



Justiits- ja Digiministeerium
info@justdigi.ee

Teie 22.09.2026 nr 8-1/6793-1, JDM/26-1041/-1K

Meie 09.10.2026 nr 1.2-3/2246-2

Kooskõlastuskiri sihipärase turvaauditi korraldamise tingimustele ja korrale

Kooskõlastame justiits- ja digiministri määruse „Sihipärase turvaauditi korraldamise täpsemad tingimused ja kord“ eelnõu järgmiste märkustega.

Toetame eesmärki parandada võrgu- ja infosüsteemide turvalisust ning tagada oluliste teenuste toimepidevus. Samas peab järelevalvemenetluses kohustusliku turvaauditi määramine olema läbipaistev ja põhjendatud ning sellega kaasnev rahaline koormus proportsionaalne ja võimalikult ettenähtav. Eelnõu vajab selles osas täiendamist.

1. Sihipärase turvaauditi määramise aluste täpsustamine

Eelnõu § 2 lõike 1 kohaselt tehakse teenuseosutajale sihipärase turvaauditi läbimise kohustus teatavaks haldusaktiga, milles määratakse muu hulgas auditi käsitlusala. Säte ei täpsusta aga, millistel asjaoludel on põhjendatud kohustada teenuseosutajat tellima audit sõltumatult audiitorilt ja kandma selle kulud.

Küberturvalisuse seaduse § 16 lõike 1¹ punkt 2 ja § 17 lõike 1¹ punkt 2 seovad sihipärase turvaauditi Riigi Infosüsteemi Ameti (edaspidi RIA) või teenuseosutaja tehtud riskihindamise või muu kättesaadava riskiteabega. Määruses tuleb täpsustada selle aluse rakendamise tingimusi - milliste asjaolude ja kaalutluste põhjal otsustab RIA, et konkreetse riski hindamiseks või nõuete täitmise kontrollimiseks on vajalik teenuseosutaja kulul tehtav sõltumatu audit. Seletuskirjas esitatud üldine viide kaalutlusõigusele ning haldusmenetluse seaduse ja korrakaitse seaduse nõuetele ei taga üksi meetme kasutamise piisavat ettenähtavust.

Palume täiendada eelnõu § 2 lõiget 1 nõudega, et auditi määramise haldusaktis tuuakse välja auditi aluseks olevad konkreetset riskid või riskiteave, auditi eesmärk ning sõltumatu audiitori kaasamise vajaduse ja proportsionaalsuse põhjendus. Auditi käsitlusala tuleb piiritleda nende riskide ja kontrollitavate nõuetega. Samuti tuleb põhjendada, miks olemasolevatest andmetest, varasemate auditite tulemustest või vähem koormavatest järelevalvemeetmetest ei piisa.

Eelnõu § 2 lõike 3 puhul palume täpsustada korduvate auditite määramise tingimusi ja sagedust ning nõuda nende vajaduse eraldi põhjendamist. Üksnes ajavahemiku määramine ei piira piisavalt võimalike auditite arvu ega nendega kaasnevat kogukulu. Korduvate auditite

määramisel tuleb arvestada varasemate auditite tulemusi ja puuduste kõrvaldamist ning vältida samade asjaolude põhjendamatut korduvat kontrollimist.

2. Auditit hinna piiramine ja kulude eelarveline kavandamine

Eelnõu § 3 lõike 1 kohaselt kannab sihipärase turvaauditi kulu üldjuhul auditeeritav teenuseosutaja. Eelnõus puudub aga mehhanism, mis piiraks kohustusliku auditit hinda või teenuseosutaja kanda jäävat kulu. E-ITSi auditite tellimise senine kogemus on näidanud, et kohustusliku auditeerimisega kaasnev nõudlus ja piiratud pakkumine võivad viia hinnad ebamõistlikult kõrgele. Auditit tellimise kohustus ja selle täitmise tähtaeg vähendavad seejuures hankija võimalusi teenuse hinnale mõju avaldada.

Eelnõu § 4 lõikes 3 ja lõike 4 punktis 3 sätestatud võrdlus samaväärse auditit turuhinnaga puudutab üksnes kulu hüvitamise ulatust. See ei piira audiitori küsitavat hinda ega kaitse teenuseosutajat olukorras, kus turuhind tervikuna tõuseb ebamõistlikult kõrgele. Lisaks ei laiene hüvitamise võimalus kõigile auditeeritavatele teenuseosutajatele. Seetõttu ei saa hüvitamise korda käsitada piisava abinõuna auditit maksumuse kontrollimiseks.

Teeme ettepaneku kehtestada vähemalt teenuseosutaja kanda jääva kohustusliku auditikulu ülempiir ehk hinnalagi. Piirmäärad võib vajaduse korral diferentseerida auditit käsitusala, mahu ja keerukuse järgi. Regulatsioon peab ühtlasi lahendama olukorra, kus nõutava auditit tegemiseks ei ole võimalik saada piirmäära piiresse jäävat pakkumust - teenuseosutajat ei tohi kohustada kandma piiramatut kulu, vaid ette tuleb näha auditit korraldamine RIA poolt või põhjendatud ülempiiri ületava kulu katmine RIA eelarvest. Kui sellise lahenduse kehtestamine ületab määruse volitusnormi piire, palume algtada vajalik seadusemuudatus.

Palume sätestada ka auditit eeldatava maksumuse ja teenuseosutaja kanda jääva kulu hindamine enne auditit määramist ning näha ette võimalus saada enne audiitoriga lepingu sõlmimist kindlus hüvitamise aluse ja ulatuse kohta. Eelnõus kavandatud tagantjärele hüvitamine ei lahenda olukorda, kus asutusel puuduvad vahendid auditit tellimiseks ja selle eest tasumiseks.

Asutuste eelarvete kavandamisel ei ole võimalik arvestada määramata ajal ja mahus tekkivate auditikuludega ning meie valitsemisalas ei ole selliste võimalike kulude katmiseks eraldi vahendeid ette nähtud. Palume selgitada, millisest rahastamisallikast kaetakse eelarveaasta kestel määratud auditit kulu, ning näha ette auditit korraldamiseks tähtaeg, mis arvestab hanke läbiviimise ja eelarvevahendite tagamisega. Kiiret sekkumist nõudvate riskide puhul tuleb lahendada auditit rahastamine viisil, mis võimaldab meetme viivitamata rakendada.

Palume täiendada seletuskirja mõjuanalüüsi auditite eeldatava arvu, maksumuse ja kogukulu hinnanguga, vajaduse korral stsenaariumide kaupa, ning hinnata audiitorite turu suutlikkust. Analüüsida tuleb ka auditeeritavate asutuste eelarvemõju. Praegune käsitus keskendub valdavalt hüvitise taotlemise halduskoormusele ega anna piisavat ülevaadet kohustuslike auditite tegelikust rahalisest mõjust.

3. RIA vastutus järelevalve korraldamisel ja välise audiitori kasutamise piirid

Eelnõuga kujundatakse järelevalve korraldus, milles RIA määrab auditit läbimise kohustuse ja käsitusala, kuid auditit tellimise ning üldjuhul ka selle rahastamise kohustus jääb järelevalvatavale. Selline korraldus vajab selgeid piire, et RIA järelevalvevõimekuse puudujääke ei kompenseeritaks põhjendamatult järelevalvatavate rahalise ja korraldusliku koormuse suurendamisega.

Arvestame, et NIS2-direktiivi artikli 32 lõige 2 ja artikli 33 lõige 2 näevad ette nii pädeva asutuse kui ka sõltumatu organi tehtava turvaauditi ning sõltumatu organi tehtava sihipärase turvaauditi kulu kandmise üldjuhul auditeeritava poolt. Samad sätted võimaldavad igakülgsest

põhjendatud juhtudel otsustada kulude kandmise teisiti. Sellest ei tulene, et välise audiitori kaasamine ja kulude jätmine teenuseosutaja kanda oleks põhjendatud pelgalt RIA töökoormuse, personali või eelarvevahendite puudumise tõttu.

Palume eelnõus ja seletuskirjas selgelt eristada sõltumatu audiitori tehtavat sihipärast turvaauditit RIA enda tehtavast kontrollist ning täpsustada, millistel kaalutlustel valitakse RIA tehtava kontrolli asemel teenuseosutaja tellitav sõltumatu audit. Välise audiitori kaasamisel peab säilima RIA vastutus järelevalve eesmärgi ja ulatuse määratlemise, auditi tulemuste hindamise ning edasiste järelevalveotsuste tegemise eest. Auditi tellimine ei tohi muutuda RIA tavapärase järelevalvetöö üldiseks asenduseks.

Teeme ettepaneku täiendada eelnõu §-s 3 sätestatud hüvitamise aluseid juhtudega, kus välise audiitori kasutamise vajadus tuleneb eeskätt RIA enda ressursside või eripädevuse puudumisest ja auditi kulu jätmine teenuseosutaja kanda oleks ebaproportsionaalne. Sellise hüvitamise võimalus ei peaks sõltuma üksnes § 3 lõikes 3 loetletud üksuste hulka kuulumisest. Palume põhjendada ka seda, miks on kulude hüvitamiseks õigustatud üksuste ring seotud E-ITSi järgimise ja välisauditi kohustuse eranditega, kuigi sihipärane turvaaudit on eraldi järelevalvemeede.

Palume eelnõu ja seletuskirja eeltoodud märkuste alusel täiendada, et auditi määramise tingimused, teenuseosutaja rahalise vastutuse piirid ning järelevalveasutuse vastutus oleksid üheselt arusaadavad ja regulatsiooni rakendamiseks vajalik rahastus tagatud.

Lugupidamisega

(allkirjastatud digitaalselt)

Karmen Joller
sotsiaalminister

Nele Labi
nele.labi@sm.ee

Kristella Kukk
kristella.kukk@sm.ee