed ei sisaldu enam siduvas õigusaktis, jääb ebaselgeks, mille vastu audiitor vastavust hindab. Mittesiduva juhendi vastu vastavuse hindamine ei ole vastavusaudit tavapärases tähenduses ning loob aluse auditite ebaühtlaseks kvaliteediks ja tõlgenduseks. Soovime rõhutada üht põhimõttelist tagajärge. Etalonturbe väärtus seisneb selles, et see võimaldab organisatsioonil teatava kaitsetarbeni toime tulla ilma pideva, kuluka ja kõrget pädevust nõudva riskihalduseta — kuna alusohte arvestav riskihaldus on kohustuslikes põhimeetmetes juba ette tehtud. Meetmed ja nende aluseks olevad ohud moodustavad lahutamatu paari. Hetkel, mil alusohte arvestavaid meetmeid ei rakendata enam täies mahus, see paar katkeb: rakendatud meetmed ei kata enam tõendatavalt tegelikke riske ning ainus, mis selle lünga taas sulgeb, on organisatsiooni enda läbiviidav täiemahuline riskihaldus. Eelnõu eeldab seega vaikimisi, et iga kohuslane suudab kohe asuda läbi viima riskihaldust tasemel, mille etalonturve seni keskselt tagas. Enamiku mikro- ja väikeorganisatsioonide puhul ei ole see eeldus realistlik, mistõttu praktiline tagajärg on infoturbe taseme langus — vastuolus määruse enda deklareeritud eesmärgiga. **Ettepanek: sätestada selgelt, kas ja millises ulatuses RIA infoturbekataloogi meetmed avaldab, ning kuivõrd need on auditi käigus vastavuse hindamise aluseks. Kaaluda § 12 sõnastuse muutmist „võib“ asemel kohustavaks osas, mis puudutab meetmete kataloogi avaldamist ja ajakohastamist, et tagada auditeeritavuse ja etalonturbe põhimõtte säilimine.**	• Riigi Infosüsteemi Amet on küberturvalisuse seaduses ja selle alusel antud õigusaktides sätestatud nõuete täitmise üle riiklikku ja haldusjärelevalvet teostav asutus, mistõttu nõuete kehtestamine sama asutuse poolt on vastuolus sõltumatu järelevalve põhimõttega. Soovituslikud juhised ei oma kohuslikkuse momenti, kuid need aitavad organisatsioonidel, eriti väiksematel organisatsioonidel, aru saada turvameetmete süsteemist ja abistavad rakendamisel. Ühtlasi annavad juhised ülevaate riigi vaatenurgast turvameetmete rakendamisel, kuid ei seo organisatsioone nendega kui õigusaktides sätestatud eesmärgid on saavutatavad muul viisil. Juhiste kaudu saab Riigi Infosüsteemi Amet edastada ka organisatsioonidele teavet turvameetmete parima praktika kohta või anda teada võimalikest ohtudest.

	Märkus	Märkusega arvestamine
2.	**Eel-, vahe- ja järelauditi kaotamine ning sõltumatu kindlustunde vähenemine** Eelnõu asendab senise eelauditi, vaheauditi ja järelauditi struktuuri organisatsioonisisese hindamisega (§ 10) ja perioodilise välisauditiga. Kõrge tasemega riski korral ei järgne enam sõltumatut järelauditit, vaid auditeeritav teavitab järelevalveasutust riski kõrvaldamisest (lisa 2 punktid 7.3–7.4). Sõltumatu järelkontroll asendub sisuliselt enesedeklaratsiooniga. Ühing peab seda murekohaks kahel põhjusel: — Järgmine sõltumatu kontroll võib olla kuni kolm aastat eemal. E-ITSi vastavusauditi välp on määruse nr 121 § 4 lõike 1 kohaselt kolm aastat. Vaheauditi kaotamisega võib varem ligikaudu aasta jooksul nõutav tegevus venida kuni kolmeaastase tsükli lõpuni, ilma vahepealse sõltumatu kontrollita. — Eelauditi kadumisega jõuab auditisse tõenäoliselt rohkem suurema hulga lahknevustega organisatsioone. Kui klient esitab teenusepartnerile või kliendile „punase“ järeldusotsuse, tekib küsimus, millisel alusel saab usaldada, et riskidega on tegelikult tegeletud, kui sõltumatu järelkontroll puudub. Jääb ebaselgeks, kas ja kuidas kujundab järelevalveasutus oma seisukoha organisatsiooni enda teavituse põhjal. Arvestades, et küberturvalisuse seaduse § 7 nõuete (mida E-ITS rakendab) rikkumisega võivad kaasneda olulised haldussanktsioonid, ei ole sõltumatu järelkontrolli asendamine enesedeklaratsiooniga ühingu hinnangul pelk menetluslik lihtsustus, vaid see nõrgendab tõenduslikku alust just seal, kus tagajärjed on kõige tõsisemad. **Ettepanek: kaaluda kõrge tasemega riski korral sõltumatu järelkontrolli (nt sihitud järelauditi) säilitamist enesedeklaratsiooni asemel või selle kõrval, ning täpsustada, kuidas järelevalveasutus kõrvaldamise tõendatust hindab. Samuti tasub kaaluda mehhanismi, mis võimaldab**	**Antud selgitus** Eelnõukohase määrusega soovitakse suurendada organisatsiooni enda vastutust turvameetmete rakendamisel. Niisamuti peab organisatsioon pidevalt hindama oma turvameetmete rakendamist. Auditi eesmärk on hinnata, kas auditeeritava organisatsiooni infoturbe halduse süsteem ja selle raames rakendatud meetmed vastavad nõuetele ning kaitsevad organisatsiooni äriprotsesse ja eesmärkide täitmist. Seega puudub täiendav vajadus auditeerida kas organisatsioon on valmis auditiks (eelaudit) ja kas organisatsioon on (põhi)auditis toodud puudused likvideerinud. Muudatuse tulemusel suureneb organisatsiooni oma vastutus kuidas ja milliste meetmetega rakendamisega reageeritakse auditis väljatoodud puudustele. Eelnõukohane määrus ei piira organisatsiooni õigust kasutada organisatsioonisisese hindamise käigus välist abi, kui organisatsioon seda vajalikuks peab ja endal vastav kompetents puudub.

	Märkus	Märkusega arvestamine
	vahepealset sõltumatut kontrolli kolmeaastase tsükli jooksul olukordades, kus tuvastatud lahknevuste tase seda õigustab.	
3.	**Kaugtöö 30% piirang (auditeerimiseeskiri punkt 2.4)** Lisa 2 punkti 2.4 kohaselt ei tohi kaugtöötunnid ületada 30% audititööks kavandatud tundide koguarvust. Ühing leiab, et see piirang ei teeni oma eesmärki ega tõsta auditite kvaliteeti. Enamik audititoiminguid — intervjuud, dokumentatsiooni läbivaatus ja aruandlus — on tänapäevaste digitaalsete töövahenditega tehtavad tõhusalt ja kvaliteeti kaotamata. Auditite ebaühtlase kvaliteedi juurpõhjus ei ole kohapeal veedetud tundide vähesus, vaid pigem audiitori pädevus ja kohusetunne ning tellija teadlikkus. Kaugtöö piiramine tõstab tarbetult auditi maksumust (transport, sellele kuluv aeg, majutus) ning koormab nii auditeeritavat kui audiitorit, ilma vastava kvaliteedivõiduta. Märgime ühtlasi, et kohustuslik paikvaatlus on juba tagatud lisa 2 punktiga 5.7.3. **Ettepanek: loobuda kaugtöö 30% piirangust. Auditi kvaliteedi tagamiseks on tulemuslikum: (a) säilitada kohustuslik paikvaatlus auditi osana (juba punkt 5.7.3); (b) luua võimalus auditite kvaliteedi (pistelisteks) järelkontrollideks, sealhulgas eeskirja mittejärgivate audiitorite ja juhtivaudiitorite suhtes meetmete rakendamiseks; ning (c) toetada auditi tellijat nõuga ja võimaldada audiitori vahetust, kui ilmneb, et teenuse kvaliteet ei ole nõuetekohane.**	**Arvestatud sisuliselt** Lisa 2 punkt 2.4 sõnastatud järgmiselt: *2.4. Auditi tegemine plaanitakse koostöös auditeeritava kontaktisikuga, kes tagab vajalike andmete ja isikute kättesaadavuse auditi ajal. Põhjendatud juhtudel ja eelneval kokkuleppel võib auditiprotseduure teha kaugtöö vormis, sellisel juhul kajastatakse see fakt auditi lõpparuandes ja auditi järeldusotsuses koos kaugtöö vormis tehtud auditi käsitlusala kirjeldusega.*
4.	**Auditiprotseduuride 60% miinimum (auditeerimiseeskiri punktid 3.8 ja 5.7)** Lisa 2 punktide 3.8 ja 5.7 kohaselt peab auditiprotseduuridele kuluvate tundide arv moodustama vähemalt 60% auditiks kavandatud töötundide koguarvust. Sarnaselt eelmise punktiga peab ühing seda ettekirjutust ebavajalikuks ja vähetõhusaks.	**Jäetud arvestamata** Ettepanek auditeerimisprotsesside piiritlemiseks saadud kehtiva E-ITSi rakendamise tagasisidena rakendajatelt.

	Märkus	Märkusega arvestamine
	Kohusetundlik, eeskirja järgiv audiitor teostab auditiprotseduurid niikuinii korrektselt; protsendi ettekirjutamine ei taga kvaliteeti. Kvaliteeti aitavad tagada punktis 3 nimetatud meetmed, mitte tundide jaotuse normimine. **Ettepanek: kaaluda punktides 3.8 ja 5.7 sätestatud 60% miinimumi väljajätmist ning auditi kvaliteedi tagamist sisuliste meetmete kaudu (kvaliteedikontroll, sanktsioonid, tellija toetamine).**	
5.	**Auditi aruande dokumenteerimise tähtaeg (auditeerimiseeskiri punkt 6.12)** Lisa 2 punkti 6.12 kohaselt esitatakse auditi järeldusotsuse ja lõpparuande kavand auditeeritavale seitsme päeva jooksul pärast auditiprotseduuride lõppemist. See tähtaeg näib olevat üle võetud ISO/IEC 27001 sertifitseerimisauditite praktikast, kus aruandluse maht on E-ITSi auditiga võrreldes väiksem. Praktikas, kus auditeid tehakse hooajaliselt suurel hulgal korraga ja hinnakonkurentsi tingimustes, surub lühike tähtaeg kahes suunas: kas vähendada aruande põhjalikkust või planeerida „viimane auditiprotseduur“ kunstlikult hetke, kus suurem osa dokumenteerimisest on juba tehtud. Juhime tähelepanu, et ebapiisav põhjalikkus on RIA enda poolt nimetatud E-ITSi ja ISO/IEC 27001 auditite probleemina. Lühike dokumenteerimistähtaeg töötab seega osaliselt reformi enda deklareeritud eesmärgi vastu. **Ettepanek: pikendada järeldusotsuse ja lõpparuande kavandi esitamise tähtaega või siduda see auditi mahuga, et tagada aruandluse põhjalikkus ilma kunstliku ajaplaneerimiseta.**	**Jäetud arvestamata** Eelnõukohase määrusega vähendatakse auditi ulatust, jättes välja kohustuse teha eelaudit, vaheaudit ja järelaudit. Seeläbi väheneb ka audiitorite töökoormus võimaldades neil keskenduda auditile (end põhiaudit) põhjalikumalt.
6.	**Üleminek ja kehtivad hankelepingud** Eelnõu näeb ette kolmeaastase üleminekuperioodi. Jääb siiski ebaselgeks, mis saab kehtivatest kolmeaastastest	**Antud selgitus**

	Märkus	Märkusega arvestamine
	hankelepingutest, milles vaheauditid on hanke tulemina juba defineeritud ja eraldi tööna eelarvestatud. Eelnõu ja seletuskiri ei käsitle, kuidas neid lepingulisi kohustusi uue auditistruktuuriga ühildatakse. **Ettepanek: täpsustada seletuskirjas või rakendussätetes, kuidas käsitletakse enne määruse jõustumist sõlmitud hankelepinguid, milles vaheauditid on eraldi tööna kokku lepitud.**	Eelnõukohases määruses ei ole volitusnormist tulenevalt lubatud reguleerida riigihangete seadusest ja selle alusel antud õigusaktides sätestatut või lepinguõigust. Eelnõukohase määruse jõustumisel on organisatsioonidel vabadus üle vaadata oma lepingud ning hinnata lepingu täitmise võimalikkust või võimatust eelpool nimetatud õigusaktides ja omavahelistes lepingutes sätestatust lähtuvalt. Samas on Justiits- ja Digiministeerium ülemineku aja sätestamisel arvestanud senise kolme aastase auditi välbaga ja sellest tulenevate võimalike vastastikuste lepinguliste kohustustega. Eelnõukohase määruse jõustumisel ei keelata organisatsioonidel E-ITS seni kehtivas versioonis sätestatud vaheauditite läbi viimist lepingu täitmise raames ja vastavat auditit on võimalik käsitleda organisatsioonisisese hindamisena.
7.	**Sõnastuslikud ja terminoloogilised ebatäpsused määruse tekstis** Lisaks eeltoodud sisulistele märkustele juhib ühing tähelepanu, et eelnõu teksti keelt on kohati sedavõrd lihtsustatud ja optimeeritud, et selle tehniline tähendus on muutunud eksitavaks. Kuna E-ITS on auditeeritav normdokument, on sätete täpne ja üheselt mõistetav sõnastus auditeeritavuse otsene eeldus. Toome alljärgnevalt illustreerivad näited — tegemist ei ole ammendava loeteluga: **/…/** **Ettepanek: viia läbi eelnõu teksti põhjalik keeleline ja terminoloogiline ülevaatus, pöörates tähelepanu tegijate eristamisele, käände- ja reemakasutusele ning põhiterminite üheselt mõistetavusele. Eeltoodud näited on illustreerivad, mitte ammendavad**	Eelnõule ja seletuskirjale on tehtud keetoimetajate poolt koostöös valdkondlike spetsialistidega keeleline ja terminoloogiline ülevaatus. Enne eelnõu esitamist määrusena allkirjastamiseks korratakse kontrolli.

	Märkus	Märkusega arvestamine
	— **§ 1 lõige 1** sätestab, et E-ITSi rakendamine „seisneb … infoturbe halduses ja infoturbe halduse meetmete auditeerimises“. Rakendamise teostab organisatsioon, kuid auditeerimise teostab sellest sõltumatu väline isik (§ 11 ja lisa 2). Rakendamine ei saa määratluse järgi hõlmata auditeerimist, kuna tegemist on eri tegijatega. Soovitame sättes tegijad eristada.	**Antud selgitus** Infoturbe süsteemi haldus hõlmab ka turvameetmetele rakendamise seiret. Seire üks osa on auditeerimine. Eesti Infosüsteemide Audiitorite Ühing on õigesti välja toonud, et auditeerimise juures eeldatakse välise osapoole hinnangut, kuid see ei tähenda, et tegemist oleks infoturbe süsteemi haldusest eraldiseisva tegevusega. Auditeerimise eraldi välja toomisega sooviti just rõhutada seda kui ühte halduse osa.
	— **§ 1 lõige 3 punkt 1** kasutab terminit „avalik“. Küberturvalisuse 2. direktiivi mõiste „public“ ja eestikeelse vaste „avalik“ tähendus ei pruugi kattuda — arvestades avaliku teabe seaduse mõistekasutust, võib „avalik“ hõlmata ka mitteavalikke või juurdepääsupiiranguga osi, eelkõige kriitiliste süsteemide kontekstis. Üks määruse põhitermineid jääb seetõttu tõlgendusele avatuks. Palume täpsustada, mida mõeldakse mõiste „avalik“ all.	**Antud selgitus** Viidatud punktis ei kasutada sõna „avalik“ eraldiseisvana vaid tegemist on „avaliku ülesandega“.
	— **§ 2 (infoturbe halduse süsteemi määratlus)** sõnastus „riskide hindamisel, käsitlemisel ja aktsepteerimisel põhinev“ jätab mulje, justkui tuleks iga risk alati aktsepteerida. Sama määruse § 4 lõike 2 punktist 4 ja § 8 lõikest 9 nähtub, et riski aktsepteerimine on otsustuskoht, mitte vältimatu samm. Soovitame sõnastust täpsustada.	**Arvestatud** Termini lahti kirjutus määruse tekstist välja jäetud.
	— **§ 2 lõige 1 punkt 4** — ingliskeelne vaste „(inglise keeles business process)“ paikneb fraasi „toode või teenus“ järel, mistõttu säte loeb nii, nagu oleks „toode või teenus“ ingliskeeli business process. Ingliskeelne vaste peab paiknema vahetult tõlgitava termini („äriprotsess“) järel. Ühing märgib ühtlasi, et ingliskeelsete vastete lisamine määruse teksti sisse väärib üldisemat kaalumist.	**Arvestatud** Viide inglise keelsele vastele määruse tekstist välja jäetud.

	Märkus	Märkusega arvestamine
	— **§ 3 lõige 2 punkt 1** — sõnastus „turvameetmed on vara kogu elutsükli ulatuses plaanitud uue vara ja teenuste hankimise etappi“ on eksitav nii käände- kui ka reemakasutuse poolest. Hankimise etapis meetmeid plaanitakse, kuid ei rakendata. Soovitame sõnastada näiteks „turvameetmed on plaanitud vara kogu elutsükli ulatuses“.	**Antud selgitus** Meetmete rakendamine võib alata juba enne uue vara kasutusele võtmist. See hõlmab ka vara kasutusele võtmiseks vajalike tingimuste loomist ja rakendamist, sh ka katsetamist.
	— **§ 6 lõige 1** — sõnastus „varade arvelevõtmine ja nende kaitseala kindlaksmääramine“ seostab kaitseala varadega. Tegemist on kategooriaveaga: kaitseala ei kuulu varadele, vaid infoturbe halduse süsteemile (vrd RIA seletav sõnaraamat). Soovitame sõnastust parandada nii, et kaitseala seostatakse õige objektiga.	**Arvestatud** § 5 lg 1 (end § 6 lg 1) sõnastust muudetud järgmiselt: *Enne riskihaldusmetoodika kasutuselevõtmist peab organisatsioon tuvastama kaitseala äriprotsessile olulised varad..*
	— **§ 10 (loetelu)** kasutab võõrkeelset, ümberpööratud süntaksit: „kas tal on kindlaks määratud äriprotsessid“ selle asemel, et öelda „kas ta on äriprotsessid kindlaks määranud“. Ümberpööramine nihutab rõhku (reemat) ja muudab loetelupunktide tehnilist tähendust — tekivad parasiittähendused nagu „kaardistatud äriprotsess“, „vastendatud infoturbekataloog“ ja eelkõige „koostatud infoturvameetmed“ (vastandina ülevõetud, mitte ise koostatud meetmetele). Viimane näide seostub otseselt käesoleva kirja punktis 1 tõstatatud küsimusega: sõnastus jätab lahtiseks, kas meetmed on organisatsiooni enda koostatud või mujalt üle võetud, mis on auditeeritavuse seisukohast oluline. Soovitame loetelu sõnastada tegevuspõhiselt.	**Võetud teadmiseks**
Eesti Kaubandus-Tööstuskoda 29.06.2026 kiri nr 4/121		

	Märkus	Märkusega arvestamine
	Eelnõu § 3 lg 2 näeb ette kohustuse määrata infoturbe halduse süsteemi toimimiseks konkreetsed rollid (hankejuht, infoturbejuht, kasutaja ja äriüksuse juht). Leiame, et sätte praegune sõnastus vajab täpsustamist. Kuigi seletuskirja lk 6 kohaselt ei tähenda nimetatud rollid tingimata konkreetseid ametikohti, vaid kirjeldavad tegevusi, loob eelnõus kasutatud sõnastus ettevõtjatele mulje, et organisatsioonis tuleb formaalselt määrata just selliste nimetustega rollid. See vähendab õigusselgust ning võib praktikas tekitada vastuolu ettevõtjate olemasoleva juhtimis- ja vastutusmudeliga. Eriti problemaatiline on mõiste „hankejuht“, millel on ettevõtluspraktikas väljakujunenud tähendus kui hangete läbiviimise eest vastutaval spetsialistil. Eelnõu § 3 lg 2 p 1 kohaselt aga hankejuht jälgib, et vara ja teenuste turvameetmed on kogu nende elutsükli ulatuses plaanitud uue vara ja teenuste hankimise etappi juba selle kavandamise käigus. Seega eelnõus kirjeldatud ülesanded ei vasta hankejuhi rolli tavapärasele sisule. Samuti on küsitav „kasutaja“ käsitlemine eraldiseisva rollina, kuna sisuliselt hõlmab see kogu organisatsiooni personali. Kaubanduskoda leiab, et määruse tasandil tuleks sätestada eelkõige organisatsiooni kohustused ja vastutusalad infoturbe halduse süsteemi toimimiseks, mitte detailsed organisatsioonisisesed rollid või ametinimetused. Organisatsioonile peab jääma paindlikkus otsustada, kuidas ja kelle kaudu neid ülesandeid täidetakse. Kui rollide loetelu siiski säilitatakse, teeme ettepaneku kasutada praktikaga paremini kooskõlas olevaid ja funktsioonipõhiseid mõisteid. **<u>Kaubanduskoja ettepanek</u>**: **Teeme ettepaneku sõnastada eelnõu § 3 lg 2 ümber selliselt, et selles sätestataks organisatsiooni kohustus tagada infoturbe halduse süsteemi toimimiseks vajalike ülesannete täitmine ja vastutusalade määramine, jättes organisatsioonile**	**Arvestatud sisuliselt** Rollid asendatud tegevustega, mida on vaja arvestada infoturbe halduse süsteemi toimimisel. Lisatud andmekaitse. Andmekaitse hõlmab organisatsiooni kui ka organisatsioonile usaldatud andmete kaitse kavandamist ja korraldamist. Muu hulgas hõlmab ka isikuandmete kaitset organisatsiooni poolt, kes neid töötleb.

	Märkus	Märkusega arvestamine
	paindlikkuse otsustada, kuidas ja kelle kaudu neid ülesandeid täidetakse. Konkreetsete rollide ja ametinimetuste loetelu tuleks sättest eemaldada.	
	Eesti Vee-ettevõtete Liit 27.06.2026 e-kri	
	Meile jõudis kooskõlastamisele justiits- ja digiministri määruse "Eesti infoturbestandard" eelnõu. *Eelnõu kohaselt ei pea E-ITSi meetmeid rakendama 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. Siinjuures ei ole oluline, kes on teenuseosutaja omanikud. See tähendab, et avaliku sektori osalus ei välista erandi tegemist. See erand ei kehti teenuseosutajale, kui ta on avaliku teabe seaduse kohane andmekogu vastutav või volitatud töötleja. Oluline on vahet teha, et andmekogu vastutav ja volitatud töötleja ei ole sama mis andmete vastutav või volitatud töötleja isikuandmete kaitse üldmääruse tähenduses.* Palun Teie seisukohta, kas vee-ettevõtted, kelle töötajate arv on alla 50 inimese ja aastakäive on alla 10 mln euro lähevad E-ITSi erandi alla või mitte. Võite selgituse anda konkreetse vee-ettevõtte näitel, nt Paide Vesi. Palun seda selgitust, kuna vee-ettevõtteid nõustavad küberturbe spetsialistid on andnud seisukoha, et kõik vee-ettevõtted	**Selgitame:** Tuleb eristada küberturvalisuse seaduse subjekte ja neile kohalduvaid nõudeid. Turvameetmete rakendamisel eristatakse subjekte tegevusvaldkonnast või subjekti olemusest. Turvameetmete rakendamisel ei eristata kas ettevõtja on ülioluline ja oluline üksus. Erisused ja Eesti infoturbestandardi rakendamise kohustuse ulatus on sätestatud Vabariigi Valitsuse 9.12.2022 määruses nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (edaspidi *määrus nr 121).* **1. Eesti infoturbestandardi rakendamisest** Määruse nr 121 § 2^1 punktist 1 lähtuvalt ei ole Eesti infoturbestandardi rakendamise kohustust teenuseosutajal, 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. Sätte juures tuleb arvesse võtta järgmist: 1) säte kohaldub vaid eraõiguslikule juriidilisele isikule, kes on kantud äriregistrisse. Sätet ei kohaldata valitsusasutuse või kohaliku omavalitsuse hallatavale asutusele, mis on kantud riigi- ja kohaliku omavalitsuse asutuste riikliku registrisse.

	Märkus	Märkusega arvestamine
	sõltumata suurusest peavad E-ITSi nõudeid rakendama ja auditi tegema. Lisaks viitavad nad oma kirjas, et KüTS § 3 lg 2 p 2 määratleb elutähtsa teenuse osutaja üliolulisekс üksuseks **sõltumata** töötajate arvust või finantsnäitajatest. Suuruse kriteerium (50+ töötajat) on lisatingimuseks vaid teatud spetsiifiliste teenuseosutajate puhul (nt KüTS § 3 lg 2 p 8 sideettevõtjad). Sellist seisukohta ma eelnõust välja ei lugenud, mistõttu sooviksin ka selles osas Teie seisukohta. Lisaks palun selgitage, kui ettevõte haldab infosüsteeme, siis kas ja millisel juhul tuleks vee-ettevõtja lugeda avaliku teabe seaduse kohaseks andmekogu vastutavaks või volitatud töötlejaks. Jään ootama Teie tagasisidet, kuna siiani oli meil seisukoht, et väikesed vee-ettevõtted E-ITSi kohaldama ei pea.	2) töötajate arvu ja aastast bilansimahtu või aastakäivet vaadatakse kolme aasta lõikes, See tähendab, et kui kolmest viimaset aastast jääb vähemalt kahel aastal kriteeriumid komisjoni soovituses toodud piiridesse, siis loetakse isik vastavalt mikro- või väikeettevõtjaks. 3) teenuse osutaja ei ole samal ajal andmekogu vastutav töötleja või andmekogu volitatud töötleja vastavalt avaliku teabe seaduse § 43^4 lõike 1 tähenduses või § 43^4 lõike 2 tähenduses. 4) teenuseosutaja ei kuulu korporatsiooni, mille kogu näitajad ületavad Euroopa komisjoni soovituses toodud väikeettevõtja määratlust. Siinjuures ei loeta korporatsiooniks kohalikku omavalitsust. **2. Andmekogu** Määruse nr 121 kohaselt on andmekogu vastutav või volitatud töötleja kohustatud Eesti infoturbestandardit rakendama, kui tegemist on andmekoguga avaliku teabe seaduse (edaspidi AvTS) tähenduses. AvTS § 43^1 lõike 1 kohaselt on andmekogu riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks. Avalikku ülesanne täitvaks isikuks loetakse eraõiguslik isik, kelle avalik ülesanne on pandud seadusega (nt Liikluskindlustuse fond) või antud halduslepinguga (nt tehnoülevaatus). Siinjuures selgitame, et andmekoguks on antud juhul vaid avaliku ülesande täitmiseks loodud andmekogu, kuid avaliku ülesande täitmise väliseid andmete kogumeid ei loeta andmekoguks AvTS

	Märkus	Märkusega arvestamine
		tähenduses. Elutähtsa teenuse osutamiseks kasutavad andmete kogumid (nt kliendiandmebaas) ei ole ka andmekogud AvTS tähenduses Eeltoodust lähtuvalt saab asuda seisukohale, et andmekogu all ei mõelda määruses nr 121 igasugust andmete kogumit vms, vaid sellist, mis on asutamine ja kasutamine eesmärk on õigusaktis sätestatud. **3. Vastutav töötleja** Avaliku teabe seaduse § 43^4 lõikes 1 on andmekogu vastutav töötleja (haldaja) defineeritud kui „riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist. Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest.“ **4. Volitatud töötleja** AvTS § 43^4 lõikes 1 on andmekogu vastutav töötleja (haldaja) defineeritud kui „riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist. Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest.“ Sama paragrahvi lõike 2 kohaselt võib andmekogu vastutav töötleja „volitada andmete töötlemise ja andmekogu majutamise teisele riigi- või kohaliku omavalitsuse asutusele, avalik-õiguslikule juriidilisele isikule või hanke- või halduslepingu alusel eraõiguslikule isikule vastutava töötleja poolt ettenähtud ulatuses“.

	Märkus	Märkusega arvestamine
		Tegemist on siis volitatud töötlejale vastava ülesande volitamisega. Andmekaitse Inspektsioon on oma andmekogude juhendis volitatud töötleja ja tema rolli kohta märkinud: „*volitatud töötleja võib olla nii vastutava töötleja kontrolli all tegutsev andmekogu igapäevane haldaja kui ka teenuste osutaja näiteks andmekogu majutaja või arendajana. Sellist volitatud töötleja rolli täidavad paljude andmekogude suhtes IT-asutused nagu RIK ja SMIT. Teenuse osutajaid ei ole vajalik põhimääruses nimepidi loetleda, piisab nende ülesannete nimetamisest*“. See tähendab et andmekogu volitatud töötleja all avaliku teabe seaduse kontekstis on mõeldud ennekõike volitatud töötlejat, kes majutab konkreetset andmekogu ja vajaduse korral tegeleb selle andmekogu arendamise ja ülalpidamisega. Andmekogu volitatud töötleja all ei ole siinjuures mõeldud näiteks andmeandjat avaliku teabe seaduse tähenduses (vt AvTS § 43^5 lõige 2) ega ka mitte igasugust isikuandmete volitatud töötlejat isikuandmete kaitse üldmääruse või isikuandmete kaitse seaduse tähenduses. Volitatud töötlejaks ei loeta isikut kes seadusest tuleneva kohustuse täitmiseks esitab iseseisvalt andmeid riiklikku või kohaliku omavalitsuse üksuse asutud registrisse (nt teabe esitamine töötamise registrisse, majandustegevuse registrisse või äriregistrisse). **5. AS Paide Vesi näide** 5.1. Näite sisustamisel oleme arvesse võtnud vaid avalikult kättesaadavat teavet, mis on avaldatud äriregistris, Riigi Teatajas ja AS Paide Vesi veebilehel (www.paidevesi.ee): 5.1.1. AS Paide Vesi on kantud äriregistrisse, õiguslik vorm aktsiaselts;

	Märkus	Märkusega arvestamine
		5.1.2. AS Paide Vesi keskmine töötajate arv aastatel 2022-2024 on vähem kui 50; 5.1.3. AS Paide Vesi aastane bilansimaht või aastakäive ei ületa aastatel 2022-2024 10 miljonit eurot; 5.1.4. Riigi Teatajas ei ole avaldatud õigusakti, millest nähtuks, et AS Paide Vesi oleks määratud mõne riikliku või kohaliku omavalitsuse andmekogu vastutavaks või volitatud töötlejaks; 5.1.5. äriregistrist ei nähtu AS Paide Vesi kuulumine laiemasse korporatsiooni. Arvestades punktis 5.1. toodut võib asuda seisukohale, et AS Paide Vesi on väiksem kui keskmise suurusega ettevõtja, kes ei ole ka samas andmekogu vastutav või volitatud töötleja. Seetõttu ei ole sellel vee-ettevõtjal määruse nr 121 kohaselt Eesti infoturbestandardi rakendamise kohustust. Küberturvalisuse seaduse subjektina peab AS Paide Vesi oma võrgu- ja infosüsteemide kaitseks esmaseid turvameetmeid. Ettevõtja võib vabatahtlikult rakendada täiendavalt Eesti infoturbestandardi meetmeid, ilma et sellega kaasneks standardi rakendamise, sealhulgas auditeerimise kohustus.
	Eesti Energia AS 25.06.2026 kiri	
1.	Teeme ettepanku viia E-ITS määruse eelnõu § 3 lõike 2 punktides 1 ja 4 olevad mõisted „hankejuht“ ja „äriüksuse juht“ ühe mõiste alla, mis võiks olla „vara omanik“. „Hankejuhi“ mõiste omab praktikas väga kindlat tähendust - tegemist on hagete läbiviimist toetava spetsialisti või hankeüksuse juhiga, kellel ei ole volitusi otsustamaks, kas midagi hankida (praktikas on tegemist rolliga, kes teab, kuidas hankida). Seega sellele mõistele praktikast	**Arvestatud sisuliselt** Rollid asendatud tegevustega, mida on vaja arvestada infoturbe halduse süsteemi toimimisel. Lisatud andmekaitse. Andmekaitse hõlmab organisatsiooni kui ka organisatsioonile usaldatud andmete kaitse kavandamist ja korraldamist. Muu hulgas hõlmab ka isikuandmete kaitset organisatsiooni poolt, kes neid töötleb.

	Märkus	Märkusega arvestamine
	erineva tähenduses andmine E-ITS määruses tekitab pigem ebaselgust ning seletuskirjas kirjeldatud rolli organisatsioonis tavaliselt hankejuht ei täida. Lähtudes mõlema mõiste sisust, siis sellist rolli organisatsioonis täitab üldjuhul „vara omanik“, kellel on olemas vajalikud ressursid (nt rahalised vahendid), et tagada vastavate tegevuste ellu viimine. See mõiste on valdkonna praktikutele ühesemalt arusaadavam. Seetõttu teeme ettepaneku kasutada „hankejuhi“ ja „äriüksuse juhi“ asemel ühtset mõistet ja rolli - „vara omanik“, mida saab defineerida järgmiselt: vara omanik - korraldab vara kaardistuse, kaitsetarbe määramise ja vajalike meetmete rakendamise regulaarse seire ning jälgib, et turvameetmed on vara kogu elutsükli ulatuses plaanitud uue vara ja teenuste hankimise etappi juba selle kavandamise käigus.	

Märkuste tabel edastatud märkuste esitajatele tutvumiseks e-kirjaga 30.07.2026