EESTI INFOSÜSTEEMIDE AUDIITORITE ÜHING
Mäealuse tn 2/1, 12618 Tallinn / registrikood 80007111 / info@eisay.ee / www.eisay.ee

Justiits- ja Digiministeerium
info@justdigi.ee
guido.paasuke@justdigi.ee

Teie 25.05.2026 nr 8-1/4143-1
Meie 26.06.2026

Arvamuse avaldamine justiits- ja digiministri määruse „Eesti infoturbestandard“ eelnõu kohta

Lugupeetud Liisa-Ly Pakosta!

Eesti Infosüsteemide Audiitorite Ühing (edaspidi *ühing*) tänab Justiits- ja Digiministeeriumi võimaluse eest avaldada arvamust justiits- ja digiministri määruse „Eesti infoturbestandard“ eelnõu (edaspidi *eelnõu*) kohta. Ühing koondab Eesti infosüsteemide ja infoturbe audiitoreid ning meie liikmed teostavad muu hulgas Eesti infoturbestandardi (edaspidi *E-ITS*) järgimise auditeid. Esitame oma seisukohad ja ettepanekud alljärgnevalt.

Üldiselt toetab ühing eelnõu eesmärki muuta E-ITS arusaadavamaks, vajaduspõhisemaks ja kiiremini ajakohastatavaks. Samuti peame mõistlikuks auditeerimiseeskirja viimist määruse tasandile ning auditi eesmärgi ja korra senisest selgemat sätestamist. Allpool toome välja mõned sisulised tähelepanekud, mille arvesse võtmine aitaks eelnõu deklareeritud eesmärke paremini saavutada.

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 keskselt 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 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.

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 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.

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. 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.

6. Üleminek ja kehtivad hankelepingud

Eelnõu näeb ette kolmeaastase üleminekuperioodi. Jääb siiski ebaselgeks, mis saab kehtivatest kolmeaastastest 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.

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:

— **§ 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.

— **§ 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.

— **§ 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.

— **§ 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.

— **§ 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“.

— **§ 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.

— **§ 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.

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.

Loodame, et peate võimalikuks ühingu seisukohti ja ettepanekuid arvesse võtta. Oleme valmis neid vajaduse korral täpsustama ning aruteludes osalema.

Lugupidamisega
/allkirjastatud digitaalselt/

Roland R. Puiestik
Eesti Infosüsteemide Audiitorite Ühingu juhatuse liige

Roland R. Puiestik, roland@puiestik.ee