SOTSIAALMINISTEERIUM

Justiits- ja Digiministeerium
info@justdigi.ee

Teie 25.05.2026 nr 8-1/4143-1, JDM/26-0608/-1K

Meie 26.06.2026 nr 1.2-3/1355-6

Kooskõlastuskiri justiits- ja digiministri
Eesti infoturbestandardi määruse eelnõule

Täname võimaluse eest esitada arvamus justiits- ja digiministri määruse „Eesti infoturbestandard“ eelnõule. Toetame üldjoontes Eesti infoturbestandardi kaasajastamist, sealhulgas riskipõhisema ja organisatsioonide eripära enam arvestava lähenemise kasutuselevõttu. Peame oluliseks, et Eesti infoturbestandard aitaks tagada võrgu- ja infosüsteemide turvalisuse ning oleks samal ajal rakendajatele selge, proportsionaalne ja auditeeritav ilma ebamõistliku halduskoormuseta.

Samuti märgime, et võrreldes varasema versiooniga on eelnõu üldjoontes paremini mõistetav ning infoturbekataloogi moodulite ülesehitus loogilisem. Kuid kooskõlastame eelnõu märkustega arvestamisel. Meie hinnangul vajavad mitmed rakendamise seisukohalt olulised küsimused täiendavat täpsustamist.

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 teatud ulatuses ülekantuks. See aitaks vältida ebaproportsionaalset topelttööd ning suunaks organisatsioonide ressursi tegeliku infoturbe parandamisele.

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.

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.
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.

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 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.

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.

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 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.

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.

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.

11. Sisehindaja erapooletus ja hindamise mõiste
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 organisatsiooniväline isik. Palume kaaluda mõiste „organisatsiooni korraldatav hindamine“ kasutamist või täpsustada, et hindamise korraldab organisatsioon, kuid selle võib läbi viia sõltumatu sisemine või väline hindaja.

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.

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 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.

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 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.

Lugupidamisega

(allkirjastatud digitaalselt)
Karmen Joller
sotsiaalminister

Nele Labi
Nele.Labi@sm.ee

Kristella Kukk
kristella.kukk@sm.ee