RAHANDUSMINISTEERIUM

Justiits- ja Digiministeerium
info@just.ee

Teie 31.07.2025 nr 8-1/6499-1,
JDM/25-0863/-1K
Meie 20.08.2025 nr 1.1-11/3522-2

Ettevõtlus- ja infotehnoloogiaministri 16. detsembri 2022. a määruse nr 101 „Eesti infoturbestandard“ muutmise eelnõu kooskõlastamine

Austatud proua Pakosta

Saadan märkused ettevõtlus- ja infotehnoloogiaministri 16. detsembri 2022. a määruse nr 101 „Eesti infoturbestandard” muutmise eelnõu kohta.

1. Kahjuks on eelnõu kooskõlastamiseks antud tähtaeg ebamõistlikult lühike. Seega on aeg eelnõu ja seletuskirja põhjalikuks analüüsiks ebapiisav.

2. Palume täpsustada E-ITS etalonturbe kataloogi moodulit DER.3.1 „Auditid ja läbivaatused“ nii, et see oleks sõnastatud kooskõlas lisa 1 „Nõuded infoturbe halduse süsteemile“ punktiga 10.2.3 ja annaks üheselt mõista, et sõltumatu läbivaatuse elluviijaks võib olla siseaudiitor, siseaudiitori rollitäitja (näiteks välisaudiitor) või käsitlusala suhtes asjakohase pädevusega sõltumatu töötaja, vältides kontrollija ja rakendaja rollide huvikonflikti.
Selgituseks lisame, et „Nõuded infoturbe halduse süsteemile“ punkt 10.2.3 sätestab selgelt, et sõltumatu läbivaatuse elluviijaks on infoturvapoliitika kohaselt kas siseaudiitor, siseaudiitori rollitäitja või käsitlusala suhtes asjakohase pädevusega sõltumatu töötaja. DER.3.1 mooduli praegune sõnastus ei väljenda seda võimalust sama selgelt, mistõttu võib jääda mulje, et sõltumatu läbivaatuse peab alati läbi viima siseaudit (vt ka mõisteid nt auditirühm). Tegelikkuses peaks organisatsioon saama valida, kas kasutada siseauditit või muud sõltumatut läbivaatust, lähtudes riskijuhtimise korraldusest või muudest asutuse sisemistest nõuetest, kordadest.

Väikeste asutuste korral on teenuse sisse ostmine kui ka asutusest sõltumatute isikute leidmine raskendatud – ei pruugi olla inim- ega finantsressurssi. Samuti eeldab ka siseaudiitorilt sellise töö tegemine teistsuguseid kompetentse, mis eeldavad eelnevate koolituste läbimist või väga häid teadmisi ITst ehk taaskord tekib küsimus, kas asutustel on olemas selliste teadmistega siseaudiitorid ning kas neid on piisavalt.

3. Punkti 10.2.5 puhul on praktika näidanud, et tulemuste sisseviimine organisatsiooni protsessidesse eeldab finantsressursse, mida avalikul sektori asutusel ei pruugi olla.

4. Lisa 2 „Etalonturbe kataloog“ tabelis CON Kontseptsioonid ja metoodikad on välja toodud, et CON.10: Veebirakenduste arendus on muudetud meetmeid sh ka CON.10.M4, kuid meetme sisu on tühi. Kas tegu võib olla eksitusega ja muudatusega tegelikult sooviti meede kustutada?

Etalonturbe kataloogis võiks liigendada meetmed selgemalt administratiivseteks ja tehnilisteks meetmeteks. Praeguses etalonturbe kataloogi ülesehituses on administratiivsed ja tehnilised meetmed esitatud läbisegi, mis võib raskendada meetmete tüübi ja vastutuse jaotuse kiiret tuvastamist ja rakendamist eri asutuste poolt (näiteks IT-maja ja asutus). Näitena võib välja tuua näiteks OPS.1.1.5 kategoorias on samas plokis nii administratiivseid meetmeid (OPS.1.1.5.M1- Logimise eeskiri, OPS.1.1.5.M5- Õiguslike raamtingimuste täitmine) kui ka tehnilisi meetmeid (OPS.1.1.5.M3- Turvasündmuste logimine, OPS.1.1.5.M6- Keskse logitaristu rajamine, OPS.1.1.5.M13- Kõrgkäideldav logimissüsteem).

5. Palume JD ja RIA-l OPS.2.3 väljast tellimise meetme nõuded üle vaadata suurte teenusepakkujate kontekstis (nt riigi IT-majad, Cloudflare, Amazon), arvestades, et selliste teenuste puhul ei ole asutustel sageli võimalik ilma märkimisväärsete lisakuludeta kõiki turbenõudeid detailselt kehtestada ja seirata. Sellisel juhul võiks tugineda keskselt kokkulepitud teenuste standarditele (nt RIT ATK standard) ja sõltumatule auditile (nt E-ITS või ISO/IEC 27001) kui vastavuse tõendile.

6. Muudatustel on rahaline mõju ehk ei saa öelda, et igasugune mõju puudub, kuna see annab vale indikatsiooni otsustajatele (nt ka RES protsessi vaates).

Lugupidamisega

(allkirjastatud digitaalselt)

Jürgen Ligi
rahandusminister

Virge Aasa 5885 1493
Virge.Aasa@fin.ee

Kristi Müürsepp 5885 1397
Kristi.muursepp@fin.ee