SOTSIAALMINISTEERIUM

Justiits- ja Digiministeerium
info@justdigi.ee

Teie 31.07.2025 nr 8-1/6499-1, JDM/25-0863/-1K/
Meie 14.08.2025 nr 1.2-3/2005-2

Vastus Eesti infoturbestandardi muutmisele

Täname, et esitasite võrgu- ja infosüsteemide küberturvalisuse nõuete määruse kooskõlastamiseks. Oleme muudatused läbi vaadanud ning kooskõlastame selle järgnevate märkuste ja ettepanekutega.

1. Üldine ettepanek versioonihaldusele

E-ITSi juhendmaterjal on väga mahukas dokumentatsioon, mille rakendamine nõuab asutustelt süsteemset tööd. Seetõttu on oluline, et muudatuste rakendamisel oleks tagatud ka selgus ja jälgitavus.

Esitatud käskkirjas ei ole **selgelt esile toodud**, et tegemist on **2024. aasta versiooni kinnitamisega**, mis tekitab segadust - kas see asendab varasemat versiooni või täiendab seda. See raskendab omakorda muudatuste sisu mõistmist ja vajalike kohanduste tegemist asutuse sisemistes protsessides.

Ettepanek on, et tuleviku versiooni juurde on lisatud **selge viide versiooni numbrile ja kehtestamise ajale**, **kokkuvõte olulistest muudatustest** või võrdlus varasema versiooniga tabelina ning vajadusel ka **sissejuhatus või rakendusjuhis**, mis aitab asutustel muudatuste sisust ja mõjust paremini aru saada.

2. E-ITS-i juhendite omavaheline vastuolu

E-ITS-i juhendite omavaheline kooskõla vajab täpsustamist, et vähendada tõlgendusruumi ja suurendada rakendamise selgust (etalonturbe kataloog, nõuded ISMS-ile ja auditeerimiseeskiri). Eksisteerib E-ITS-i kohustuslike dokumentide (etalonturbe kataloog, nõuded ISMS-ile ja auditeerimiseeskiri) ja soovituslike juhendite (rakendusjuhend, riskihaldusjuhend) sisuline vastuolu. Lisaks esineb ka vastuolu kohustuslike dokumentide osas.

Näiteks on auditeerimiseeskirja järgi kohustus läbida siseaudit **või** sõltumatu läbivaatus, sama viitavad DER.3.1 meetmed ka sisemise auditi protsessile. Sealhulgas eeldavad välisaudiitorid, et siseaudit on läbi viidud 3. kaitseliinina, millele nad saavad vastavusaudiitoritena tugineda. See loob olukorra, kus juhendite vahelised erinevused jätavad audiitorile laia tõlgendamisruumi ja võivad viia samade olukordade erineva hindamiseni (nt mittevastavus vs tähelepanek), sõltuvalt sellest, kummale juhendile rohkem tuginetakse.

Lisaks tuleb kriitiliselt hinnata siseauditi nõude adekvaatsust väiksemate või piiratud ressurssidega asutuste kontekstis. Infoturbe hindamine eeldab spetsiifilist pädevust ning

sõltumatust. Paljudes asutustes ei ole inimest, kes oleks ühtaegu nii sõltumatu kui ka piisava kompetentsiga, et viia läbi kvaliteetne siseaudit ISMS-i osas.

3. E-ITS-i käsitlus konsolideeritud teenuste puhul

E-ITS-i juhendites puudub hetkel selge raamistik või tõlgendusruum olukordadele, kus infoturbe teenuseid pakub konsolideeritud üksus, mis ei ole otseselt asutuse sees ega ka klassikalises mõttes „väljast tellitav teenusepakkuja“.

Näiteks Rahandusministeeriumi ühisosakond pakub mitmele ministeeriumile konsolideeritud teenuseid (dokumendihalduse teenus, üldine ühisministeeriumi hoone haldus jt). E-ITS-i mõistes ei ole tegemist asutusesisese funktsiooni täitmisega ega ka standardse välise teenuse tellimisega (nagu seda käsitleb E-ITS meede OPS 2.3). See on hübriidne partnerlus, kus vastutuse ja kontrolli jagunemine ei ole tavapärane - ühisosakond on formaalselt väljaspool ministeeriumi struktuuri, kuid funktsionaalselt selle osa. Sellise mudeli puhul tekib küsimus, kes on infoturbe eest vastutav isik ja kuidas rakenduvad kontrollmeetmed?

Ettepanek on töötada E-ITS-i juhendis välja täiendav käsitlus (või suunised), mis arvestab konsolideeritud teenuste eripära.

4. Tehniliste infoturbenõuete määramine välistele teenustele

Nii praktika kui E-ITS-i meetmetes toodud juhised eeldavad, et teenuse tellija määrab teenusele tehnilised infoturbenõuded (st asutus, kes kasutab teenust). See lähenemine on põhjendatud olukorras, kus teenust kujundatakse organisatsioonipõhiselt. Samas ei pruugi see alati olla realistlik ega otstarbekas – eriti juhul, kui tellitakse standardiseeritud või kesksetest platvormidest pakutavat teenust (nt riiklikud pilveteenused, IT majutusteenused, SAP, RTIP jms). Selliste teenuste puhul asub tehniline kompetents valdavalt teenusepakkuja juures. Teenuse tellija võimalused tehnilise sisendi kujundamiseks on piiratud.

Kui riigi tasandil on sõlmitud kokkulepe, et kõigile osapooltele pakutakse ühtset, standardiseeritud teenust, ei ole mõistlik ega teostatav esitada sellele „oma tellimusena“ täiendavaid või eristuvaid infoturbenõudeid. Näiteks ei saa ükski asutus mõistlikult eeldada, et tema kasutuses olev RTIP versioon oleks teistest „turvalisem“. **Teenuse tellija roll** peaks keskenduma sellele, et infoturbe nõuded oleksid lepinguliselt ja sisuliselt kaetud, teenusepakkuja infoturbe praktika oleks läbipaistev ja kontrollitav ning vajadusel oleks olemas infoturbealane koostöömehhanism ja kokkulepitud seire.

Ettepanek, et standardteenuste puhul oleks tehniliste infoturbenõuete määramine ja täitmine teenusepakkuja roll.

5. Kordame juba varem tehtud ettepanekut muuta E-ITS-i auditeerimine vabatahtlikuks

Kõik senised kogemused näitavad, et **auditeerimise protsessi kulu ja sellesse pandav töömaht ei vasta sellest protsessist saadavale kasule,** mistõttu oleks mõistlik see ressurss suunata reaalsete meetmete rakendamisele, kus sellel on mõju. Neile asutustele, kes vajavad muudel põhjustel (mitte küberturvalisuse seadusest tulenevalt) sõltumatut hindamist E-ITS-i meetmete rakendamisele, tasub võimalus alles jätta, ent vabatahtlikuna. See tähendab, et kui teatud juhtudel on see küberturvalisuse seadusest tulenevate nõuete osas vajalik, siis jääb see ka edaspidi võimaliku variandina alles (näiteks alternatiivina rakendatav ISO27001, mille üks kohustuslik osa on ka välise audiitori poolne auditeerimine, et saada sertifikaat).

Ettepaneku mõte on kaotada liigne bürokraatia ja mõju mitteomavad kulutused (audit on kulukas, ent ei loo iseenesest lisaväärtust!) osapooltele, kellele see ei ole vältimatult muudel asjaoludel vajalik. Auditit ei asendata muu välise osapoole hindamisega, vastutus meetmete

rakendamise eest lasub nii auditiga kui auditita niikuinii ettevõttel/asutusel, kes peab E-ITS-i rakendama.

6. Tippjuhtkondade toetamine keskse selge materjali ja tööriistadega ning juhtumisteemade eristamine tehnilistest

E-ITS-i rakendamisel on praegu puudu tippjuhtkonnale suunatud lihtne ja ülevaatlik materjal või tööriist, mis **toetaks infoturbe juhtimist strateegilisel tasandil**. Kui muudatuse eesmärk oli kaasata infoturbesse laiem ring töötajaid, siis seda ei ole võimalik saavutata sellise mastaabi ning keerukuse tasemega – kui ISKE puhul oli tegemist ainult näitlikult IT-juhi vastutusvaldkonnaga, siis E-ITS on selle laiendanud. Kuid strateegiliselt või ülevaatlikult teemaga tegelemiseks puuduvad tööriistad ja üldistustase, mis iga asutus loob neid ise kulutades aega ja ressurssi.

Soovitame kaaluda **E-ITS-ist puhtalt juhtimisalaste teemade eristamist, mis ei ole otseselt seotud infoturbe tehnilise korralduse või küberturbe meetmetega**. Praegusel kujul sisaldavad mitmed meetmed nii juhtkonna kui ka tehnilise üksuse ülesandeid läbisegi, mistõttu võib tekkida segadus vastutuste ja rollide jaotuses – eriti juhul, kui meetme juures toodud vastutaja ei ole sisuliselt seotud kogu meetme ulatusega. Lisaks on oluline arvestada, et IT-audiitoritel ei pruugi olla pädevust hinnata strateegilisi juhtimisotsuseid või juhtkonna töökorraldust puudutavaid teemasid. Selliste elementide kontrollimine eeldaks teistsugust metoodikat ja erialast tausta. Ettepanek on selguse ja asjakohasuse tagamiseks juhtimissüsteeme puudutavad teemad minimeerida ning alles jäävad selgelt eraldada tehnilistest.

7. Tähelepanekud isikuandmete kaitse osas

Täiendatud juhistes palume kaaluda esitatud ohtude loetelu selliselt, kus need sisuliselt ei kattuks (lisa 2). Segadust tekitavad omavahel kattuvad ohud, millel sisulist erinevust ei näi olevat. Näiteks esitatakse ohtudena eraldi nii „puudulik privaatsus“ kui „isikuandmete konfidentsiaalsuse kadu“ (2.4 ja 2.5), samas kui tekib konfidentsiaalsuse kadu, siis tekib andmete kolmanda isiku kätte sattumisega ka eraelu riive. Ohtude loetelu võiks olla näidetena laiapindsem ning ka järelmid ei seostu ainiti eraelu riivega (vt AKI juhist). Ohtudeks võib olla ressursi- või juhiste puudus, kübernõuete rikkumine vms, millega võib kaasneda olenevalt süsteemist või andmetest nii oht elule, oht eraelu riiveks aga ka maine kahju vms.

Lugupidamisega

(allkirjastatud digitaalselt)
Karmen Joller
sotsiaalminister

Anni Heinaste
Anni.Heinaste@sm.ee

Ene Kröönstöm
Ene.Kroonstrom@sm.ee

Nele Nisu
Nele.Nisu@sm.ee