Tervise Arengu Instituut

Sotsiaalministeerium
info@sm.ee

Teie 28.05.2026 nr 1.2-3/1355-1

Meie 17.06.2026 nr 1-5/267-1

Arvamuse andmine määruse eelnõule

Tervise Arengu Instituut (TAI) on läbi vaadanud Sotsiaalministeeriumi poolt arvamuse avaldamiseks edastatud Justiits- ja Digiministeeriumi koostatud **määruse „Eesti Infoturbestandard“** eelnõu koos lisadega (edaspidi eelnõu).

Esitame omaltpoolt järgnevad märkused ja ettepanekud:

1) Eelnõu § 2 ja läbivalt; lisa 2 p 3.1, 6.4.2, 6.6.3–6.6.4
Eelnõu keskne mõiste on „äriprotsess“. Avalikus sektoris on aga juba aastaid rakendatud teenusepõhist juhtimis- ja eelarvestamisloogikat. Tegevuspõhise riigieelarve metoodika kohaselt on asutused kaardistanud teenused, sidunud kulud teenustega ning loonud teenuste loetelud ja teenuskaardid. Kui E-ITS nõuab lisaks „äriprotsesside“ eraldi kaardistamist ja kaitsetarbe määramist, tekib paralleelne kirjeldus- ja juhtimiskiht. See on ressursimahukas, dubleeriv ja tekitab auditis tõlgendusriski.

Ettepanek: Asendada eelnõus ja lisades „äriprotsess“ 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. Võimalik sõnastus lisa 2 p 3.1 kohta: „Auditeeritav kirjeldab üheselt ja arusaadavalt auditi käsitlusala, sealhulgas auditeeritavad teenused või protsessid, neile määratud kaitsetarbe ning nende erisused.“

2) Eelnõu § 3 lg 2 p 4 – „äriüksuse juht“
„Äriüksuse juht“ ei ole avaliku sektori asutustes üheselt mõistetav roll. Riigiasutustes, hallatavates asutustes ja KOVides 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.

Ettepanek: Asendada „äriüksuse juht“ mõistega „teenuse omanik või struktuuriüksuse juht“. Võimalik sõnastus: „teenuse omanik või struktuuriüksuse juht - korraldab tema vastutusalas oleva teenuse, ja vara kaardistuse, kaitsetarbe määramise ning vajalike meetmete rakendamise regulaarse seire.“

3) Eelnõu § 3 lg 2; § 4 lg 2; lisa 1 infoturbekataloog; lisa 2 p 3.2 ja 6.4.4
Eelnõus on infoturbe halduse süsteemi toimimiseks nimetatud üksnes neli rolli: hankejuht, infoturbejuht, kasutaja ja äriüksuse juht. Senises E-ITS rakenduskeskkonnas on kasutusel olnud oluliselt laiem rollimääratluste loetelu, sh andmekaitsespetsialist, arendaja, arhitekt, auditirühm, haldusosakond, hankeosakond, infoturbe läbivaatuse rühm, infoturbejuht, kasutaja, organisatsiooni juhtkond, personaliosakond, testija, vastavushaldur, vastutav spetsialist ja IT talitus. Eelnõust ega seletuskirjast ei selgu, kas need rollid kaotatakse, asendatakse, jäetakse juhendmaterjali tasandile või eeldatakse nende määramist organisatsiooni enda rollijaotuses. See tekitab rakendamisel ja auditis ebaselgust, sest lisa 1 meetmed eeldavad jätkuvalt sisulisi vastutajaid eri valdkondades: IT haldus, varade haldus, isikuandmete

kaitse, vastavuse haldus, personali haldus, muudatusehaldus, varundus, logimine, tarkvara testimine ja kasutuselevõtt, tarneahela infoturve ning tarkvaraarendus.

Ettepanek: Palume selgitada, kas senises E-ITS-is kasutatud rollid jäävad E-ITS rakendamisel kehtima juhendmaterjali või rakenduspraktika tasandil või on need teadlikult ISMS-i rollimudelist välja jäetud. Kui need rollid jäetakse määrusest välja, tuleks seletuskirjas või rakendusjuhises esitada vastavustabel seniste ja uute rollide vahel. Samuti tuleks selgelt märkida, et organisatsioon peab määrama rollid ja vastutajad vähemalt nende valdkondade kohta, mille meetmeid ta rakendab. Eriti vajab täpsustamist IT talituse / IT-juhi / IT-teenuse vastutaja roll, sest praktikas on see tehniliste meetmete rakendamise, IT-varade halduse, muudatuste, seire, logihalduse, varunduse ja tehniliste intsidentide lahendamise võtmeroll.

4) Eelnõu § 2; § 6; § 8; lisa 2 p 3.1, 5.5.1, 6.4.2, 6.6.4

Kaitsetarve on E-ITS-i rakendamise ja auditeerimise keskne mõiste, kuid eelnõu terminite hulgas seda ei defineerita. Samas sõltuvad kaitsetarbest meetmete valik, prioriteedid, tähtajad, tarneahela nõuded ja auditi valim. Samuti ei ole piisavalt selge, kas senised kaitsetarbe tasemed jäävad kehtima või peab organisatsioon ise skaala kehtestama. Kui mõiste ja skaala ei ole ühesed, suureneb rakendajate ja audiitorite tõlgenduserinevus.

Ettepanek: Lisada eelnõu § 2 terminite hulka „kaitsetarve“ ning täpsustada kaitsetarbe määramise skaala või miinimumnõuded skaalale. Võimalik definitsioon: „kaitsetarve - 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 skaala jäetakse organisatsiooni otsustada, peab riskihalduse metoodikas olema kohustuslikult kirjeldatud kaitsetarbe määramise skaala, kriteeriumid, otsustaja ja dokumenteerimise viis.

5) Eelnõu § 6 – riskihaldusmetoodika ja riskide aktsepteerimine

Riskihaldusmetoodika peab olema auditeeritav, korratav ja võrreldav. Praegune sõnastus ei ütle piisavalt selgelt, millised miinimumelemendid peavad metoodikas olema. Samuti on ebaselge, kes on riskiomanik, kes hindab riski ja kes võib riski aktsepteerida. See võib põhjustada olukorra, kus metoodika on küll formaalselt olemas, kuid auditis ei ole võimalik järjepidevalt hinnata riskide käsitlemise piisavust.

Ettepanek: Täpsustada riskihalduse metoodika 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.

6) Eelnõu § 10 lg 3; lisa 2 p 5.1

Eelnõu ja auditeerimiseeskiri ütlevad, et organisatsioonisisese hindamise käigus tuvastatud puudused peavad auditi alguseks olema kõrvaldatud. See on liiga absoluutne. Praktikas võib asutus olla puuduse kõrvaldamise asemel rakendanud kompenseeriva meetme, aktsepteerinud jääkriski või kinnitanud tegevuskava. Kui see ei ole lubatud, võib audit takerduda formaalse puuduse taha, kuigi risk on juhitud ja dokumenteeritud.

Ettepanek: Sõnastada nõue paindlikumalt: „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.“

7) Rollide ja vastutuse auditeeritavus; eelnõu § 3, § 4 ja § 5; lisa 2 p 6.4.4

Eelnõus on rollid nimetatud, kuid puudub selge vastutuse jaotus: 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. Ilma rollide ja vastutuste miinimumloogikata võib sama nõue olla eri asutustes ja eri auditites erinevalt tõlgendatud.

Ettepanek: Lisada seletuskirja või rakendusjuhisesse minimaalne RACI-põhine vastutusmudel. RACI tähendab vastutusmaatriksit: Responsible- teeb töö ära; Accountable - lõplikult vastutab ja kinnitab; Consulted - annab sisendi või kooskõlastab; Informed - teda teavitatakse. E-ITS-i puhul võiks miinimumnõue olla, et organisatsioonil on kaitsetarbe määramise, riskide aktsepteerimise ja infoturvameetmete rakendamise plaani täitmise kohta rollide ja vastutuste jaotus taasesitatavas vormis olemas.

Lisamärkused terminoloogia ja sõnastuse kohta

1) „Infoturbe“ ja „infoturva-“ vormide kasutus

Eelnõus ja lisades kasutatakse eri vorme: infoturbe halduse süsteem, infoturbekataloog, infoturvameetmed, infoturvasündmus, infoturvapoliitika, infoturvaoht, infoturvaintsident. Rakendaja jaoks ei ole selge, kas vormidel on tähenduserinevus või on tegemist üksnes keelelise liitsõnamoodustusega.

Ettepanek: Ühtlustada terminikasutus või lisada seletuskirja terminoloogiline märkus. Soovitatav on kasutada läbivalt ühtset põhimõistete loogikat, näiteks „infoturbe halduse süsteem“, „infoturbe meetmed“, „infoturbe sündmus“, „infoturbe poliitika“, „infoturbe kataloog“. Kui liitsõnavormid jäävad alles, tuleks selgitada, et sisulist tähenduserinevust ei ole.

2) „Organisatsiooni juhatus“

Avaliku sektori asutustes ei pruugi „juhatus“ olla korrektne mõiste. Riigiasutuses on asutuse juht, hallatavas asutuses asutuse juht, KOV-is täitevorgan või ametiasutuse juht, sihtasutuses juhatus.

Ettepanek: Asendada normitekstis „organisatsiooni juhatus“ mõistega „organisatsiooni juhtorgan või asutuse juht“.

3) „Hankejuht“

„Hankejuht“ seostub avalikus sektoris riigihanke ja ostumenetlusega. Seletuskiri küll selgitab, et hankejuhi all ei mõisteta üksnes ostujuhti või riigihanke eest vastutajat, kuid normitekstist see ei selgu.

Ettepanek: Kaaluda rollinimetust „vara või teenuse kasutuselevõtu eest vastutav isik“ või „soetuse ja kasutuselevõtu turvanõuete eest vastutav roll“.

4) „Organisatsioonisisene hindamine“

Eelnõu järgi võib hindamist teha ka organisatsioonivälise isik. Seetõttu on mõiste „organisatsioonisisene hindamine“ ebatäpne ja võib tekitada segadust, kas tegemist on sisehindamise, enesehindamise või sõltumatu eelhindamisega.

Ettepanek: Kasutada mõistet „organisatsiooni korraldatav hindamine“ või täpsustada, et hindamise korraldab organisatsioon, kuid selle võib läbi viia sõltumatu sisemine või väline hindaja.

5) „Teenuseandja“ lisa 2 tähenduses

Auditeerimiseeskirjas kasutatakse mõistet „teenuseandja“, kuid E-ITS põhitekst ja KüTS-i loogika kasutavad teenuseosutaja / organisatsiooni mõistet. Mõiste võib minna segi välise IT-teenuse osutaja, pilvteenuse tarnija või tarneahela osalisega.

Ettepanek: Kasutada läbivalt mõistet „väline teenuseosutaja“ või „tarneahela osaline“ kui mõeldakse välist IT-teenuse osutajat, pilvteenuse tarnijat või tarneahela osalist ning eristada see KüTS-i tähenduses teenuseosutajast.

6) Autentsus riskihindamise kriteeriumina

Eelnõu § 6 nimetab konfidentsiaalsust, terviklust ja käideldavust, kuid seletuskirjas on samas kontekstis lisatud ka autentsus. See võib auditis tekitada küsimuse, kas autentsus on kohustuslik hindamiskriteerium.

Ettepanek: Ühtlustada eelnõu ja seletuskiri. Kui autentsus peab olema kohustuslik hindamiskriteerium, lisada see normiteksti. Kui kohustuslikuks jäävad konfidentsiaalsus, terviklus ja käideldavus, käsitleda autentsust seletuskirjas näitliku lisakriteeriumina.

7) Lisa 1 äriprotsessi sõnastused

Lisa 1 sisaldab mitmes kohas äriprotsessi mõistet, näiteks pilvteenuse integratsioon äriprotsessiga, X-tee turvaserveriga seotud äriprotsesside usaldusväärsus ja mobiilirakendus äriprotsessi toetajana.

Ettepanek: Kui põhitekstis kasutatakse „teenus või protsess“ mõistet, tuleb sama muudatus teha ka lisas 1. Näiteks „pilvteenuse integratsioon teenuse või protsessiga“, „X-tee turvaserveriga seotud teenuste ja protsesside usaldusväärsus“, „teenust või protsessi toetav mobiilirakendus“.

Lugupidamisega

(allkirjastatud digitaalselt)

Annika Veimer
direktor

Koostajad:

Heli Jaago
heli.jaago@tai.ee

Enrico Kaljurand
enrico.kaljurand@tai.ee