IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes

Kas omavalitsuste kätte usaldatud andmete turvalisus on nõuetele kohaselt tagatud?

Riigikontrolli aruanne Riigikogule
Tallinn, 5. juuni 2018

Head lugejad

Kohalike omavalitsuste infoturbes valitseb üüratu korralagedus. Alustades elementaarsest teadmisest, mida ja miks peab turvama, kuni selleni, keda omavalitsustes infoturbega seotud tegevus või tegevusetus üldse huvitab. Kohati jäi Riigikontrolli audiitoritele auditit tehes mulje, et mitmetes kohalikes omavalitsustes on justkui Metsik Lääs, kuhu kuuldused Eestis kehtivatest nõuetest infosüsteemide pidamisel pole jõudnud. Omavalitsus teeb ühes X-tee otsas, mida iganes tahab, ilma et see kuigivõrd kellelegi korda läheks, ning teises X-tee otsas on kohusetundlikult (kes rohkem, kes vähem) turvameetmete süsteemi rakendav riigiasutus, kes ka muu hulgas vastutab andmete eest, mis omavalitsusele täiesti kontrollimata kasutada antakse. Turvalisest andmevahetusest X-teel ei saa sellisel juhul rääkida. Keelata omavalitsusele andmetele ligipääsu aga ka ei saa, sest neid on tal vaja oma avalike ülesannete täitmiseks. Kuna omavalitsuste ja riigi andmekogude vaheline andmete vahetus on paratamatus ning Eesti peab Euroopa Liidu liikmena järgima *once-only*-printsiipi kodanikelt ja ettevõtjatelt andmete kogumisel, tähendab see, et omavalitsustes tähelepanuta jäetud nõrkused kanduvad edasi ja võivad teha kahju laiemalt.

Kui Riigikontroll n-ö kaablite sasipundart lahti hakkas arutama, selgus, et esiteks puudub korralik ülevaade omavalitsustes peetavatest andmekogudest (seda nentis Riigikontroll ka juba 2017. aastal avaldatud ülevaates). Teiseks ei vasta need andmekogud, mille eksisteerimise kohta on teave olemas, seatud nõuetele. Näiteks selgus, et omavalitsuste andmekogud ei läbi nende pidamise õigust andvat kooskõlastamise protsessi ja seda ka siis, kui need kooskõlastamiseks esitatakse. Omavalitsuste aktiivsus kasutada X-teed mujal juba kogutavate andmete kättesaamiseks on kasin. Seega koormatakse kodanikke ja ettevõtjaid mitmekordselt andmepäringutega või teine variant – kasutatakse andmevahetusviise, mis ei pruugi olla niisama turvalised kui X-tee.

Kolmandaks, ja see on ka kõige murettekitavam, kohtasid audiitorid kohalikes omavalitsustes vastutavaid ametnikke, kelle jaoks turvameetmete süsteemi rakendamise, sh andmekaitse vajalikkus jäi niisama arusaamatuks kui investeerida turismireisi Marsile – see on midagi kauget, mis nende eluaja jooksul nagunii ei juhtu. Ajal, kus teadaolevate küberturbejuhtumite arv Eestis on juba üle 10 000 aastas, on naiivne ja ohtlik endiselt arvata, et „meiega seda ju ei juhtu“ või „meie andmed ei ole olulised“.

Riigikontrollile sai auditi käigus teatavaks mitmeid juhtumeid, kus just omavalitsuste infosüsteemidesse on tehtud teenustõkestusründeid, nakatatud süsteeme pahavaraga ja kahjustatud veebilehti.

Andmete turve peab olema iseenesest mõistetav kõikidele teenistujatele, mitte ainult IT-spetsialistile ja tööprotsessidesse lõimitud nii, et oleks tagatud andmete turvalisuse vajalik tase, mis vastaks ohtudele ja

kaitstavate andmete laadile. Auditi toimingute ajal ei olnud andmete turvaanalüüsi teinud ükski auditeeritud omavalitsus, keegi ei pidanud selle läbiviimist ka otseselt enda ülesandeks ning IT-vahendite kasutamise suunised kas puudusid üldse või ei olnud nende olemasolust teenistujaid teavitatud. Probleeme ilmnes ka turvameetmete rakendamisega, näiteks seoses paroolipoliitika, andmevarunduse, turvauuenduste ja pääsuõigustega. Hea on siiski tõdeda, et oma vastustes käesoleva auditi aruandele on auditeeritud omavalitsused oma suhtumist andmete turvalisuse tagamise kohustuse täitmisesse märgatavalt parandanud.

IT turvalisus on ennekõike omavalitsusasutuste juhtide pärusmaa. Iga asutuse juhtkonna ülesanne ja vastutus on tagada andmete turvaline töötlemine. Juhtkond on ka infoturbekultuuri kujundaja. Seetõttu on eriti oluline just juhtkonna initsiatiiv nii enda kui ka oma asutuse teenistujate teadlikkuse parandamisel ja loodud suuniste täitmisel. See kannustab ka töötajaid nõudeid järgima ja andmetega hoolikamalt ringi käima. Usutavasti ei ole ametnikke, kes pahatahtlikult rikuvad turvanõudeid. On aga juhtumeid, kus ametnik, kes toimetades oma teadlikkuse piirides, väärkasutab, näiteks avaldab, hävitab või teeb IT-süsteemis juurdepääsetavaks enda kätte usaldatud andmeid. Ka levinud lunavararünnete puhul aitaks ennekõike see, kui teenistujad oleks koolitatud ja teadlikud sellest, et iga kahtlast e-kirja manust või linki ei tohi niisama „igaks juhuks“ avada. Tänapäeval on paljud ründed üles ehitatud lootuses, et leitakse küberohtudest vähem teadlik töötaja, kes heauskselt vajutaks linki, avaks manuse või teeks ülekande, edastaks andmeid täiesti võhivõõrale ja autentimata isikule.

Kuna turvalisus sõltub suuresti inimesest, kes istub arvuti taga ja kelle tegemist on võimalik suunata erinevate ettekirjutiste, koolituste ja teavitustega, ei saa ka väita, et turvameetmete süsteemne rakendamine on liiga kallis ja seda raha on omavalitsusel mõistlikum põhitegevusse investeerida. Ajad, kus andmete turvalisus tähendas ainult konfidentsiaalsust, on möödas. Avaliku sektori edukaks toimimiseks ja üleüldse oma põhiülesannete täitmiseks on vaja tagada ka andmete kättesaadavus ja õigsus.

Kuigi erinevatele nõuetele vastavust peaksid kontrollima vähemalt kaks järelevalvega tegelevat riigiasutust, ei hinnata omavalitsustes töödeldavaid andmeid või nende mahtu piisavalt oluliseks, et jõulisemat kontrolli teha. Oma vastustes Riigikontrollile avaldati korduvalt seisukohta, et võrreldes teiste järelevalvatavatega on omavalitsuste andmetöötlus vähem tähtis ning ressurss suunatakse sinna, kus andmeid on rohkem. Samas aga töötlevad omavalitsuste ametnikud mitmesuguseid andmeid – lemmikloomade vaktsineerimisest kuni inimese surmani välja. Inimesele on oluline, et temaga seotud andmete turvalisus ei oleks tagatud mitte ainult riigi andmekogudes, vaid ka omavalitsuses. Audit ei näidanud, et riik oleks saavutanud märkimisväärset mõju ainuüksi teavitustegevusest ja toetuste jagamisest omavalitsustele: kõik kolm hooba – järelevalve, teavitus ja toetused – peaksid üksteist täiendama. Loomulikult peabki alguses teavitama, aga kui olukord sellele vaatamata ei parane, siis on järelevalveasutusel kohustus ka sunnimeetmeid kasutada.

Omavalitsustes on turvameetmete süsteemi auditeerimine jäänud aga toppama, kuna kaks ministeeriumi – majandus- ja kommunikatsiooniministeerium ning rahandusministeerium – ei suuda kokku leppida, kelle rahakotist omavalitsuste infosüsteemide auditeerimise peaks kinni maksma: kas seda peab tegema ministeerium, kes vastutab infoühiskonna arengu eest, või ministeerium, kelle vastutusalasse kuulub regionaalhaldus. Riigikontroll soovitab tungivalt see ära otsustada, enne kui järgmine 10 aastat kontrollimatut infoturbetegevust omavalitsustes mööda läheb. Siinkohal on aga oluline nüanss: olemuslikult on turvaaudit siiski osa asutuse sisekontrollist. Seega peaksid ka omavalitsused ise tundma rohkem huvi infosüsteemide auditeerimise vastu ning pole välistatud, et tulevikus infosüsteemide turbeauditeid ka ehk tellima asuma.

Korralagedus on piisavalt suur selleks, et otsida tõhusaid koostöövorme kohalike omavalitsuste enda ning ka omavalitsuste ja keskvalitsuse vahel. Esimesel juhul maksab omavalitsustel tõsiselt kaaluda ühiste IT-keskuste loomist, mis pakuks teenuseid kõigile keskuse asutanud omavalitsustele. See aitaks koondada parimat teadmist ning olla ka konkurentsivõimeline IT-spetsialistide palgaturul. Teisel juhul peaks keskvalitsus võtma suurema rolli omavalitsuste toetamisel – erinevate nõuete kehtestamisel tuleks pakkuda kohalikele omavalitsustele ka standardlahendusi nende nõuete täitmise tagamiseks.

Janar Holm
riigikontrolör

juunis 2018

IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes

Kas omavalitsuste kätte usaldatud andmete turvalisus on nõuetele kohaselt tagatud?

Kokkuvõte auditeerimise tulemustest

Mida me auditeerisime?

Riigikontroll auditeeris, kas omavalitsustele usaldatud andmed on turvaliselt hoitud. Selleks vaadati tegevusi nii omavalitsuse kui ka riigi tasemel. 10 vallas ja linnas hinnati IT-turbe planeerimist ja seatud nõuete täitmist (nt andmevarundust, paroolide kasutamist, IT-kasutajate õiguste jagamist, turvauuenduste tegemist, viirusetõrjet).

Auditeeritud KOVid	
Kuusalu vald	Võru vald
Rapla vald	Audru vald
Viljandi vald	Kohtla-Järve linn
Paide linn	Avinurme vald
Valga linn	Vihula vald

Nelja riikliku andmekogu puhul analüüsiti, mida on teinud andmekogu pidaja, et tagada omavalitsuse osavõtul toimuva andmevahetuse turvalisus. Need andmekogud olid Siseministeeriumi rahvastikuregister, Justiitsministeeriumi e-toimik, Haridus- ja Teadusministeeriumi (HTM) Eesti hariduse infosüsteem (EHIS) ning Maa-ameti aadressiandmete süsteem (ADS). Lisaks analüüsiti Riigi Infosüsteemi Ameti (RIA), Andmekaitse Inspektsiooni (AKI) ning Majandus- ja Kommunikatsiooniministeeriumi (MKM) tegevust, kelle vastutada on toimiv järelevalve IT-turbe küsimustes. Lisaks vaadati ka omavalitsustele pakutavaid teavitustegevusi ning toetusi.

Miks on see maksumaksjatele oluline?

Avaliku sektori edukas toimimine rajaneb järjest enam infotehnoloogial ja andmetel, mida riigi ja kohaliku omavalitsuse asutused koguvad. Võimaluse kõrval arendada välja paremaid, mugavamaid ja soodsamaid avalikke teenuseid kasvab andmete hulgaga samas suunas ka oht, et andmed satuvad valedesse kätesse, hävinevad, saavad kahjustada jne. Ka omavalitsused ei ole selle vastu immuunsed.

X-tee – infosüsteemide turvaline andmevahetuskiht, mida peab kasutama andmeid vahetades avalikus sektoris (andmekogude vahel) ja ka väliste süsteemidega (nt ettevõtjate infosüsteemidega).

On näiteid, kus omavalitsuste infosüsteemidesse on tehtud teenustõkestusründeid, nakatatud süsteeme pahavaraga ja kahjustatud veebilehti. Erinevate rünnete tagajärjed võivad küündida mainekahjust kuni asutuse vastu esitatud kohtuasjadeni või viia ebamõistlike juhtimisotsusteni. Omavalitsuste ja riigi andmekogud vahetavad üksteisega X-tee kaudu andmeid, mis tähendab, et omavalitsustes tähelepanuta jäetud nõrkused kanduvad edasi ja võivad teha kahju laiemalt.

Mida me auditi tulemusel leidsime ja järeldasime?

Auditeeritud omavalitsuste kätte usaldatud andmete turvalisus ei ole nõuetekohaselt tagatud. IT-turve on paljude omavalitsuste jaoks küsimus, millega seotud riske endiselt ei teadvustata, mistõttu ei täideta valdavalt ka riigi seatud nõudeid, ehkki need on praeguseks kehtinud pea 10 aastat. Riigipoolne järelevalve on vähene ega sunni

omavalitsusi pingutama. Loodetud arengut ei ole kaasa toonud ka riigi teavitustegevus ega rahaline toetus.

Riigikontrolli olulisemad tähelepanekud auditeeritud omavalitsuste kohta:

- Omavalitsuste üldine infoturbekultuur on madal nii teenistujate kui ka juhtkonna tasandil; mitte ühelgi auditeeritul ei olnud ajakohast infoturbe kontseptsiooni; neljas omavalitsuses ei olnud määratud IT-turbe eest vastutavaid töötajad. IT-vahendite kasutamise suunised kas puuduvad üldse või ei ole nende olemasolust teenistujaid teavitatud; IT-nõuete täitmist toetavaid koolitusi ega muud teavitustööd ei olnud teinud ükski auditeeritud omavalitsus.
- Infoturbe planeerimise ja rakendamise seis omavalitsustes on kehv. Tõhusa infoturbe lähtekoht on turvaanalüüs, mille alusel määratakse kogutavatele andmetele turvaklassid, millest omakorda sõltub rakendatavate meetmete valik. Turvaanalüüs oli tegemata ja turvaklassid kehtestamata kõigil 10-l auditeeritud omavalitsusel. Puudujääke ilmnes ka näiteks seoses paroolipoliitika, andmevarunduse, turvauuenduste ja pääsuõigustega.
- Omavalitsuse kogutavatest andmetest puudub terviklik ülevaade. Suur osa andmekogudest on RIHAs registreerimata ja need, mis on registreeritud, ei ole enamasti läbinud andmekoosseisu kontrolli. X-tee liidestusi omavalitsuste andmekogudega on vähe ja andmeid kogutakse mitmel pool topelt.
- Auditeeritud omavalitsused ei pea ennast vastutavaks mujal majutatud andmekogude andmete turvalisuse, andmekogude RIHAs registreerimise ja X-teega liidestamise eest, kuid ei nõua seda ka teenuse osutajalt.

RIHA on riigi infosüsteemi halduse infosüsteem, kus kontrollitakse, kas vajalikke andmeid kogutakse juba mõne asutatud andmekogu koosseisus või mitte. Kui kogutakse, saab RIHA kaudu esitada uue andmekogu asutaja selle andmekogu vastutavale töötlejale taotluse andmete kättesaadavaks tegemiseks riigi infosüsteemis, s.t ühtlasi X-teega liidestumise protsessi algatust.

Allikas: Vabariigi Valitsuse määrus „Riigi infosüsteemi haldussüsteem“, § 6 lg 4

Riigikontrolli olulisemad tähelepanekud riigi tegevuse kohta:

- Võttes arvesse auditis omavalitsuste infoturbe olukorra kohta tehtud tähelepanekuid, ei saa senist järelevalve korraldust pidada piisavaks. Näiteks võiks RIHA andmestik omavalitsuste andmekogude kohta olla märksa korrastatum ning liidestusi X-teel rohkem, kui Andmekaitse Inspektsioon registreerimist ja andmekoosseise kontrolliks. Teadaolevalt ei ole järelevalve eest vastutavad asutused teinud omavalitsustes ühtegi ettekirjutust ISKE kehva rakendamise või selle auditeerimiskohustuse eiramise kohta. Lisaks puudub ka ISKE rakendamise auditi tellimise eest vastutaval ministeeriumil tahe omavalitsustele auditeid tellida.
- Seni kuni omavalitsustes ISKE-auditeid tellitud ei ole, ei saa andmekogude pidajad tugineda sertifitseeritud audiitori hinnangule turbevajadusele vastavuse kohta. Riigiregistrite pidajad peavad seetõttu läbi viima eraldi kontrolle omavalitsuste osavõtul toimuva andmevahetuse turvalisuse üle. Seesuguseid kontrolle ei ole aga ükski auditeeritud riigiregistri pidaja teinud.
- Infoturbetaset omavalitsustes on seni püütud tasemel hoida n-ö kampaaniapõhiselt ja sõltuvalt välisrahastusest. Riik on küll teinud omavalitsuste suunas mitmeid teavitusi (sh koolitused, ringkirjad,

ISKE – riigi ja KOVide andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteemide kolmeastmeline etalonturbe süsteem. ISKEs on kirjeldatud kolm turbetaset: madal (L), keskmine (M) ja kõrge (H). Vastav turbetase määratakse andmetele turvaklasside (turvaosaklasside) määramise kaudu.

Allikas. ISKE rakendusjuhend 8.0

juhendid jms) ja jaganud sihtotstarbelisi toetusi, kuid nendel tegevustel ei ole olnud oodatud pikemaajalist püsivat mõju.

- Audit ei näidanud, et ISKE oleks omavalitsustele sobimatu, ent selle rakendamisel peaks võimaldama suuremat paindlikkust, võttes arvesse omavalitsuste andmekogude pidamise eripärasid. Näiteks kasutavad omavalitsused andmekogude pidamisel sageli standardlahendusi (84% RIHAs registreeritud andmekogudest), mille turvalisuse küsimused võiks teatud ulatuses lahendada ühetaoliselt ja ühekordselt (nt turvaklasside määramine, registreeringud RIHAs ja andmekoosseisu kontrollid, auditeerimine).

Mida me auditi tulemusel soovitasime?

Riigikontrolli soovitas auditeeritud omavalitsustel määrata infoturbe juhi ülesannete täitja või tellida infoturbe juhtimine teenusena sisse; seada andmekogude pidamiseks kasutatavatele standardsetele tarkvaralahendustele nõuded sisestatavate andmete turbevajadusest lähtudes; veenduda, et lahendus oleks vajaduse korral liidestatav X-teega; ning leppida lepingus teenuse osutajaga kokku turvameetmete auditeerimise korraldus.

Auditeeritud omavalitsused on oma vastustes auditiaruandele üldjoontes läbivalt arvamusel, et Riigikontrolli soovitused on rakendatavad, ning mitmel pool on ka olukorra parandamiseks juba samme astutud. Auditi valmimise jooksul on infoturbe juhi ülesannete täitja määramisega tegelenud vähemalt Võru, Rapla, Mustvee, Valga ja Haljala vald ning Pärnu linn.

Riigikontroll soovitas ettevõtlus- ja infotehnoloogiaministril läbi mõelda omavalitsustele omasest andmekogude pidamise praktikast lähtudes nii RIHA, X-tee kui ka turvameetmete süsteemi õigusnõuete täitmise suunised. Lisaks peab analüüsima põhjuseid, miks turvameetmete süsteemi rakendamine omavalitsustes on pikalt viibinud, ning sellest tulenevalt töötama välja tegevused, kuidas muuta ISKE rakendamine omavalitsustes paindlikumaks. Riigikontroll soovitas muuta ISKE-auditi tellimise korda nii, et neid hakataks järjepidevalt tellima. Infoturbe toetamiseks mõeldud meetmete puhul tuleb võtta arvesse, et need motiveeriks omavalitsusi kasutusele võtma lahendusi, mille riik või mõni teine omavalitsus on juba maksumaksja raha eest loonud.

Ettevõtlus- ja infotehnoloogiaminister nõustus soovitustega ja märkis oma vastuskirjas, et sarnaste või ühetaoliste andmekogude pidamisele peab ta õigeks turvaklasside määramisel lähtuda ühtsetest alustest ja protseduure mitte dubleerida. Lisaks nõustus MKM, et senine korraldus KOVide ISKE-auditite tellimiseks on ebaõnnestunud. Riigikontrolli soovitusi on kavas käsitleda RIHA protsessi uuendamisel ning ISKE rakendamise ja auditeerimise kohta tehtud tähelepanekuid koos küberturvalisuse seadusest tingitud muudatustega. X-teega liidestumise tingimused täpsustatakse Vabariigi Valitsuse määruse nr 105 „Infosüsteemide andmevahetuskiht“ ajakohastamise käigus. Toetusmeetmete tingimuste koostamisel ja ülevaatamisel lähtub MKM juba praegu põhimõttest, mille kohaselt eelistatakse IT-lahenduste ühiskasutust ja -arendust.

Riigikontrolli soovitas mõlemal järelevalveasutusel (s.o RIA ja AKI) oma pädevusest lähtudes tõhustada omavalitsustes kontrolli ISKE rakendamise, X-teega liitumise ning RIHAs registreerimise üle. RIA-l

soovitas Riigikontroll IT-spetsialistidele mõeldud koolituste kõrval propageerida rohkem omavalitsuste juhtkonnale suunatud koolitusi ja teha laiemat teavitustööd.

Andmekaitse Inspektsiooni peadirektor nõustus üldjuhul auditi soovitusega ning lubas sellega edaspidises töös võimaluse korral arvestada. Direktor tõi välja asjaolu, et soovituse täitmist lähiaastatel raskendab niigi paljudele järelevalve subjektidele lisaks mais jõustunud isikuandmete kaitse üldmääruse ning sellega koos ka uue isikuandmete kaitse seaduse tõttu suurenev töökoormus. Lisaks nimetas direktor takistusena asjaolu, et asutusesisese teabe kaitseks rakendatavate turvameetmete loetelu ei ole kehtestatud.

Riigi Infosüsteemi Ameti peadirektor nõustus tehtud soovitustega ning teatas, et tehtud soovitused on auditi valmimise ajaks juba täitmisel. Plaanis on haldusreformi järel kohalikke omavalitsusi kontrollida. Tippjuhtidele suunatud koolitustega on alustatud 2017. aastal ning 2018. aastal on plaanis korraldada infoturbeteadlikkuse suurendamise koolitusi ka kohalikele omavalitsustele ja nende juhtkondadele. RIA tõi lisaks välja, et kuna asutuste tippjuhtide motiveeritus infoturbega tegeleda ja koolitustel osaleda võiks olla parem, võiks Riigikontrolli soovitus olla pigem suunatud omavalitsuste juhtidele.

Sisukord

Valdkonna ülevaade 9

Omavalitsuste tegevus andmete turvalisuse tagamisel 12

Omavalitsused ei teadvusta andmete töötlemisel oma vastutuse ulatust ega kaasnevaid nõudeid 12
Infoturbe planeerimise ja rakendamine seis omavalitsustes on kehv 15
Omavalitsuste infoturbekultuur on madal nii teenistujate kui ka juhtkonna tasandil 19

Riigi tegevus andmete turvalisuse tagamisel 23

Omavalitsuste ja riigi andmekogude vahel on andmete vahetust vähe 23
Andmeteenuse osutajad ei esita konkreetseid turbenõudeid ega kontrolli oma andmete kasutajaid 26
Seni on riiklikku järelevalvet turvameetmete süsteemi rakendamise üle omavalitsustes tehtud vähe 28
Teavitustegevused ei ole toonud loodetud tulemusi 29
Infoturbe valdkonna toetamise tegelik mõju omavalitsustes ei ole teada 31

Riigikontrolli hinnang auditeeritud omavalitsustele 33

Riigikontrolli soovitused ja auditeeritute vastused 35

Auditi iseloomustus 40

Riigikontrolli varasemaid auditeid info- ja kommunikatsioonitehnoloogia valdkonnas 42

Lisa A. Majandus- ja Kommunikatsiooniministeeriumi, Andmekaitse Inspektsiooni, Riigi Infosüsteemi Ameti ja auditeeritud kohalike omavalitsuste vastuste täistekstid 43

Valdkonna ülevaade

Miks andmeid üksteisega vahetatakse?

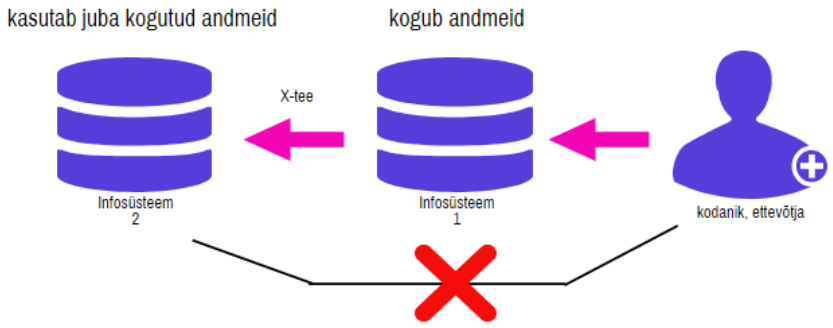
1. Praegu ei pea enam kõik asutused koguma ühtesid ja samasid andmeid eraldi andmekogudesse. Piisab sellest, kui kogumisega tegeleb üks asutus ja kõik teised võtavad andmed tema käest (vt joonis 1). Õiguse elanikke ja ettevõtjaid andmete kogumisega koormata saab ainult see asutus, kelle andmekogus on need andmed põhiandmete staatuses.

Põhiandmed on riigi infosüsteemi kuuluvasse andmekogusse kogutavad unikaalsed andmed. Ühest küljest on andmed põhiandmeteks seal, kus nad tekivad. Teisest küljest määratakse andmete põhiandmeteks olek kindlaks RIHAs.

Enne uue andmekogu asutamist tuleb kontrollida, kas andmekoosseisus olevaid andmeid juba kogutakse kuskil teises andmekogus või mitte. Kui see nii on, siis tuleb need andmed sealt küsida.

Allikas: avaliku teabe seadus, § 43[6]

Joonis 1. Andmete dubleeriva küsimise keeld



Allikas: Riigikontroll avaliku teabe seaduse § 43[6] andmetel

2. Andmete kogumise varasem praktika ei olnud tülikas mitte ainult ettevõtetele ja elanikele, vaid ka andmeid käsitlenud asutusele endale. Näiteks pidi ametnik isikuandmeid mitu korda sisestama. Praegu pole seda vaja enam teha, sest need saab automaatselt võtta rahvastikuregistrist. Samuti pole juhul, kui KOV juba kogub andmeid enda nõuetekohaselt peetud infosüsteemi, enam ametnikul vaja riigiregistritesse andmeid sisestada – need saab riigiasutus vajaduse korral kätte KOVi andmekogust.

Andmeteenuse kasutamise kokkulepe – kahe X-tee liikme kokkulepe, milles muu hulgas määratakse kindlaks andmete kasutamiseks vajalikud infoturvameetmed ning kasutajalt nõutavad turvameetmed.

Allikas: Vabariigi Valitsuse määrus „Infosüsteemide andmevahetuskiht“, § 12 lg 1

3. Kogu seesugune andmevahetus avalikus sektoris (andmekogude vahel) ja ka väliste süsteemidega (nt ettevõtjate infosüsteemidega) peab toimuma, kasutades infosüsteemide andmevahetuskihti (X-tee). X-tee kasutamise õiguse saamiseks peavad KOVid tegema riigi infosüsteemi haldussüsteemis (RIHA) andmekogu registreeringu, sõlmima andmeteenuse osutajaga andmete kasutamise kokkuleppe ning rakendama nõutud tasemel turvalisust tagavaid meetmeid.

Miks on andmete turvalisus oluline?

4. Kuna põhiandmetega andmekogu on ühtseks allikaks kõikidele teistele andmekogudele, mida peetakse avalike ülesannete täitmiseks, on andmete turvalisus eriti oluline. Turvalisus tähendab seda, et andmekogu pidaja asutus teeb kõik endast oleneva, et tagada nii enda kui ka teiste asutuste andmekogudest saadud andmete käideldavus, terviklus ja konfidentsiaalsus (vt joonis 3).

Andmete terviklus – andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamata muutuste puudumine.

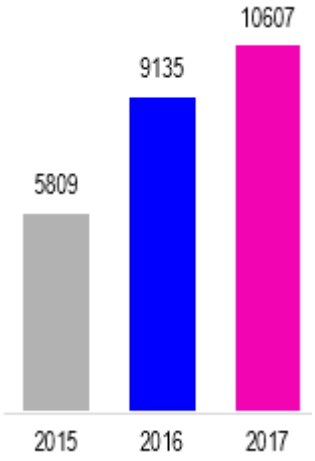
Millist ohtu vähene turvalisus endast kujutab?

5. Küberintsidente, millel oli reaalne mõju infosüsteemide käideldavusele, terviklusele või konfidentsiaalsusele, oli 2017. aastal 3147, mida on ligi 1000 rohkem kui 2016. aastal.[1] Levinumad ründed 2017. aastal olid kalastusründed, lunavara ründed ja tegevjuhi petuskeemid (ingl *CEO fraud*) – kõigi nende juhtumite vältimine on võimalik vaid nii IT eest vastutavate töötajate (arvutite turvaseadistused, varukoopiad) kui ka iga IT-kasutaja teadliku ja vastutustundliku

[1] RIA küberturvalisuse teenistuse 2017. a kuu kokkuvõtete andmetel.

käitumise korral, mis nõuab lisaks tehnoloogilisele ka organisatsioonilist tuge.

Joonis 2. Riigi Infosüsteemi Ameti infoturbe intsidentide käsitlemise osakonnas CERT-EE registreeritud infoturbe sündmused (2015, 2016, 2017)



Allikas: Riigikontroll RIA küberturvalisuse teenistuse andmetel

6. Andmeturve muutub aasta-aastalt järjest komplitseeritumaks ja ründed massilisemaks (vt joonis 2). Enam pole häkkimiseks vaja põhjalikke teadmisi – ka internetiühendusega koolipoiss on võimeline tekitama vägagi suuri probleeme, sest internetis levivad ka juba valmis kirjutatud ründekoodid jms.

7. KOVides on teadaolevalt toimunud näiteks järgmised suuremad intsidendid:

- 2017. aastal murti sisse nelja Harjumaa KOVi valvekaameratesse. Rünneteks kasutati ära kaamerate lappimata turvaauke ning asjaolu, et ligipääs seadmetele oli piiramata.
- 2017. aastal andis teadmatuse tõttu Viljandi muusikakooli töötaja ligipääsu oma arvutile ingliskeelse telefonikõne peale, kus helistaja teatas, et on Microsofti esindaja ning vajab ligipääsu arvutile, sest see on viirusi täis. Selleks ajaks, kui IT-spetsialistid jaole said, oli jõutud arvutile parool peale panna. Andmeid pahalased seekord siiski kätte ei saanud.
- Mainimist väärt on 2017. aastal ka ulatuslikum kasutajaandmete leke (üle 550 kasutajakonto) Tartu Kutsehariduskeskuses arvutitesse paigutatud nn klahvinuhi kaudu.
- 2014. aastal toimus paljudes KOVides kalastusrünne, kus teenistujatele saadeti heas eesti keeles e-kiri, mis kutsus üles ühes n-ö andmebaasis enda, kolleegide ja asutuse kontakte uuendama ja parandama.
- 2013. aastal olid mitmed koolid hädas kooli veebiserverisse istutatud pornolehtede, pahavara levitavate ja ravimimüügile keskendunud veebilehtedega.
- 2010. aastal said tundmatud pahalased ligipääsu Narva Kesklinna Gümnaasiumi serveritele, mille kaudu suunati ringi ligi 3700 Miami ja Kuuba telefonikasutajate kõnet. Gümnaasiumile esitati ligi 24 000 euro suurune arve, mis tasuti Narva linna eelarvest.

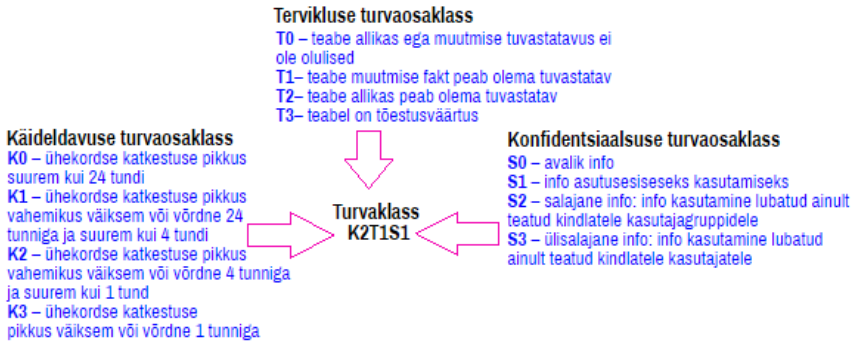
8. Riigikontrolli auditeeritud kümnest omavalitsusest kolm olid kokku puutunud lunavara ründega. Kahes neist õnnestus krüpteeritud töökohaarvuti kõik andmed taastada, aga ühes mitte, kuna osa andmeid ei olnud varundatud. Ühe auditeeritu veebilehe kaudu said pahalased välja saata rämpskirju, sest veebilehe tarkvaraversioon oli uuendamata. Veel tõid auditeeritud intervjuudes välja, et üldiselt on tavapärane, et nende sisevõrgu portide avatust skaneeritakse ning proovitakse ka eelseadistatud paroolidega seadmetesse (näiteks tulemüüri) sisse pääseda. Oli näiteid, kus KOVi sisevõrku on ühe kuu jooksul proovitud pääseda 4000–5000 erineva välise seadmega.

Mida peab tegema andmete kaitsmiseks?

9. Avaliku sektori andmekogude andmete infoturbe riskide maandamiseks tuleb abinõud valida, järgides infosüsteemide

kolmeastmelist etalonturbe süsteemi (ISKE).[2] Eestis kujunenud praktika kohaselt seisneb infoturbe nõuete ehk turvaklassi määramine selles, et konkreetsetele andmetele ja neid töötlevale infosüsteemile omistatakse nii konfidentsiaalsus-, käideldavus- (aegkriitilisus ja hilinemise tagajärgede kaalukus) kui ka terviklusnõuded (skaalal 0–3). Saadud turvaklassi järgi määratakse nõutav turbeaste ja valitakse sellele vastavad turvameetmed. ISKE pakub selleks kolme astet: madalat (L), keskmist (M) ja kõrget (H).[3] Näiteks vastab joonisel 3 kuvatud turvaklassile turbeaste M, sest käideldavuse väärtus on hinnatud tasemele 2. Oleks üks turvaosaklass tasemel 3, siis vastav turbeaste oleks H.

Joonis 3. Andmete turvaosaklassid ja tasemete kirjeldus



Allikas: ISKE rakendusjuhend 8.0

Vastutav töötleja (haldaja) – avalikku ülesannet täitev asutus, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist ning kes vastutab andmekogu haldamise seaduslikkuse (sh ISKE rakendamise) ja andmekogu arendamise eest.

Allikas: avaliku teabe seadus, § 43[4] lg 1

Andmeteenuse kasutaja – X-tee liige, kes kasutab andmeteenust.

Andmeteenuse osutaja – X-tee liige, kes osutab teistele liikmetele andmeteenust

Allikas: Vabariigi Valitsuse määrus „Infosüsteemide andmevahetuskiht“, § 2

Kes kontrollib, et andmete kaitsmisega tegeletakse?

10. Nõutud turbetaseme peab määrama enda vastutusel olevate andmete puhul asutus ise. Kui aga kasutatakse andmeid, mille eest vastutab teine asutus, siis peab arvestama ka teise asutuse seatud nõuetega. Näiteks on rahvastikuregistri põhiandmed isikuandmed, s.t kui teised registrid tahavad isikuandmeid töödelda, peab kasutama rahvastikuregistri andmeid. Siseministeeriumil kui rahvastikuregistri vastutaval töötlejal on seega õigus nõuda, et kõik, kes tema andmeid töötlevad, tagavad turbetaseme, mis on andmetele kehtestanud. Seejuures on Siseministeeriumil õigus kontrollida, kas andmeteenuse kasutajad täidavad seatud infoturbe nõudeid.

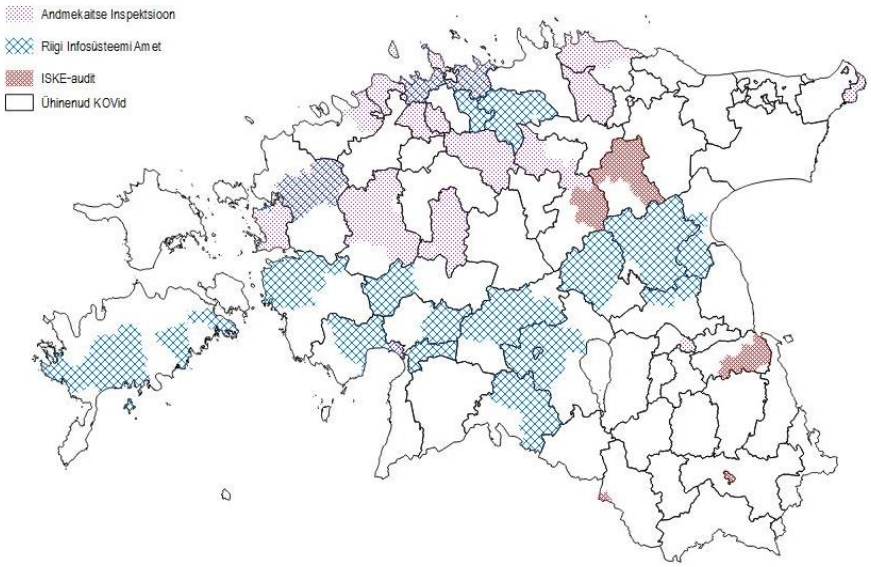
11. Erasektorilt nõutud turbetasemed peavad olema kirjas andmeteenuse kasutamise kokkulepetes. Lisaks peavad kõik isikuandmeid vahetavad osapooled arvestama isikuandmete kaitse seaduses (IKS) sätestatud kohustustega.

12. Andmeteenuse osutajad peavad tegema järelevalvet andmeteenuse kasutamise kokkuleppe tingimuste (sh infoturbe) üle. Riiklik kohustus teha järelevalvet turvameetmete rakendamise üle on RIA-l. Isikuandmete infoturbe üle teeb järelevalvet ka AKI. Lisaks on MKMile pandud kohustus vajaduse korral tellida KOVidele turvameetmete süsteemi rakendamise auditeid (ISKE-audit).

13. RIA on perioodil 2010–2017 hinnanud erinevate toimingute käigus 48 KOVi infoturbe olukorda (mh on tellitud ka 5 ISKE-auditit). AKI on kontrollinud kokku 24 KOVi infoturbe olukorda (vt joonis 4). MKMi initsiatiivil ei ole tellitud senini ühtegi ISKE-auditit ja neid ei ole planeeritud tellida ka tulevikus.

[2] Vabariigi Valitsuse määrus nr 252 „Infosüsteemide turvameetmete süsteem“, § 9 lg 2.
[3] ISKE rakendusjuhend 8.0.

Joonis 4. Senised IT-turvalisuse olukorra kontrollid haldusterritoriaalse jaotuse reformi eelsetes KOVides 2010–2017



Allikas: Riigikontroll AKI ja RIA andmetel

14. 2016. aastal sõlmisid RIA ja AKI lepingu asutuste koostööks. Seni on koostööleppe alusel toimunud ühiselt läbi viidud kontrollid ning RIHA-teemaline infovahetus. Nii AKI kui ka RIA kontrollivad RIHAs andmekogude dokumentatsiooni kooskõlastamise käigus, kas ISKE on rakendatud ja audit tehtud. 2017. aastal olid RIA eksperdid kaasatud AKI kontrollkäikudesse kuuel korral (neist 2 KOVi).

Omavalitsuste tegevus andmete turvalisuse tagamisel

Omavalitsused ei teadvusta andmete töötlemisel oma vastutuse ulatust ega kaasnevaid nõudeid

Andmete turvalisuse eesmärkide seadmine

15. Andmetele infoturbe nõuete seadmisel tuleb võtta arvesse andmekogule kehtivaid seadustest, lepingutest, põhitegevusest ja tagajärgede kaalukusest tulenevaid tingimusi. Kui turbevajadus ei ole selge, siis pole võimalik öelda, millele vastavaid turvameetmeid peaks andmete kaitseks rakendama. See omakorda võib tähendada, et andmeturbesse pannakse liiga vähe või liiga palju ressursse. Sama oht on ka siis, kui andmetele määratakse vale turvaklass. Andmete väärtust ja nõudeid käideldavusele, konfidentsiaalsusele ja terviklusele teab kõige paremini ametnik, kellel on neid vaja oma ülesannete täitmiseks ehk andmete omanik, ja mitte infoturbe spetsialist. Pärast andmete turvaklasside määramist tuleb turvaklassid asutuse juhtkonnal kinnitada.

Standardlahendus – andmekogu tarkvaraline lahendus, mille kirjeldus on kantud RIHAsse ja millel on kasutajaid rohkem kui üks või mida on mitmel asutusel võimalik andmekogu pidamiseks kasutada. Standardlahendus ja sinna sisestatavad andmed võivad olla majutatud nii asutuse enda serveris kui ka tarkvara pakkuja juures.

Allikas: Vabariigi Valitsuse määrus „Riigi infosüsteemi haldussüsteem“, § 4 lg 5

16. Riigikontrolli arvates on tähelepanuväärne, et senimaani ei olnud üks auditeeritu (s.o endine Avinurme vald) teadvustanud, et turvaklasse tuleks üldse andmekogudele kehtestada. Auditi käigus selgus, et isegi kui andmete turvaklassid olid kirja pandud, siis need ei olnud kinnitatud ja andmete turvaanalüüsi ei oldud tehtud mitte üheski auditeeritud KOVis. Enamik (s.o 7) auditeerituid tunnistas Riigikontrollile, et tegelikult lastakse andmekogu pidamiseks kasutatava tarkvaralahenduse pakkujal (standardlahenduse pakkuja) turvaklass ette öelda.

17. Auditis selgus, et standardlahenduse turbevõimekuseks pakutud turvaosaklasside (s.o K, T, S) parameetrid ei vasta alati KOVide tegelikele vajadustele ning KOVide enda kirja pandud turvaklassid ei vasta seadustest tulenevatele nõuetele.[4]

> Näiteks endise Viljandi valla personaliarvestuse infosüsteemi turvaklass on 0, kuigi see sisaldab isikuandmeid.
>
> Näiteks oli vähemalt kaks auditeeritut (s.o Rapla vald ja Avinurme vald), kes tunnistasid, et reaalsuses häiriks dokumendiregistri standardlahenduse pakkujaga lepingus kokku lepitud maksimaalselt lubatav käideldavuse tase (s.t lubatud katkestuste aeg) tõsiselt asutuse tööd. Täiesti tähelepanuta on auditeeritud siinkohal jätnud, et Andmekaitse Inspektsioon võib algatada järelevalvemenetluse, kui esinevad dokumendiregistri käideldavuse probleemid.

18. Ühe põhjusena, miks auditeeritud KOVid ei arvesta andmekogu pidamiseks tarkvara valides, millise turbeastmega andmete töötlemiseks on pakutav lahendus mõeldud, toodi, et turul puuduvad alternatiivsed pakkujad (nt lemmiklooma- ja kalmisturegistri puhul). Riigikontrolli arvates ei ole see piisav põhjendus turvaklasside määramata jätmiseks. Riigikontroll toonitab, et standardlahenduse pakkuja saab KOVile pelgalt tutvustada, millisele turvaklassile vastavaid andmeid saab tema pakutud lahenduses töödelda. Kui see on väiksem, kui KOVi kehtestatud turvaklass, siis peab KOV kõrgema turbeastme saavutamiseks arvestama omapoolsete lisameetmete rakendamisega.

19. RIHAsse sisestatud andmeid analüüsides selgus, et nelja auditeeritud KOVi puhul oli standardlahendus väiksema turvaklassiga[5], kui KOV pidas vajalikuks, kuid mingeid erimeetmeid nõutud taseme saavutamiseks ei rakendatud.

> Näiteks on raamatupidamisregistri PMEN (asutamisel) turbeaste märgitud RIHAs L, aga kasutusele võtnud auditeeritud KOVid on pidanud vajalikuks turbeastet M. See tähendab sisuliselt, et lisaks L-turbeastme meetmetele peab rakendama ka M-turbeastme meetmeid.

20. Riigikontrolli arvates saab riik KOVidele standardlahenduste pakkujana appi tulla. Kui KOVid ei leia praeguste standardlahenduste pakkujate seast endale sobivat nõuetele vastavat lahendust, siis Rahandusministeerium on juba tegemas samme, et hakata ise pakkuma KOVides enim vaja minevat tarkvara.

21. Nimelt on koostöös Eesti Linnade ja Valdade Liiduga [6] tehtud KOVides kasutatavatest andmekogudest ülevaade. Tulevikus kaalutakse, kas arendada välja ka need kesksed standardlahendused, mida turul praegu ei pakuta. Paljusid lahendusi saab riik pakkuda KOVidele, olles ise andmekogu vastutava töötleja rollis ehk luues keskselt hallatavaid riigiregistreid KOVidele seadusega pandud ülesannete täitmiseks.

---

[4] Vt täpsemalt ISKE rakendusjuhend 8.0, alapeatükk 2.3 „Andmete turvaklassi määramine“ (https://iske.ria.ee/8_03).
[5] Andmekogude andmete turvaklassid oli kirja pannud neli auditeeritut (s.o Kuusalu vald, Valga linn, Paide linn, Viljandi vald), kuid need olid kinnitamata.
[6] Kuni 27. veebruarini 2018 Eesti Linnade Liit ja Eesti Maaomavalitsuste Liit.

22. Teise põhjusena toodi välja, et kuna KOVid täidavad tihti sarnaseid ülesandeid, kogutakse ülesande täitmisel andmekogudesse ka samu andmeid. Auditeeritud KOVid ei pea otstarbekaks, et neile määrab iga KOV ise turvaklassi, tehes selleks eraldi turvaanalüüsi. Seda eriti olukorras, kus peetakse andmekogusid, mille pidamise vajadus tuleneb seadusandja soovist, s.o näiteks jäätmevaldajate register, kalmisturegister, lemmikloomade register.

23. Riigikontroll näeb selliste andmekogude puhul andmetele turbevajaduse määramisel rolli ka ministeeriumil, kui ta algatab seaduse eelnõu, millega KOVile andmekogu asutamise kohustus pannakse. Vastav ministeerium võiks anda tegevusjuhised (sh infoturbealased) kõikides nendes küsimustes, mis talle huvi pakuvad ning mille suhtes ta on KOVidele ette näinud volituse konkreetsete andmetega tegelemiseks.

Vastutus andmete töötlemisel

24. Kolmas põhjus on KOVides kujunenud väärarusaam, et andmete käideldavuse, tervikluse ja konfidentsiaalsuse eest vastutab standardlahenduse pakkuja, kelle juures andmeid hoitakse. Riigikontroll toonitab, et kuigi paljud andmed asuvad füüsiliselt standardlahenduse pakkuja mõjualas, ei ole lahenduse pakkuja kunagi vastutav töötleja. Standardlahenduse pakkuja saab vastutusele võtta vaid siis, kui KOV on omalt poolt seadnud infoturbe nõuded, mille täitmine on kokku lepitud.

Teadmiseks, et

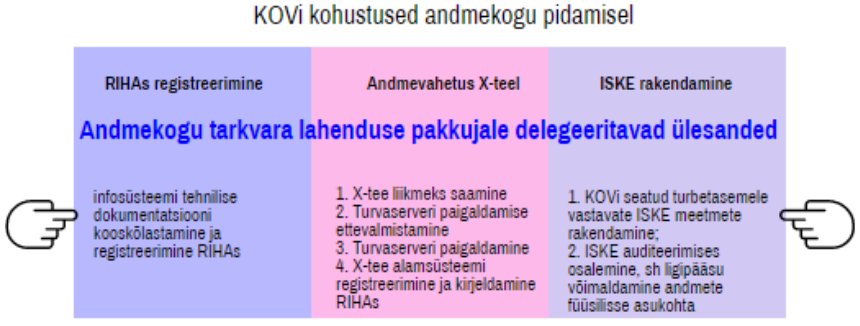
avaliku teabe seaduse § 53[1] lg 1 alusel teeb RIA haldus- ja riiklikku järelevalvet ISKE rakendamise ning infosüsteemide andmevahetuskihiga liitumise üle.

RIA-l on õigus teha ettekirjutusi, kasutada haldussunnivahendeid ning vahetut sundi, kui turvameetmete süsteemi rakendamisel leitakse puudusi.

Allikas: korrakaitseseadus § 28

25. Lepingutingimuste (nt nõutav turbeaste) seadmisel standardlahenduse pakkujale saab KOV delegeerida andmete töötlemisega kaasnevate kohustuste täitmise (vt joonis 5), kuid jääb siiski vastutavaks kehtivate seaduste rikkumise eest. Nii võib RIA võtta KOVi juhtkonna vastutusele näiteks ISKE rakendamisega seotud puuduste korral, kuigi nende puuduste kõrvaldamisega saab tegeleda ainult standardlahenduse pakkuja. Lisaks kohustuste seadmisele peab KOV ka veenduma, et standardlahenduse pakkuja täidab lepingutingimusi ning seega lepingus ette nägema ka ülesande täitmise kontrollitingimused (sh ISKE auditeerimine).

Joonis 5. Ülesannete jaotus andmekogu tarkvaralahenduse pakkuja ja KOVi vahel



Allikas: Riigikontroll Vabariigi Valitsuse määruste nr 105 „Infosüsteemide andmevahetuskiht“, nr 252 „Infosüsteemide turvameetmete süsteem“ ja nr 58 „Riigi infosüsteemi haldussüsteem“ alusel

Teadmiseks, et

on standardlahenduste pakkujaid, kes on ise üles näidanud initsiatiivi andmekogudele seatud nõudeid rakendada. Nt AS Eesti Post (Omniva) teavitab oma kodulehel, et tema andmetöötluseks kasutatavad ruumid vastavad ISKE nõuetele. Omniva arvekeskus on X-tee liige ning RIHAs on registreeritud e-arvete vahendamiseks X-tee alamsüsteem.

Allikas: Omniva koduleht; RIHA

26. Sama pakkujaga sõlmitud lepingute võrdlus auditeeritud KOVides näitas, et ettevõtja ettevalmistatud tüüplepingut ei muudeta. Osas lepingutes on turvalisuse sätted küll sees, kuid need on üldsõnalised ega viita otseselt ISKE-le või nõutud turbetasemele. IT-etalonturve oli miinimumnõudeks enamasti ainult nende andmekogude puhul, kus ettevõtja pakkus KOVile riigi arendatud tarkvaralisi lahendusi (nt omavalitsuste teenuseportaal KOVTP, volikogu infosüsteem VOLIS). X-

teel andmevahetust oli kajastatud vaid ühes teenuseosutajaga sõlmitud lepingus.

27. Kuna paljud lepingud on sõlmitud juba aastaid tagasi, ei plaani KOVid neid tagantjärele muuta. Haldusreform võib mitmes KOVis tähendada ka uute lepingute sõlmimist. Samas tõid auditeeritud välja, et nende arvates pole lepinguid vaja muuta, kuna kohapeal ei ole pädevust standardlahenduse pakkujaga läbirääkimiste pidamiseks ega lepingu tingimuste täitmise kontrolliks ning ei tähtsustata KOVi e-teenuste mõju inimeste elule.

28. Riigikontrolli arvates ei mõista auditeeritud KOVid andmekogude pidamise (sh infoturbe halduse süsteemi) põhimõtteid, kuna ei ole seatud andmeturbe eesmärke ega võetud vastutust andmekogude RIHAs registreerimise, X-teega liidestumise ja andmete turvalisuse eest. Need nõuded ei ole olnud ka standardlahenduse valiku kriteeriumiks ega seatud standardlahenduse pakkuja ülesandeks.

29. Riigikontrolli soovitused auditeeritud KOVidele:

- veenduda andmekogu tarkvaralahenduse valimisel, et tarkvaralahendus on vajaduse korral liidestatav X-teega ning et standardlahenduse turbeaste vastaks sinna sisestatavate andmete turbeastmenõudele;
- leppida lepingus teenuseosutajaga kokku, millised turvameetmed peavad olema rakendatud ja milline on turvameetmete auditeerimise korraldus.

Auditeeritud KOVide vastused (refereeritud, kõikide auditeeritud omavalitsuste vastuste terviktekstid on lisas A): Oma vastuskirjas olid soovitustega nõus ja lubasid neid edaspidi arvestada Rapla, Kuusalu, Valga ja Haljala vald ning Kohtla-Järve linn. Võru, Viljandi ja Mustvee vald ega Pärnu ja Paide linn ei avaldanud vastuväiteid soovituste kohta.

30. Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile: hinnata, kas ministeeriumid saavad seadusega ära määrata ka andmete turvaklassi andmekogu(de) puhul, mille pidamist nõutakse KOVilt kohustusliku ülesande täitmiseks.

Ettevõtlus- ja infotehnoloogiaministri vastus: Majandus- ja Kommunikatsiooniministeerium peab mõistlikuks, et sarnaste või ühetaoliste andmekogude turvaklassi määramine lähtuks ühtsetest alustest ning toimuks dubleerivate protseduurideta. Riigi infosüsteemi seisukohalt on optimaalne korraldus, kus infosüsteemid on üleriigilised ning KOVid teevad sinna kandeid. Juhul, kui seadusandja on siiski ette näinud, et iga KOV peab ise mingit registrit pidama, siis tuleb kindlasti hinnata kõikvõimalikke meetmeid, kuidas sellise andmekogu pidamisele kaasa aidata, kaasa arvatud ühtse lähenemise kujundamine turvaklassi määramisele ning turvameetmete rakendamisele.

Infoturbe planeerimise ja rakendamine seis omavalitsustes on kehv

Turvameetmete süsteemi rakendamine

31. Andmete turvalisuse omaduste säilitamiseks peab iga X-teega liituja tagama oma infosüsteemide turvalisuse. Andmete turvalisusega peab arvestama iga teenistuja oma tööülesandeid täites, sh iga infosüsteemi

kasutuselevõtu planeerimisel ja väljast tellitava teenuse hankimisel. ISKE on selleks välja töötatud turvameetmete süsteem, mis ütleb, mida peaks tegema, et asutuse töös oleks andmete turvalisus säilitatud minimaalselt aktsepteeritud turbeastmel.

Teadmiseks, et

ISKE kataloogide ajakohasuse ja kättesaadavuse parendamiseks on loodud veebipõhine rakendus **ISKE Portaal** aadressil iske.ria.ee.

32. ISKE kataloogist ei pea iga asutus absoluutselt kõike rakendama. ISKE turvameetmete kataloog sisaldab organisatsioonilisi (15%), füüsilisi (10%) ja infotehnilisi (75%) turvameetmeid, millest tuleb teha valik, lähtudes asutuse juhtkonna kinnitatud turvaklassidest ja kasutusel olevatest infovaradest. See tähendab, et kui KOVis ei ole kasutusel enam näiteks operatsioonisüsteemi MS Windows 7 või Novell, siis ei pea ka sellega seotud turvameetmeid rakendama.

33. Turvameetmete süsteemi[7] (vt joonis 6) korrektse rakendamise üheks osaks on auditi läbiviimine infosüsteemide sertifitseeritud audiitori poolt ja selle tulemustega arvestamine. KOVide andmekogudele peab ISKE-auditi tellima MKM, lähtudes vajadusest. Näiteks võidakse audit tellida enne andmekogu liitmist riigi infosüsteemiga, pärast mõnda tõsisemat turvaintsidenti, teatud riskide olemasolul turvaintsidentide ennetamiseks, pisteliselt teatud ajaperioodi tagant või muudel põhjendatud juhtudel.

Joonis 6. Turvameetme süsteemi rakendamine

Allikas: Riigikontroll Vabariigi Valitsuse määruse „Infosüsteemide turvameetmete süsteem“ andmetel

Käitavad infovarad – varad, mis otseselt on vajalikud andmekogu töö tagamiseks (nt rakendus, andmebaas, server jms).
Toetavad infovarad – varad, mis on vajalikud andmekogude ja/või nendega seotud käitavate varade toimimise tagamiseks.
Autonoomsed infovarad – varad, mille esmane funktsioon ei ole seotud andmete ega andmekogudega (nt tööruumid, majad, telefonisüsteem).

Allikas: ISKE rakendusjuhend

Tüüpmoodulid – infovarade liigid (nt B.3.101. „Server“, B.3.203. „Sülearvuti“, aga ka B.2.4. „Serveriruum“), millel on teatud eriomadused ja oma turvaspetsiifika. Iga tüüpmooduli kirjelduses on toodud ohtude ja rakendatavate turvameetmete loetelu.

Allikas. ISKE kataloog 8.0

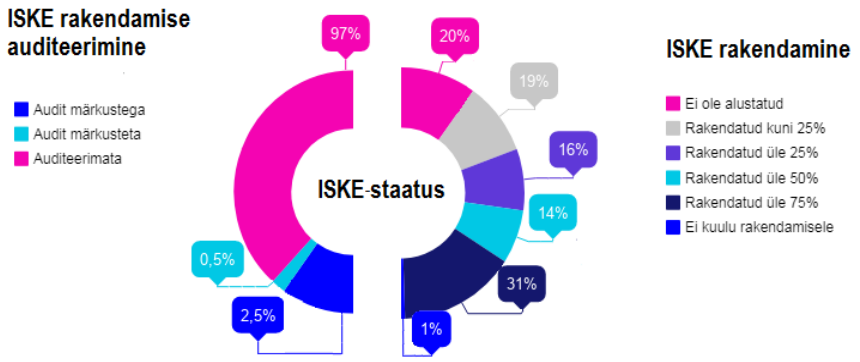
34. Selleks et ISKE-auditi edukas läbiviimine oleks võimalik, peaksid KOVis olema eelnevalt täidetud teatud eeldused. Esimese asjana peaksid KOVid saama ülevaate sellest, mis neil olemas on, s.t andma ülevaate andmekogudest ja inventeerima infovarad (sh riist- ja tarkvara, ruumid). Seejärel tuleb määrata andmete omanikega koos turvaklassid andmekogudele ja nendega seotud infovaradele, vastavalt turbeastmele valida ISKE kataloogist välja rakendamisele kuuluvad tüüpmoodulid, nendest omakorda rakendada asjakohased turvameetmed ja kontrollida nende rakendamist.

35. RIA korraldatud küsitlused (2010, 2012, 2016) näitavad, et KOVides on valmisolek ISKE-auditi edukaks läbiviimiseks aastatega pigem paranenud. RIHAs on KOVid valdavalt märkinud oma andmekogude puhul ISKE rakendamise mittetäielikuks ja mitteauditeerituks.

36. Riigikontrolli arvates on tähelepanuväärne, et hoolimata sellest, et ISKE on KOVides olnud kohustuslik juba 10 aastat, leidub endiselt KOVisid, kes ei pea ISKE rakendamist kohustuslikuks (vt joonis 7). Riigikontroll rõhutab, et ISKE osaline rakendamine kasutusele võetud andmekogu puhul ei anna kindlust turvameetmete piisavuse suhtes ning ISKE on kohalduv ka siis, kui tegemist on asutusesiseseks kasutuseks mõeldud andmekoguga.

[7] Vabariigi Valitsuse määrus nr 252 „Infosüsteemide turvameetmete süsteem“, § 2.

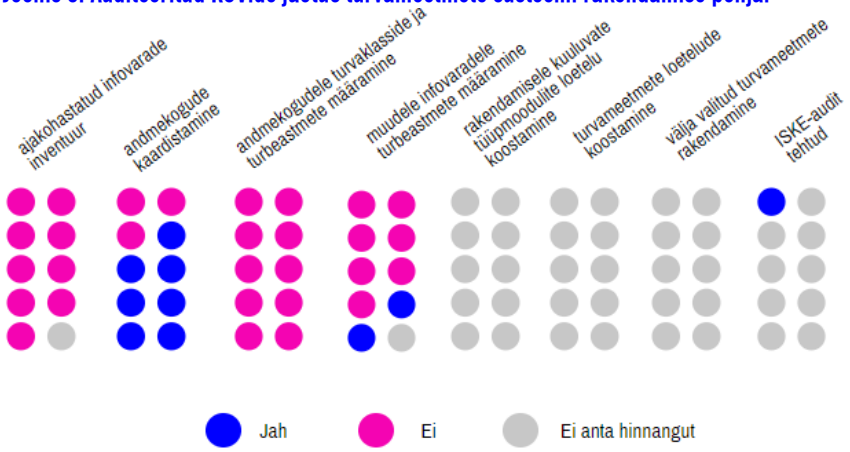
Joonis 7. RIHAS registreeritud KOVides kasutusel olevate andmekogude ISKE-staatus



Allikas: Riigikontroll RIHA andmetel (2017)

37. Auditeeritud KOVides saadakse enamasti hakkama infovarade ja andmekogude loetelu koostamisega, kuid turvaklasside määramine on osutunud suureks probleemiks (vt joonis 8). Paraku ei saa ilma selleta täita (s.t ei saa hinnata) ka joonisel toodud järgmisi tegevusi, sest need kõik sõltuvad määratud turvaklassist. Isegi kui turvameetmete loetelu on koostatud ning seda rakendatakse, pole võimalik öelda, kas see on piisav, sest pole millelegi vastavust hinnata.

Joonis 8. Auditeeritud KOVide jaotus turvameetmete süsteemi rakendamise põhjal[8]



Allikas: Riigikontroll

Turvameetmete süsteemi rakendamise auditeerimine KOVides

38. Riigikontroll tegi oma 2017. aastal avaldatud märgukirjas „Isikuandmete kaitse riiklikes andmekogudes“ Majandus- ja Kommunikatsiooniministeeriumile (MKM) soovituse alustada oma kohustuse täitmist, s.t hakata tellima KOVidele ISKE-audititeid. MKM ei ole seni talle määrusega pandud ülesannet täitma asunud ning käesoleva auditi käigus antud selgituste kohaselt ei kavatse seda ka tulevikus täitma hakata. MKM ei pea praegust KOVide ISKE-auditite tellimise korraldust finantside, kompetentsi (eelkõige järelevalve) ja muude ressursside vaates jätkusuutlikuks. Samal ajal ei ole aga Riigikontrollile teadaolevalt alustatud tegevust, mis muudaks MKMi kohustust seda ülesannet täita, s.t algatatud määruse muutmist.

39. Varem on auditeid tellitud RIA initsiatiivil. ISKE-auditite, mis viidi läbi 2013. aastal, ei ole järelauditit tellitud, hoolimata sellest et auditites

[8] Valga Linnavalitsuses õnnestus ISKE-audit läbi viia, kuna ISKE-audit tehti RIA etteantud ISKE tüüpmoodulite põhjal ja see ei olnud otseselt sõltuvuses turvameetmete süsteemi senise rakendamise seisust KOVis.

oli ka märkusi kõrge riskiastmega meetmete kohta. Riigikontroll tuvastas auditi käigus, et vähemalt üks KOV, kelle juures RIA tellitud ISKE-audit läbi viidi, ei ole auditijärgseid tegevusi täies mahus ette võtnud – RIHAsse on ISKE-auditi tulemus märkimata ja pooled kõrge riskiastmega meetmed endiselt vaid osaliselt rakendatud.

40. Riigikontroll hindas ka valikuliselt ISKE kataloogi turvameetmete rakendamist KOVides. Kokku hinnati 15 erinevast tüüpmoodulist valitud 85 turvameetmest 129 kriteeriumi täitmist (vt tabel 1). Kuna KOVid ise turvameetmeid välja valinud ei ole, tehti valik nendest tüüpmoodulitest, mille täitmisega on KOVides RIA andmetel varem probleeme olnud.

Tabel 1. Tüüpmoodulite kriteeriumitele antud hinnangute jagunemine (%)

Tüüp-moodulid / Hinnang	1.0. Infoturbe haldus	1.1. Organisatsioon	1.2. Personal	1.4. Andmevarundus-poliitika	1.6. Viirusetõrje kontseptsioon	1.8. Turvaintsidentide käsitlus	1.9. Riist- ja tarkvara haldus	1.11. Väljastellimine	1.13. Infoturbe teadlikkus ja -koolitus	3.301. Turvalüüs (tulemüür)	1.10. Tüüptarkvara	1.14.. Turvapaikade ja muudatuste haldus	3.201 Klient	3.302. Marsruuterid ja kommutaatorid	5.7. Andmebaasid	2.4. Serveriruum
Positiivne	18	66	61	56	59	48	50	49	20	20	65	68	80	100	27	45
Negatiivne	41	22	28	36	24	10	46	40	60	40	35	23	20	0	67	50
Ei kohaldu	41	12	11	8	17	42	4	11	20	40	0	10	0	0	7	5

Allikas. Riigikontroll

41. Selgus, et auditeeritud KOVides on endiselt raskusi mitmete madala turbeastme turvameetmete rakendamisega. Näiteks on IT-kasutajatele antud kergekäeliselt piiranguteta õigusi, tihti puudus ka ülevaade, kes ja kuhu üldse ligi pääseb, paroolihaldus oli puudulik, turvapaikade paigaldamine oli jäetud paljuski kasutajate meelevalda, tarkvara legaalsust töökohaarvutites ei kontrollitud.

42. Täpsed hinnangud kriteeriumite täitmise kohta on Riigikontroll edastanud auditeeritud KOVidele eraldi.

43. Jooniselt 8 selgub, et **kohustuslikku turvameetmete süsteemi ei ole suutnud täies ulatuses ükski KOV rakendada**. KOVid on seda põhjendanud ISKE töömahukusega. Selgituste kohaselt käib ISKE dokumentatsiooni väljatöötamine ja ka kogu IT-taristu haldamine ISKE rakendusjuhendi ja meetmete kataloogi järgi KOVidele üle jõu. KOVid on teinud RIA küsitlustes ettepaneku ISKEt kohaldada etapiviisi või vähendatud mahus. Kuigi ISKE rakendamise seisu selgitamiseks on tehtud küsitlusi, pole rakendamist takistavaid asjaolusid seni analüüsitud.

44. Auditi käigus ISKE rakendamist kontrollides ei selgunud olemuslikke küsitavusi ISKE metoodika kohasuses. Siiski peaks ISKE metoodika rakendamise suunistes (sh turvaklassi määramine kohustuslikus korras peetavatele andmekogudele, standardlahenduste auditeerimine) rohkem arvesse võtma KOVide spetsiifilisi vajadusi.

45. Auditis selgus muu hulgas, et andmekogude pidamiseks kasutab valdav osa KOVe standardseid lahendusi (84% RIHAs registreeritud

andmekogude puhul). Riigikontrolli arvates oleks optimaalne viia turvameetmete rakendamise kontroll läbi välise teenuseosutaja (sh standardlahenduse pakkuja) juures üks kord. Kuna aga turvaklassi peab määrama (sh kinnitama) andmekogule iga KOV ise, siis saab ühe juba läbi viidud ISKE-auditi antav kindlustunne teenuseosutajat puudutavas osas olla ülekantav teistesse audititesse vaid kattuvate turvameetmete puhul. Praegu puudub kindlus, et ISKE rakendamise metoodika väljatöötamisel on seda eripära arvestatud.

46. Riigikontrolli soovitused ettevõtlus- ja infotehnoloogiaministrile:

- analüüsida põhjuseid, miks turvameetmete süsteemi rakendamine KOVides on pikalt viibinud ning sellest tulenevalt töötada välja tegevused ISKE rakendamise paindlikumaks muutmiseks (sh kaaluda standardsete tarkvaralahenduste osutajatele ISKE-auditi läbimise kohustuse seadmist) KOVides nii, et see oleks rohkem kohapealseid olusid arvestav;
- muuta ISKE-auditi tellimise korraldust (sh ISKE-auditi juhendit) nii, et selle tellimine oleks järjepidevalt tagatud.
- algatada Rahandusministeeriumiga ISKE-auditite tellimise rahastuse läbirääkimised.

Ettevõtlus- ja infotehnoloogiaministri vastus: Majandus- ja Kommunikatsiooniministeerium adresseerib Riigikontrolli tõstatud probleeme ISKE määruse uuendamisel ja ISKEga seotud juhendite ja materjalide läbivaatamisel. Küberturvalisuse seadusega laieneb turvameetmete rakendamise kohustus ka teistele infosüsteemidele lisaks nendele, mida kasutatakse andmekogude pidamisel (01.01.2020). ISKE määrus, juhendid ja materjalid vajavad eelnevat kaasajastamist selle muudatuse realiseerimiseks. Riigikontrolli tõstatud küsimusi on otstarbekas käsitleda koos küberturvalisuse seadusest tingitud muudatustega. MKM nõustub, et senine korraldus KOVide ISKE auditite tellimiseks on ebaõnnestunud.

Riigikontrolli täiendav kommentaar: Riigikontroll rõhutab, et KOVides peab olema tagatud järjekindel ISKE-auditite tellimine. Kuigi infoturbe süsteemi auditi ülesanne on muu hulgas anda kindlus turvameetmete süsteemi kavandatud toimimise kohta eelkõige asutuse juhtkonnale, on alguses otstarbekas tellida ISKE-auditid KOVides tsentraalselt, sest see tuleks odavam ja lahendaks esialgu ka standardlahenduste pakkujate auditeerimise küsimuse.

Infoturbe kontseptsioon – ametiasutuse infoturbe protsessis keskne dokument, mille puhul kehtib eeldus, et turbevajadus on kindlaks määratud, ning mis sisaldab turvameetmete nimekirja ja realiseerimisplaani (meetmete rakendamise järjekord ja vastutavad isikud või osakond). Praktikas võetakse infoturbe kontseptsioon kasutusele selleks, et kontrollida konkreetsete turvameetmete rakendamist või nende aktuaalsust.

Allikas: ISKE kataloog M 2.195

Omavalitsuste infoturbekultuur on madal nii teenistujate kui ka juhtkonna tasandil

47. Kõikidel teenistujatel peab olema arusaam infoturbest kui ühest olulisest osast asutuse iga ülesande täitmisel. Infoturbe kontseptsiooni algatus ja rakendamise eeskuju peab tulema ametiasutuse juhtkonnast. Selle näitamiseks tuleb juhtkonnal kinnitada turvaklassid ja infoturbepoliitika, need lõimida kogu asutuse tegevusse; määrata IT-turbe eest vastutavad töötajad, tagada neile piisav koolitus ja anda nende käsutusse

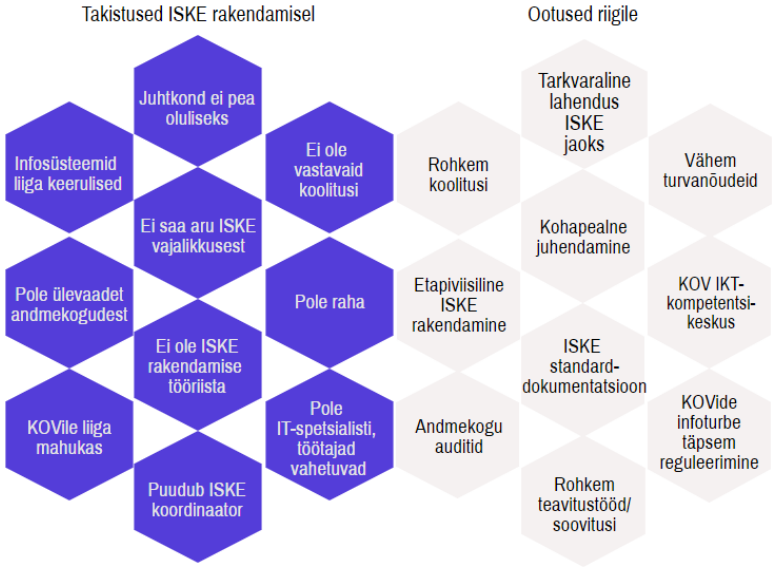
vajalik eraldis eelarvest.[9] Infoturbe kontseptsiooni ajakohasust tuleb seejuures kontrollida vähemalt pärast ISKE rakendusjuhendi uuendamist.

ISKE rakendusjuhendi uuendamine – ISKE rakendusjuhend ilmub täiendatud kujul uue versioonina kord aastas, sõltuvalt allikmaterjali uute versioonide avaldamisest. Kehtiv ISKE rakendusjuhendi versioon on 8.00. See tähendab, et kõik dokumendid, mis on koostatud eelnevate versioonide põhjal, tuleb üle kontrollida ja uuendada.

Allikas: ISKE rakendusjuhend 8.0

48. RIA küsitluste põhjal on läbi aastate KOVides ISKE puuduliku rakendamise põhjusteks toodud juhtkonna vähest huvi infoturbe meetmete rakendamise vastu, IT-ametikoha puudumist, ametnike vähest arusaama turbetegevuse olulisusest ja vajalikkusest ning riigipoolsete koolituste-teavitusürituste, kohapealse juhendamise ning ISKE rakendamise üle sisulise kontrolli vähesust (vt lisaks joonis 9).

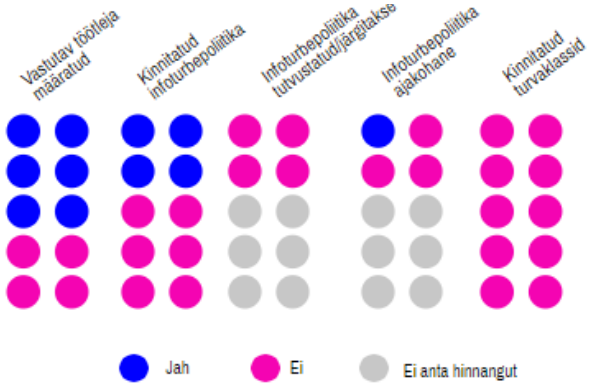
Joonis 9. KOVide ootused riigile ISKE rakendamisel ja senised takistused (2010, 2012, 2016)



Allikas: Riigikontroll RIA 2012. ja 2016. aasta küsitluse andmetel

49. Riigikontroll tuvastas auditi käigus, et mitte ühelgi auditeeritul ei olnud ajakohast infoturbe kontseptsiooni, mis sisaldaks infoturbe eesmärke ja täideviimise eest vastutavaid isikuid (vt joonis 10). Neljas KOVis oli küll kehtestatud infoturbepoliitika, kuid selle sisu ei olnud teenistujatele tutvustatud (v.a endine Rapla vald) ega nõuetekohaselt ajakohastatud. Intervjuudes tunnistasid KOVide esindajad valdavalt, et infoturbepoliitikast päriselus ei lähtuta ning selle rakendamine on eelarveraha jagamisel teisejärguline.

Joonis 10. Auditeeritute jaotus juhtkonna tasemel turvameetmete rakendamise järgi



Allikas: Riigikontroll

[9] ISKE M 2.336 „Koguvastutus infoturbe eest juhtkonna tasemel“.

50. Sõltumata suurusest peab asutuses olema töötaja, kes vastutab kõigi IT-turbega seotud asjaolude eest.[10] IT-turbe eest vastutav töötaja tuleb kaasata kõikidesse IT-ga seotud tegevustesse, et oleks tagatud piisav tähelepanu ka turvalisusega seotud aspektidele.

Teadmiseks, et

2016. aastal tehtud uuringu kohaselt panustatakse IT-turvalisusele kõige sagedamini kogu IKT-kulust 4–6%.[11] Auditeeritud KOVide IKT-kulud jäid 2017. aastal vahemikku 10 000 kuni 200 000 eurot. Seega oleks potentsiaalne kulu IT-turbele keskmiselt olnud vahemikus 1000 kuni 10 000 eurot aastas.

Allikas: Riigikontroll riigiraha rakenduse andmetel

51. Väikestes asutustes võib IT-turvalisuse eest vastutava töötaja funktsiooni üle võtta ka mõni selleks kvalifitseeruv isik, kes täidab lisaks ka veel teisi tööülesandeid. Sellisel juhul peab olema tagatud, et IT-turvalisuse ees vastutavale töötajale jääb oma tööülesannete täitmiseks piisavalt aega. Eriti oluline on piisava ajalise ressursi planeerimine siis, kui IT-turbe protsesse hakatakse juurutama esimest korda. Lisaks peab vastutavale töötajale määrama ka kvalifitseeritud asendaja.

52. Kõigis auditeeritud KOVides oli kasutajatele mingil viisil IT-tugi tagatud. Pooltes KOVides oli IT-hooldusteenus kas täielikult või osaliselt väljast tellitud ja pooltes oli tööle võetud IT eest vastutaja (nt Kohtla-Järve linnas ja Viljandi vallas 2 IT-töötajat). 6-l KOVil on lepingutes teenuseosutajatega või teenistujate ametijuhendites kirjalikult välja toodud tingimus infoturbenõuetega arvestada või sellega seotud ülesandeid täita. Asendaja oli määramata 3 KOVis. Ühes KOVis oli asendaja küll määratud, kuid isikul puudus piisav väljaõpe.

53. PricewaterhouseCoopersi 2015. aastal koostatud eksperdihinnangus „Kohalike omavalitsuste IT juhtimise, e-teenuste analüüs ja arendusettepanekud“ toodi välja, et üldiselt on väikestes KOVides IT antud mõne teise valdkonna spetsialisti vastutusalasse ning keskmise suurusega KOVides koosneb IT-teenistus kuni paarist spetsialistist.[12] Lisaks kirjeldati, et peamiselt suudetakse pakkuda IT tehnilist tuge, aga spetsialiseerumist (sh infoturbele) on vähe ning keerukamate tehniliste probleemide puhul on vajadus välise abi järele.

Teadmiseks, et

Kuusalu vald on asunud andmekogude majutust ja spetsiifilist teadmist vajavaid haldusteenuseid väljast sisse tellima. Sama praktikat kasutatakse ka Võru vallas spetsiifilisemate seadmete (nt võrguseadmete) haldamisel.

54. Ka Riigikontrolli audit kinnitas, et spetsialiste, kel oleks konkreetsete seadmete kohta põhjalikud teadmised, on vähe. Näiteks võis kohapealne IT-spetsialist saada väga hästi hakkama töökohaarvutite keskhalduse reeglite seadmisega, kuid tulemüüri seadistamisega jäi hätta ning mitmel juhul olid n-ö vaikeseadistused (*default*) jäänud muutmata. Vaikeseadistuste juures tuleb aga silmas pidada, et tootja või levitaja algsätted ei pruugi olla optimaalselt turvalised, sest tähtsamaks peetakse tihti lihtsat paigaldamist ja kasutuselevõttu. Tulemüüride vaikeseadistusi ei tasu seetõttu pimesi pidada turvaliseks ja kohe kasutamiseks võtta.

55. Kuna iga seadme haldamiseks ei ole mõistlik palgata eraldi inimest, saaksid Riigikontrolli arvates KOVid siinkohal teha rohkem koostööd erasektoriga või teiste KOVidega. Näiteks on MKM viidanud praktikale mujalt maailmast, kus KOVid on ühiselt asutanud IT-haldusteenuseid pakkuva ettevõtte.

Teenistujate infoturbe teadlikkuse suurendamine

56. KOV peab oma teenistujaid kursis hoidma nii kasutusele võetud infoturbe meetmetest kui ka nende rakendamata jätmisega seotud tagajärgedest. Turvameetmed ei tööta, kui teenistujad käivad nii reeglite kui ka tehnoloogiliste lahendustega hooletult ümber. Näited selle kohta

[10] ISKE M 2.193 „Infoturbeks sobiva organisatsioonilise struktuuri rajamine“.
[11] Filkins, Barbara (2016). IT Security Spending Trends. SANS Institute. https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697.
[12] 5000 – 20 000 elanikuga KOVides on keskmiselt 0,73 IT-spetsialisti KOVi kohta.

on parooli jätmine lauale, varunduse vahelejätt, süsteemi lahtijätt lahkumisel.

57. Pooltel KOVidest puudusid audititoimingute ajal üldse kehtestatud suunised IT-kasutajatele olulisemate turbeaspektidega ümberkäimiseks (sh infovahetuseks). Auditeeritute vastuste põhjal võib öelda, et teenistujate teavitamine infoturbe suunistest on valdavalt suuline ning neile ei ole alati loodud võimalust tutvuda dokumentatsiooniga iseseisvalt. Paaril juhul selgus intervjuu käigus, et KOV ei olnud teavitanud oma teenistujaid suuniste olemasolust.

Teadmiseks, et

2010. a Tartu Linnavalitsuse tulemüüri riist- ja tarkvara vahetus mõjutas linna dokumendiregistri seadistust nii, et paari nädala jooksul oli avaliku kasutajana Tartu kodulehe kaudu linna dokumendiregistrisse sisenejal võimalik lugeda sotsiaalabiosakonna korraldusi hooldajate määramise, alaealise varaga tehingute teostamiseks nõusoleku andmise jm kohta.

Karistusseadustiku kohaselt (KarS, § 157 ja 157 lg 1) karistatakse delikaatsete isikuandmete ebaseadusliku avaldamise või juurdepääsu võimaldamise eest rahatrahviga kuni 300 trahviühikut.

Allikas. Postimees Online (19. märts 2010)

58. Riigikontroll tuvastas, et vähemalt kahel auditeeritul kümnest esineb igapäevatöös ebakorrektset delikaatsete andmete edastamise praktikat. Delikaatsete andmete edastamisel ei hinda ametnik ise nende kaitse vajadust ning rakendab erimeetmeid vaid juhul, kui adressaat on seda palunud teha. Praktika, kus kahe osapoole suhtluses edastatakse delikaatseid isikuandmeid avalike võrkude kaudu ilma erimeetmeid (nt andmete krüpteerimine) rakendamata, võib olla tõsiste tagajärgedega nii isikule, kelle andmed võivad avalikuks saada, kui ka asutuse enda jaoks.

59. Ükskõik millise infoturbe halduse süsteemi (sh ISKE) rakendamine eeldab, et juhtkond on teadlik infoturbe vajalikkusest.[13] Auditeeritud KOVide juhtkonna liikmeid intervjueerides selgus, et üheski KOVis ei ole infoturbe eest vastutav isik juhtkonnale selgitanud seadusest tulenevaid infoturbenõudeid ja riske, nendega seotud kulusid ja mõju tööprotsessidele. Riigikontroll toonitab, et taoliste koolituste läbimine ei ole valikuline. Kui majasiseseid koolitusi ei tehta, siis on juhtkonnal võimalus osaleda RIA korraldatud vastavasisulistel koolitustel.

60. Mõnel auditeeritul on saanud tavaks majakoosolekutel jagada infoturbeteavet kõigi töötajatega (s.o Audru, Kuusalu, Paide), kuid mitte ükski auditeeritud KOV pole majasiseselt enda teenistujaid infoturbe valdkonnas koolitanud.[14] RIA esitatud andmetel on perioodil 2010–2017 (III kv) kümnest auditeeritud KOVist seitsme teenistujad osalenud ISKE-teemalisel koolitusel.[15]

61. Riigikontrolli arvates võib öelda, et oma teenistujate infoturbe teadlikkuse suurendamisse ja infoturbekoolitustesse ei panustata. Sellest järeldades on mõistlik KOVidel kaaluda IT-halduse valdkonnas koostöö tegemist vähemalt selles ulatuses, mis aitab kaasa infoturbenõuete paremale täitmisele.

62. Riigikontrolli soovitus auditeeritud KOVidele: määrata infoturbejuhi ülesannete täitja või tellida infoturbejuhtimine teenusena sisse, et oleks tagatud piisav tähelepanu IT-turvalisusega seotud aspektidele.

Auditeeritud KOVide vastused (refereeritud; kõikide auditeeritud omavalitsuste vastuste tervikteksti on lisas A): Oma vastuskirjas olid soovitusega üldiselt nõus ja lubasid sellega arvestada või olid asunud soovitust täitma Rapla, Kuusalu, Valga, Haljala, Võru ja Mustvee vald

[13] ISKE M 3.44 „Juhtkonna teadlikkuse tõstmine infoturbe alal“.
[14] ISKE M 3.5 „Turvameetmete koolitus“.
[15] ISKE M 3.49 „Koolitus etalonturbe protseduuride alal“.

ning Kohtla-Järve linn. Viljandi vald ning Pärnu ja Paide linn ei avaldanud vastuväiteid soovituse kohta.

Riigi tegevus andmete turvalisuse tagamisel

Omavalitsuste ja riigi andmekogude vahel on andmete vahetust vähe

Andmekoosseisu kontroll

63. Platvormina tagab X-tee turvalise andmevahetuse erinevate liikmete (sh KOVid) vahel. Ainult RIHAs registreeritud andmekogudel on juurdepääs teistele andmekogudele (ehk X-teele), kelle andmeid saab n-ö ristkasutada, et säästa käsitsi andmesisestusele kuluvat aega. Riigi ja KOVi andmekogud peavad läbima selleks kooskõlastuse, mis annab andmekogu pidajale kindluse nõuetele vastavuse suhtes.

64. Näiteks kontrollitakse andmekogu asutamisel kooskõlastuse käigus, kas andmekogusse on plaanis koguda andmeid, mida juba mujale kogutakse.[16] Kui selgub, et andmeid on võimalik mujalt saada, siis ei pea avaliku ülesande täitja enam ise neid andmeid kodanikelt koguma.

Andmekogude kaardistus – ISKE rakendamiseks on vaja KOVil koostada ülevaade andmekogudest, mille andmeid töödeldakse (sh volitatud töötlejana).

Allikas: ISKE rakendusjuhend 8.0

65. Auditi käigus uuriti, kui paljud auditeeritud KOVidest olid oma andmekogude kaardistuses ja mujal loetletud andmekogusid RIHAs registreerinud. Riigikontroll leidis juba oma 2017. aastal avalikustatud ülevaates, et valdavalt KOVid oma andmekogusid RIHAs ei registreeri. 2018. aasta alguse seisuga oli registreeritud 218 andmekogu, mida on selgelt vähem, kui KOVides tegelikult kasutuses on. Ainuüksi auditeeritud 10 KOVis oli kokku kaardistatud 78 andmekogu.

66. Selgus, et kuigi kõik auditeeritud (v.a endine Vihula vald) olid ühtviisi teadlikud kohustusest registreerida andmekogud RIHAs, ei olnud ükski KOV registreerinud kõiki oma andmekogusid. Paaril juhul (endine Avinurme vald, endine Paide linn) ei olnud registreeritud ühtegi andmekogu. Enamasti põhjendati andmekogude registreerimata jätmist kas RIHA keerukusega või mööndi, et sellega lihtsalt ei ole tegeletud.

Teadmiseks, et

juhtudeks, kus asutusel on vaja X-tee teenuseid kasutada, aga päringuid tehakse nii vähe, et oma infosüsteemi väljatöötamine või olemasoleva infosüsteemi X-teega liidestamine ei ole majanduslikult mõistlik, on loodud priivara MISP (mini infosüsteem-portaal).

Allikas: RIA

67. Võimalus kasutada andmekogude pidamiseks standardlahendusi on hea, sest siis ei pea iga KOV ise sama ülesande täitmiseks oma tarkvara välja arendama. Samas tuleb teadvustada, et standardlahenduse pakkuja ei pea oma toodet RIHAs registreerima ega registreerimisel kooskõlastama ning ka kooskõlastajate tehtud märkused standardtarkvara pakkujale ei ole siduvad täitmiseks.

68. Standardlahenduse peab alles siis registreerima, kui see on kasutusele võetud ja sinna on hakatud andmeid sisestama, s.t kui ta on omandanud andmekogu staatuse.[17] Avaliku teabe seaduse mõte on, et kooskõlastama peab iga standardlahenduse kasutuselevõtu, sest kohe, kui KOVi ametnik standardlahenduse sisse andmed paneb, saab sellest suure tõenäosusega teistega andmeid vahetav andmekogu.

Teadmiseks, et

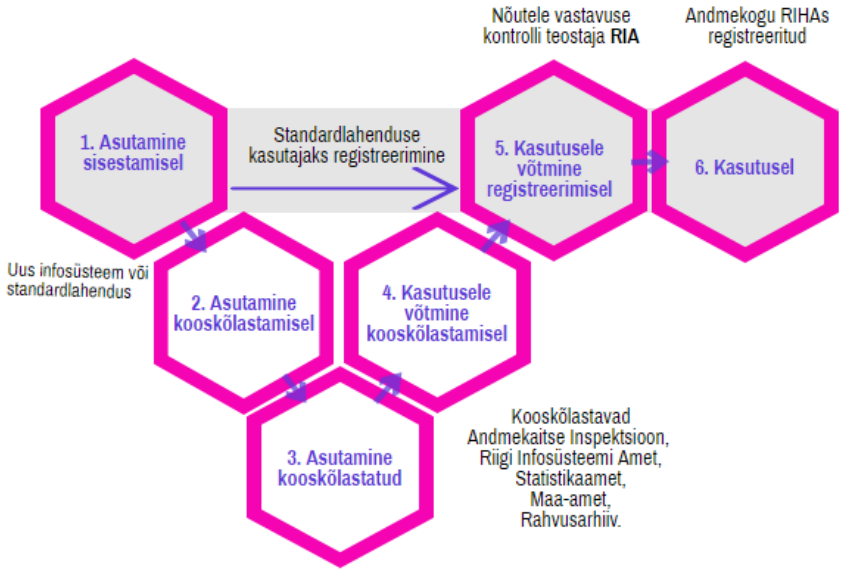
RIHAsse on ettevõtjate omal initsiatiivil registreeritud 17 erinevat standardlahendust, mille kasutajaks saavad KOVid ennast registreerida.

69. Endine Rapla vald ja Kuusalu vald selgitasid Riigikontrollile, et nemad registreerivad andmekogu alles siis, kui standardlahenduse pakkuja on oma toote RIHAs ära registreerinud, sest standardlahenduse kasutajaks registreerimine on lihtsustatud (vt joonis 11). Kui standardlahenduse pakkuja on otsustanud oma toote RIHAs registreerida,

[16] Vabariigi Valitsuse määrus nr 58 „Riigi infosüsteemi haldussüsteem“, § 7 lg 5, 6.
[17] Avaliku teabe seadus, § 43^7 lg 1.

siis enamik andmeid tarkvara kohta on juba sisestatud ning KOV ei pea sisuliselt muud tegema, kui märkima ennast selle tarkvaralahenduse kasutajaks.[18]

Joonis 11. Andmekogu pidamiseks standardlahenduse kasutusele võtmise kooskõlastamine RIHAs



Allikas: Riigikontroll RIHA baaskoolituse „Infosüsteemi staatused“ andmetel

70. Kui tegemist on potentsiaalselt riigi infosüsteemi kuuluva standardlahenduse kasutuselevõtuga, ei saa piirduda ainult registreerimisega ning RIHAs kooskõlastamisel peavad andmete koosseisu kontrollima vähemalt RIA ja AKI.[19] Auditi käigus selgus, et praktikas näiteks AKI seda ei tee. Seega ei läbi enamik (84%) RIHAsse registreeritud KOVide andmekogudest andmete koosseisu kontrolli. AKI ei pea seda otstarbekaks, sest eeldab, et kui standardlahenduse on juba tarkvara pakkuja registreerinud, siis KOVid ei muuda selle kasutuselevõtul andmete koosseisu.

71. Riigikontrollile antud selgitustes AKI küll möönis, et eraldi iga KOVi kaupa kooskõlastamine on korrektsem kui ainult standardlahenduse ühekordne kooskõlastamine, kuid samas tõi välja, et see tekitaks ebamõistlikku koormust, kui kooskõlastus antakse sama andmekoosseisu ja sisult identse põhimäärusega andmekogule ühe korra asemel näiteks 79 korda.

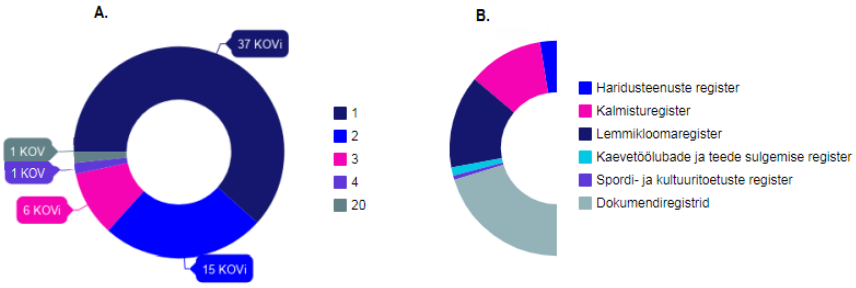
72. Mitmed standardlahenduste pakkujad on valmis kõigile oma toote kasutajatele andmevahetust X-tee vahendusel pakkuma. Siiski ei ole kõik kasutajatest KOVid oma andmekogusid lasknud X-teega liidestada ja sisestavad endiselt andmeid topelt või kasutavad muud andmevahetusviisi, sest pakutav tarkvaralahendus ei pruugi olla X-teega liidestatav.

73. RIHA andmetel on X-teega liidestatud 109 KOVide andmekogu (vt joonis 12).

[18] Vt täpsemalt juhend „Standardlahenduse kasutajaks registreerumine“.
[19] Avaliku teabe seadus, § 43^3 lg 3.

Riigikontroll tuvastas oma auditi „Riigi ja kohalike omavalitsuste tegevus olmejäätmete kogumisel ja taaskasutusse suunamisel“ käigus, et 83%-l KOVidest oli andmekogu jäätmevaldajate üle arvestuse pidamiseks ning valdavalt kasutati selle pidamiseks mõnda standardlahendust. RIHAsse on jäätmevaldajate registreid registreeritud vaid 7. Andmekogu andmekoosseis sisaldab mh aadressiandmeid, mida peab pärima otse Maa-ameti aadressiandmete süsteemist või kaudselt Siseministeeriumi rahvastikuregistrist. Kummagi asutusega pole standardlahenduse pakkuja X-tee liidestusi loonud.

Joonis 12. A. KOVide jaotus X-teega liidestatud andmekogude arvu järgi. B. Andmekogude standardlahendused, millel on enim X-tee liidestusi (2017), osakaalu järgi



Allikas: Riigikontroll RIA andmetel

74. Kuna andmekogusid ei esitata RIHAsse kooskõlastamisele, ei läbi need ka andmekoosseisu kontrolli. Jooniselt 12 on näha, et vähesed KOVid on hinnanud oma andmekogu planeerimisel andmete kättesaadavust teistest andmekogudest. Kokku on 60 KOVi märkinud RIHAs, et nende andmekogud on X-teega liidestatud. 37 KOVi (s.o 62%) on RIHAs märkinud vaid ühe oma andmekogudest X-teega liidestatuks.

Näiteks on EHISes loodud X-tee teenused automaatseks andmeedastuseks koolide õppeinfosüsteemidega. Andmeid on võimalus esitada automaatselt EHISesse, ilma et kasutaja peaks ise läbi kasutajaliidese midagi sisestama. Ainult ligi 35–40 kooli on aga andnud oma õppeinfosüsteemi standardlahenduse pakkujale volituse seda teha. Ülejäänud on otsustanud jätkata kahekordset sisestamist, s.t samad andmed sisestatakse eraldi õppeinfosüsteemi ja EHISesse. Mitmesse kohta käsitsi andmete sisestamine ei ole ainult ajakulukas – selle käigus tekib ka palju vigu.

75. Riigikontrolli hinnangul ei täida praegu RIHA talle seadusega pandud üldist eesmärki, sest senisest märksa enam KOVide andmekogusid peaks olema X-teega liidestatud. Praegu enamikku KOVide andmekogusid RIHAst ei leia.

76. RIHA kooskõlastamise seadusjärgset nõuet ei järgita, kuna selles ei ole võetud arvesse standardlahendustega seotud kasutusjuhte KOVides. Riigikontroll möönab, et praegune kooskõlastuspraktika on mõistlikum kui see, mille seadus ette näeb. Kooskõlastajate ja andmekogu pidajate koormus väheneks, kui avalikule sektorile teenust pakkuvale tarkvara-arendajale laieneks RIHAs registreerimise (sh kooskõlastuse) kohustus.

77. **Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile**: hinnata koostöös Justiitsministeeriumiga avalikule sektorile standard-lahenduste pakkujatele registreerimise kohustuse seadmist RIHAs.

Ettevõtlus- ja infotehnoloogiaministri vastus: Majandus- ja Kommunikatsiooniministeerium peab oluliseks, et avalikule sektorile pakutavad standardlahendused vastaksid asjakohastele turvanõuetele. Peame samuti oluliseks, et andmekogu pidajate kohustused seoses RIHAga oleksid optimaalsed ja realistlikud. Riigikontrolli ettepanekut on kavas käsitleda RIHA protsessi uuendamisel.

Andmete kasutajatele turbenõuete seadmine

Andmeteenuse osutajad ei esita konkreetseid turbenõudeid ega kontrolli oma andmete kasutajaid

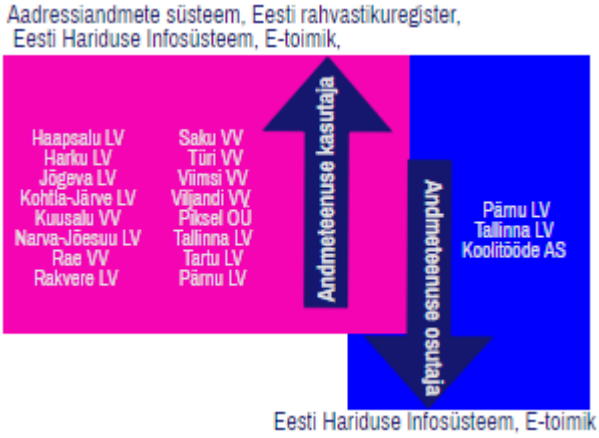
Andmeteenus – X-teega liitunud asutuse või isiku teenus, mille kaudu toimub internetipõhine andmevahetus.

Allikas: Vabariigi Valitsuse määrus nr 105 „Infosüsteemide andmevahetuskiht“, § 2

78. X-teel peab osutama ja kasutama andmeteenust, lähtudes X-tee liikmete kokkuleppest. Selles peab määrama muu hulgas kindlaks andmeteenuse kasutamiseks nõutavad organisatsioonilised, füüsilised ja infotehnilised turvameetmed.[20]

79. Auditi käigus selgus, et KOVide andmekogud on nii põhiandmete andjad teistele andmekogudele kui ka teiste andmekogude põhiandmete kasutajad (vt joonis 13). Riigikontroll uuris, kas andmeteenuse osutajad on sõlminud andmeteenuse kasutamise kokkulepped ja kas neis on selgelt välja toodud infoturvameetmed, mida andmeteenuse kasutaja peab rakendama.

Joonis 13. Auditeeritud riigiregistrites KOVidest andmeteenuse kasutajad ja osutajad



Allikas: Riigikontroll

80. Selgus, et andmeteenuse kasutamise kokkulepped on sõlmitud rahvastikuregistri (213st 15 KOVi) ja EHISe (2 KOVi, 1 standardlahenduse pakkuja) andmeteenuste kasutajatega. Sõlmitud lepingud sisaldavad peamiselt viiteid seadustele ning otsest seost andmetele määratud turbeastmega ega turvameetmeid ei ole välja toodud.

Teadmiseks, et

ADS ehk Maa-ameti aadressiandmete süsteem on riigi infosüsteemi kindlustav süsteem, mille andmeid peab kasutama iga andmekogu, kus töödeldakse aadressiandmeid.

Teatud juhtudel võib oma andmekogu liidestada ADSi infosüsteemiga kaudselt ehk teise teabevaldaja andmekogu kaudu.

Allikas: Vabariigi Valitsuse määrus nr 103 „Aadressiandmete süsteem“, § 4 lg 1; lg 5

81. E-toimik saab andmeid Tallinna ja Pärnu väärteoasjade registrist, kuid kummagagi ei ole Justiitsministeerium andmeteenuse kasutamiseks kokkulepet sõlminud. Aadressiandmete süsteemist (ADS) saavad andmeteenust 3 KOVi ja 1 standardlahenduse pakkuja, kuid kirjalikke lepinguid ADSi X-tee teenuste kasutamiseks seni sõlmitud ei ole.

82. Enne andmeteenuse kasutamise kokkuleppe sõlmimist peab andmeteenuse osutaja olema veendunud, et andmeteenuse kasutaja juba

[20] Vabariigi Valitsuse määrus nr 105 „Infosüsteemide andmevahetuskiht“, § 12 lg 1 p 1; § 12 lg 2 p 2.

rakendab nõutud turbetaset. MKMi sõnul seisneb andmeteenuse osutaja ja kasutaja juures turvameetmete rakendamise kontrollimise mõte selles, et enne oma andmetele juurdepääsu võimaldamist peaks kindlaks tegema, kas teise poole rakendatavad meetmed on n-ö piisavalt head, et ta võiks kogutud andmeid töödelda.

X-tee alamsüsteem on tehnoloogiliselt ja organisatoorselt piiritletud X-tee liikme infosüsteemi osa andmeteenuse osutamiseks või kasutamiseks.

Allikas: Vabariigi Valitsuse määrus nr 105 „Infosüsteemide andmevahetuskiht", § 2

83. MKM on seisukohal, et turbeastmele vastavuses veendumiseks võib tugineda ka RIHA andmetele ja meetmete tegelikku rakendamist enne kokkuleppe sõlmimist kontrollima ei pea. RIA on soovitanud andmeteenuse osutajal ja kasutajal veenduda läbirääkimiste käigus, kas andmeteenuse kasutaja X-tee alamsüsteem on piisava turbetasemega. Täpsemaid juhiseid turbetaseme hindamiseks ei ole antud.

84. Seesugust kontrolli ei olnud teinud ükski auditeeritud andmeteenuse osutaja.[21] Auditeeritud tõid välja, et praegu ei ole selge, miks andmeteenuse osutaja peab läbi viima kontrolli andmeteenuse kasutaja üle, kui viimane täidab ISKE nõudeid, ning kuidas ja mille põhjal andmeteenuse osutaja turvameetmete kontrolli tegema peaks.

85. Lisaks leidsid auditeeritud, et enne lepingulisse suhtesse astumist puudub õigus kontrolli teha. Andmeteenuse osutaja saab küsida ainult teenuse kasutaja kinnitust, et andmeid hoitakse nõutud turbeastme kohaselt. Samuti seati kahtluse alla, kas andmeteenuse osutajal on tegelikult õigus keelduda X-tee vahendusel andmete edastamisest, kui seda on vaja teisel asutusel, et täita avaliku teabe seaduse[22] nõuete kohaselt oma avalikku ülesannet.

86. Auditeeritud andmekogude vastutavad töötlejad[23] arvasid valdavalt, et andmeteenuse kasutaja turvasüsteemi rakendatuse kohta saadakse piisav kindlus ISKE-auditi tulemustega tutvumisel. See aga ei toimi erasektori puhul, sest ISKE rakendamine ei ole kohustuslik, ja KOVides, sest ISKE-auditeid ei ole kuigi palju tellitud. HTM selgitas, et KOVide puhul puudub ka selge arusaam, missugused koolides kasutatavatest infosüsteemidest, millele andmeteenus on avatud, käivad andmekogu mõiste alla, ja sellest tulenevalt, millistel neist peaks olema infoturbe halduse süsteemina kasutusel ISKE. Tähelepanu tuleb pöörata ka sellele, et juba tehtud ISKE-auditile saab tugineda ainult osas, kus turvameetmed kattuvad andmeteenuse osutaja seatud turvameetmetega

87. MKMi antud selgituste kohaselt on kehtiv infosüsteemide andmevahetuskihi määrus loodud pigem erasektori tarbeks, kellele ISKE rakendamine ei ole kohustuslik. Kuna riigi ja KOVi asutused, kellele kohaldub X-tee määrus, on ka ISKE määruse subjektid, siis nendele X-tee määrusega täiendavate kontrollinõuete sätestamine on praktikas üleliigne.

88. Riigikontrolli arvates ei ole avalikus sektoris enne andmeteenuse kokkuleppe sõlmimist realistlik kontrollida, kas KOVidest andmeteenuse kasutajad on täitnud kohustuse rakendada turvameetmete süsteem. Samuti on praktikas üleliigne määrata iga andmeteenuse kasutamise kokkuleppe sõlmimise juhul konkreetsetele andmetele nõutavad spetsiifilised turvameetmed, kui avalikus sektoris rakendatakse juba niigi ISKE-metoodikat. Samas on selge, et kui andmeteenuse kasutamise kokkuleppe

[21] Maa-amet, Siseministeerium, Haridus- ja Teadusministeerium.
[22] Avaliku teabe seadus, § 43^9 lg 5.
[23] Maa-amet, Siseministeerium, Haridus- ja Teadusministeerium, Justiitsministeerium.

teine pool on erasektor, siis ei saa jätta turvameetmete määramise kohustust sätestamata, kuna erasektorile ISKE ei rakendu.

89. **Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile:** täpsustada Vabariigi Valitsuse määrust nr 105 „Infosüsteemide andmevahetuskiht“ nii, et oleks üheselt selge, kellele ja mis osas määrus kohaldub, ning veenduda, et sellega ei loodaks andmeteenuse osutajatele ja kasutajatele dubleerivaid kohustusi (mh tuleks arvestada ka olukorraga, kus KOV on andmeteenuse osutaja riigiregistritele).

Ettevõtlus- ja infotehnoloogiaministri vastus: Majandus- ja Kommunikatsiooniministeerium võtab arvesse Riigikontrolli soovitust Vabariigi Valitsuse määruse nr 105 „Infosüsteemide andmevahetuskiht“ ajakohastamisel.

Järelevalve KOVides

Seni on riiklikku järelevalvet turvameetmete süsteemi rakendamise üle omavalitsustes tehtud vähe

90. Riigikontroll analüüsis riiklikku järelevalvet tegevate asutuste viimaste aastate tööplaanide täitmist, selle tulemeid ning seda, millised tegevused on plaanis tuleval aastal.

91. RIA 2016. ja 2017. aasta tööplaani järgi oli ette nähtud teha järelevalvet infoturbenõuete täitmise üle KOVides. Kuigi kontrollitoiminguid tehti vaid mõnes üksikus KOVis, on sellega tööplaan siiski täidetud. AKI tööplaaniga ette nähtud tegevused 2016. aastal olid enamasti teavitava iseloomuga: korraldati seminare ja infopäevi ning saadeti ringkirju. Kahel viimasel aastal tehti kontrolli asutusesiseseks kasutamiseks mõeldud teabe (sh turvameetmete) üle ja kontrolli käigus külastati ka nelja KOVi. Samas otsustas nii RIA kui ka AKI, et ühinemiste tõttu ei ole mõtet väiksemates KOVides kontrolle teha.

92. RIA-l on plaanis 2018. aastal järelevalvetoiminguid teha suuremates linnades (Tallinn, Tartu, Pärnu jt). AKI ei olnud Riigikontrolli auditi toimingute ajaks veel tööplaani planeerinud konkreetselt KOVides tehtavat järelevalvet. KOVide sattumine inspektsiooni järelevalve objektiks on pigem juhuslik, sest tegevusi kavandatakse valdkondade järgi. Näiteks pandi 2017. aastal rõhk tervishoiuvaldkonna kontrollile. Tihti selgub aga vajadus kontrollida infoturbenõuetest kinnipidamist alles siis, kui ollakse juba kohapeal toiminguid tegemas või reageeritakse kaebustele.

Rikkumistele reageerimine

93. Nii AKI-l kui ka RIA-l on õigus teha ettekirjutusi, kui KOV ei rakenda andmete kaitseks organisatsioonilisi, füüsilisi ega infotehnilisi turvameetmeid. AKI võib teha ettekirjutusi isikuandmete kaitse seaduse rikkumiste[24] puhul ning RIA siis, kui ei rakendata ISKEt või X-tee määrust.[25]

94. Auditi käigus selgus, et RIA ei ole seni KOVidele ühtegi ettekirjutust teinud. Samas on RIA oma kontrollkäikudel rikkumisi rohkem kui ühel korral tuvastanud ja infot, mille alusel on põhjendatud ettekirjutuse tegemine, võib saada ka mujalt (nt Euroopa Liidu toetusraha kasutamise järelevalve käigus, RIHAsse registreerimisel esitatud andmete alusel).

[24] Isikuandmete kaitse seadus, § 40 lg 1.
[25] Avaliku teabe seadus, § 53[1] lg 1.

AKI ei osanud välja tuua, kas üldse või kui palju on KOVidele isikuandmete kaitse seaduses sätestatud turbenõuete rikkumiste tõttu ettekirjutusi tehtud.

95. Riigikontrolli hinnangul, võttes arvesse auditeeritud KOVides infoturbe olukorra kohta tehtud tähelepanekuid, peab järelevalve KOVides olema senisest tõhusam. Praktikas on mitmeid probleeme, mille põhjuseks võib pidada ka vähesest järelevalvest tingitud ükskõiksust KOVides, sh andmekogude RIHAs registreerimata jätmine, andmete topelt kogumine elanikelt ja ettevõtjatelt, andmete vahetamiseks selleks ettenähtud X-tee mittekasutamine, turvameetmete süsteemi kehv rakendamine.

96. Riigikontrolli soovitus Riigi Infosüsteemi Ameti peadirektorile ja Andmekaitse Inspektsiooni peadirektorile: tõhustada kontrolli KOVides turvameetmete süsteemi rakendamise, X-teega liitumise ning RIHAs registreerimise üle.

Riigi Infosüsteemi Ameti peadirektori vastus: Riigi Infosüsteemi Amet on turvameetmete rakendamise kontrollimisega (sh X-tee) kohalikes omavalitsustes tegelenud ning jätkab sellega tegelemist vastavalt riskihinnangutest tulenevale prioriteetsusele. Kohalike omavalitsuste kontrollimine haldusreformi järel oli RIA plaanides juba varem, seega võib öelda, et antud soovitus on juba täitmisel.

Andmekaitse Inspektsiooni peadirektori vastus (refereeritud): AKI pädevuses on teha järelevalvet nii isikuandmete kaitse seaduse (IKS) kui ka osa avaliku teabe seaduse (AvTS) nõuete täitmise üle. AKI leiab, et kohati on raske täita asutusesiseseks kasutamiseks mõeldud teabe kaitsmise ülesannet, kuna seni ei ole Vabariigi Valitsus vastu võtnud AvTS-i § 43 lg 3 alusel määrust, millega kehtestatakse asutusesisese teabe kaitseks rakendatavate turvameetmete loetelu. Selle asemel on AKI enda avaliku teabe seaduse üldjuhendis sisustanud ja selgitanud nende nõuete täitmist.

AKI ei tee avaliku sektori asutustes järelevalvet ISKE nõuete rakendamise üle. Inspektsiooni pädevuses on teha järelevalvet andmekogude üle. AvTS § 43^3 lg 3 kohaselt kooskõlastatakse andmekogu tehniline dokumentatsioon RIHA kaudu AKIga. AKI selgituste kohaselt on neil järelevalveks 18 täidetud ametikohta, kuid järelevalve subjektide ja peetavate andmekogude arv on liiga suur, et kõigiga jõuaks tegeleda. Töökoormust mõjutab ka selle aasta mais jõustunud isikuandmete kaitse üldmäärus ning sellega koos ka uus isikuandmete kaitse seadus. AKI prognoosi kohaselt mõjutavad sellega seotud muudatused vähemalt 2018. aasta toimetusi. Seetõttu tegeletakse Riigikontrolli soovituse täitmisega võimalustest lähtudes.

Teavitustegevused ei ole toonud loodetud tulemusi

Teavitustegevus KOVides

97. Mõlemad järelevalveasutused selgitasid, et enamasti on rikkumised põhjustatud teadmatusest või oskamatusest kasutusel oleva infosüsteemi funktsioone kasutada. Riigikontroll uuris auditi käigus, mida on infoturbe valdkonnas teadlikkuse suurendamiseks ette võetud ning milline on olnud auditeeritud KOVide osalus selles.

Teadmiseks, et

RIA on käivitanud ka **küberhügieeni e-õppekeskkonna**, kuhu saavad asutused ennast registreerida ja oma teadlikkust testida.

Esimesena KOVidest katsetati seda Tartu Linnavalitsuses.

Allikas: uudisteportaal Geenius (2017)

98. Auditi käigus selgus, et riik on korraldanud arvukalt tegevusi, selleks et teadlikkust infoturbe valdkonnas suurendada, sh

- RIA infoturbe intsidentide käsitlemise osakonna CERT-EE jooksvad teavitused turvanõrkuste kohta;
- RIA korraldatud koolitused ISKE rakendamiseks;
- infoturbejuhtide komisjoni vedamine;
- RIA koolitused kontrollkäikude osana;
- AKI avaliku teabe päevad;
- AKI dokumendiregistrite seire ning parimate tunnustamine;
- esinemised iga-aastastel linnade ja valdade päevadel;
- saadetud märgukirjad, ringkirjad;
- koostatud juhendmaterjalid.

99. Euroopa Liidu eelmisel rahastamisperioodil panustati infoühiskonnateemalistesse koolitustesse, konverentsidesse, teabepäevadesse jms ligi 2 miljonit eurot.

100. Kõik auditeeritud KOVid kinnitasid Riigikontrollile, et nad on saanud RIA koolituste kutseid. Auditeeritud KOVidest enamik oli vähemalt korra RIA korraldatud koolitusel[26] osalenud. Koolitustel mitteosalemise põhjuseks toodi, et need on liiga spetsiifilised IT-valdkonna välisele inimesele, tihti korraldatakse neid Tallinnas, tööülesannete kõrvalt ei ole aega koolitustel osaleda, koolitustel ei jagu alati kohti.

101. Auditeeritud KOVide ametnikud on osalenud ka riigiregistrite kasutajate koolitustel. Uurides auditeeritavate osalust koolitustel, selgus, et näiteks rahvastikuregistri koolitusel on aastatel 2015–2016 käinud kõik peale ühe auditeeritud KOVi.

102. Riigikontrolli hinnangul on teavitustegevused olnud KOVidele kättesaadavad, aga infoturbe olukord ei ole sellest paranenud. Põhjus võib olla selles, et senine sihtrühm, kes koolitustel on käinud, on olnud IT-spetsialistid. Samas jääb RIA sõnutsi juhtkonna vähene osalus koolitustel ka huvipuuduse taha. Seetõttu ei ole asutuse juhtkond koolitustel osalenud ja juhtideni ei ole jõudnud teadmised infoturbe meetmete rakendamise olulisusest.

103. **Riigikontrolli soovitus Riigi Infosüsteemi Ameti peadirektorile**: propageerida IT-spetsialistidele mõeldud koolituste kõrval rohkem KOVi juhtkonnale suunatud koolitusi või teha laiemat teavitust, mh kaaluda uute linna- ja vallajuhtide jaoks koolitusprogrammi väljatöötamist.

Riigi Infosüsteemi Ameti peadirektori vastus (refereeritud): Riigi Infosüsteemi Amet tänas Riigikontrolli selle soovituse eest ning rõhutas, et on soovitusega igati nõus. Ka RIA on oma toimingute käigus korduvalt

[26] Riigikontrollile on edastatud aastatel 2010–2013 koolitusel „Infoturbe sissejuhatus“ ja 2017. aasta koolituse „Infoturbe halduse koolitus ISKE baasil“ osalejate nimekirjad.

leidnud, et asutuste tippjuhtide teadlikkus infoturbest ning motiveeritus sellega tegeleda võiks olla parem. Sellest tulenevalt on tippjuhtide huvi sellistel koolitustel osaleda vähene ning seetõttu võiks Riigikontrolli soovitus olla pigem suunatud omavalitsuste juhtidele.

Tippjuhtide koolitustega, kus osalesid peamiselt avaliku sektori juhid, alustas RIA juba 2017. aastal. 2018. aastal on kavas korraldada infoturbeteadlikkuse suurendamise, ISKE jm tasuta koolitusi ka kohalikele omavalitsustele ja nende juhtidele. Teave nende koolituste kohta on edastatud muu hulgas linna- ja vallasekretäride e-posti listi ning Eesti Maaomavalitsuste Liidu esindajatele.

2018. a II poolaastast kuni 2019. aastani hakkavad RIA küberturvalisuse teenistuse töötajad muu hulgas külastama kohalikke omavalitsusi, et suurendada koostööd ja parandada omavalitsuste juhtkondade teadlikkust, sh selgitada välja nende vajadus nõustamise, koolitamise jms järele. 2018. a II poolaastal plaanitakse kohalike omavalitsuste esindajaid kaasata infoturbejuhtide komisjoni töösse.

Infoturbe valdkonna toetamise tegelik mõju omavalitsustes ei ole teada

104. Infoturbe järelevalve ja teavitustöö kõrval analüüsiti auditis ka KOVidele jagatud toetusi, et selgitada välja, kui palju on riik seni KOVide infoturbesse investeerinud ning kas toetuste mõju on hinnatud tulemuslikuks.

105. Perioodil 2007–2013 rahastati IT-turvalisuse taseme tõstmist KOVides mitme taotlusvooru ja projekti raames:

- 2008. aastal toetati KOVe ligi 500 000 euroga (KOVISKE ehk omavalitsuse infosüsteemide turvameetmete tõhustamine).
- 2012. aasta rahastati KOVide IT-turvalisuse taseme tõstmist ligi 300 000 euroga.
- 2013. aastal viidi ISKE-auditeid läbi 5 KOVis kogusummas 20 880 eurot.

106. Kogu perioodi vältel toetatud tegevused hõlmasid nii ISKE nõuetele vastava dokumentatsiooni loomist (sh infoturbepoliitika, turvameetmete rakendusplaan) kui ka turvameetmete rakendamiseks vajalike seadmete ostmist (sh tulemüür, hallatav võrgulüliti (*switch*), seadmekapp).

107. Enim KOVe (122) hõlmanud projekt oli perioodil 2008–2010 läbi viidud KOVISKE. Taotlusvooru eesmärk oli, et asutused võtaksid vastavalt ISKE turvaklassile kasutusele vajalikud ja piisavad turvameetmed. Projekti lõppedes oli ootus, et saadud kogemusest lähtudes oskavad KOVid tulevikus hankida turvanõuetele vastavaid seadmeid ja lahendusi ise ning teevad seda ka ühiselt.

108. Riigikontrolli auditisse oli kaasatud kuus KOVISKE-projektis osalenud KOVi. Selgus, et selle projekti käigus loodud dokumentatsioon oli jäetud KOVide juhtkonnal kinnitamata, see oli 2010. aastast alates muutmata või päriselus jõustamata. Sama on toodud välja ka ISKE-auditites ja RIA hilisemate kontrollkäikude põhjal tehtud tähelepanekutes.

KOVide IKT-kompetentsikeskus – 16.05.2016 sõlmisid KOVide infotehnoloogia arendamise toetamiseks ja koordineerimiseks Rahandusministeerium, MTÜ Linnade Liit ja MTÜ Eesti Maaomavalitsuste Liit lepingu. Lepingu alusel on määratud keskne vastutaja (projektijuht), kes esindab KOVe infotehnoloogilistes küsimustes läbirääkimistel keskvalitsusega ning on kontaktisikuks KOVidele infotehnoloogilistes küsimustes

Allikas: Rahandusministeerium

109. Eelmisel aastal lõpule jõudnud KOVide IKT-kompetentsikeskuse andmekorje KOVides näitas, et paljudes kohtades on endiselt kasutusel seadmed, mis said sinna projekti raames paigaldatud ligi 10 aastat tagasi. 2011. aastast pärineva Siseministeeriumi küsitluse andmete kohaselt ei uuenda KOVid järjepidevalt oma IKT-töövahendeid, vaid planeerivad sellised suuremad investeeringud, kui saavad välisrahastuse.

110. Kuigi Euroopa Liidu toetusraha kasutamise tulemuslikkust KOVide infoturbetaseme olukorra parandamisel ei ole hinnatud, ei pea MKM ega Rahandusministeerium sellist toetust kuigi jätkusuutlikuks lahenduseks, mille abil tagada KOVide IKT-taristu ISKE nõuetega vastavus pikemaks ajaks. ISKE rakendamine ei saa sõltuda Euroopa Liidu toetusraha olemasolust.

111. Lisaks on MKM intervjuus Riigikontrollile öelnud, et ei poolda KOVide eraldiseisvaid üksikuid arendusi ja seadmete ostu, kui riik on juba välja arendanud nõuetele vastava taristu (nt riigipilv) ja ühislahendused (nt VOLIS, KOVTP, ruumilise planeeringu infosüsteem RPIS), mida võiksid kasutada kõik KOVid.

112. Riigikontrolli hinnangul aitab ISKE nõuete vastavusse viimisele riigi sihtotstarbeline toetus kindlasti kaasa, kuid olemuslikult ei saa infoturbetaseme hoidmine jätkuda n-ö kampaaniapõhiselt ega sõltuda välisrahastusest.

113. **Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile:** toetusmeetmete tingimuste koostamisel võtta arvesse, et need motiveeriks kasutusele võtma lahendusi, mis riik või mõni teine KOV on juba maksumaksja raha eest loonud.

Ettevõtlus- ja infotehnoloogiaministri vastus: Majandus- ja Kommunikatsiooniministeerium lähtub juba tänasel päeval üldisest põhimõttest, mille kohaselt eelistatakse IT-lahenduste ühiskasutust ja -arendust. Toetusmeetmete tingimuste koostamisel ja ülevaatamisel lähtub MKM ka edaspidi nendest põhimõtetest.

Riigikontrolli hinnang auditeeritud omavalitsustele

Kokkuvõte auditis antud hinnangute kohta on toodud tabelis 2. Täpsed hinnangud kriteeriumite täitmise kohta on Riigikontroll edastanud auditeeritud KOVidele eraldi.

Kokku anti hinnang 129 kriteeriumile, mis valiti välja 85-st ISKE kataloogi turvameetmest (neist 3 soovituslikku, millele hinnangut ei antud). 35% kõigist hinnangutest olid positiivsed ja 50% negatiivsed ning 15%-l juhtudest kriteerium ei kohaldunud ja hinnangut ei saanud anda.

Kriteeriumeid, mis kirjeldasid meetmete planeerimist (sh dokumentatsiooni loomist), oli kokku 42 ja neid, mis kirjeldasid nende rakendamist, 87. Planeerimist puudutavate meetmete hinnangud jagunesid järgmiselt: 50% negatiivseid ja 50% positiivseid. Rakendamist puudutavate meetmete hinnangutest oli 38% negatiivseid ja 62% positiivseid.

Tabel 2. Kokkuvõte tüüpmoodulis saadud hinnangute kohta (%)

Tüüpmoodul	Kriteeriumite arv	Hinnang	Kohtla-Järve linn	Avinurme vald	Audru vald	Vihula vald	Võru vald	Paide linn	Valga linn	Viljandi vald	Kuusalu vald	Rapla vald
1.0. Infoturbe haldus	14	Positiivne	0	14	7	21	29	14	29	0	36	43
		Negatiivne	43	36	43	50	43	36	43	43	36	29
		Ei kohaldu*	57	50	50	29	29	50	29	57	29	29
1.1. Organisatsioon	18	Positiivne	56	61	94	56	72	50	61	50	72	89
		Negatiivne	39	28	6	28	22	22	28	33	11	6
		Ei kohaldu	6	11	0	17	6	28	11	17	17	6
1.2. Personal	16	Positiivne	69	50	88	63	44	50	50	56	56	81
		Negatiivne	19	44	6	25	50	31	38	19	38	13
		Ei kohaldu	13	6	6	13	6	19	13	25	6	6
1.4. Andmevarunduspoliitika	11	Positiivne	55	64	73	64	45	55	45	36	55	73
		Negatiivne	36	36	18	18	45	36	55	55	45	18
		Ei kohaldu	9	0	9	18	9	9	0	9	0	9
1.6. Viirusetõrje kontseptsioon	10	Positiivne	40	30	60	50	50	80	70	50	90	70
		Negatiivne	30	40	30	20	40	10	20	20	10	20
		Ei kohaldu	30	30	10	30	10	10	10	30	0	10
1.8. Turva-intsidentide käsitlus	5	Positiivne	40	40	40	20	40	100	100	20	40	40
		Negatiivne	60	0	0	20	0	0	0	20	0	0
		Ei kohaldu	0	60	60	60	60	0	0	60	60	60
1.9. Riist- ja tarkvara haldus	26	Positiivne	27	42	62	42	42	62	50	58	50	69
		Negatiivne	69	54	35	54	54	38	46	35	46	31
		Ei kohaldu	4	4	4	4	4	0	4	8	4	0
1.11. Väljastellimine	7	Positiivne	57	43	43	29	57	57	43	57	57	43
		Negatiivne	43	43	43	71	29	29	43	29	29	43
		Ei kohaldu	0	14	14	0	14	14	14	14	14	14
	5	Positiivne	0	0	40	20	40	20	20	20	40	0

1.13. Infoturbe-teadlikkus ja -koolitus		Negatiivne	80	80	40	60	40	60	60	60	40	80
		Ei kohaldu	20	20	20	20	20	20	20	20	20	20
3.301. Turva-lüüs (tulemüür)	4	Positiivne	0	0	50	25	0	75	25	25	0	0
		Negatiivne	25	50	0	25	50	25	75	75	25	50
		Ei kohaldu	75	50	50	50	50	0	0	0	75	50
1.10. Tüüp-tarkvara	2	Positiivne	50	0	50	100	0	50	0	50	50	0
		Negatiivne	50	100	50	0	100	50	100	50	50	100
		Ei kohaldu	0	0	0	0	0	0	0	0	0	0
1.14. Turva-paikade ja muudatuste haldus	4	Positiivne	50	50	100	100	25	100	25	75	50	100
		Negatiivne	50	25	0	0	50	0	50	25	25	0
		Ei kohaldu	0	25	0	0	25	0	25	0	25	0
3.201. Klient	1	Positiivne	100	0	100	100	100	100	100	100	0	100
		Negatiivne	0	100	0	0	0	0	0	0	100	0
		Ei kohaldu	0	0	0	0	0	0	0	0	0	0
3.302. Marsruuterid ja kommutaatorid	1	Positiivne	100	100	100	100	100	100	100	100	100	100
		Negatiivne	0	0	0	0	0	0	0	0	0	0
		Ei kohaldu	0	0	0	0	0	0	0	0	0	0
5.7. Andme-baasid	3	Positiivne	0	0	33	33	0	100	33	0	0	67
		Negatiivne	100	100	67	67	100	0	67	100	67	0
		Ei kohaldu	0	0	0	0	0	0	0	0	33	33
2.4. Serveri-ruum	2	Positiivne	50	50	50	0	0	50	50	50	50	100
		Negatiivne	50	50	50	100	100	50	50	50	0	0
		Ei kohaldu	0	0	0	0	0	0	0	0	50	0

* Ei kohaldu on märgitud hinnanguks juhul, kui auditeeritule ei saanud kriteeriumi alusel hinnangut anda (nt puudus dokument või ei olnud kasutusel seadet, mille vastavust kriteeriumile hinnata).

/allkirjastatud digitaalselt/

Ines Metsalu-Nurminen
auditiosakonna peakontrolör

Riigikontrolli soovitused ja auditeeritute vastused

Riigikontroll andis auditi põhjal Majandus- ja Kommunikatsiooniministeeriumile, Riigi Infosüsteemi Ametile, Andmekaitse Inspektsioonile ning auditeeritud kohalikele omavalitsustele mitmeid soovitusi. Minister, peadirektorid ja omavalitsused saatsid ajavahemikul 24.04.–23.05.2018 oma vastused Riigikontrolli soovitustele. Vastuste täistekstid on toodud lisas A.

Üldised kommentaarid auditiaruande kohta
Rapla Vallavalitsus: Rapla Vallavalitsus, tutvunud Riigikontrolli kontrolliaruande „IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes“ kavandiga, nendib, et auditis käsitletud teemade ring on omavalitsuste tasandil oluline ning annab sisuka ülevaate valdkonna probleemidest, võimalikest põhjustest ning lahendustest. Nõustume Riigikontrolli seisukohtadega, et kohalikus omavalitsuses on IT-turvameetmetele liialt vähe tähelepanu pööratud ja süsteemi rakendamine jäänud tagaplaanile. Vallavalitsus on teinud oma järeldused ning alustanud abinõude kavandamist auditeerimise käigus esinenud puuduste kõrvaldamiseks, samuti tehtud soovituste arvestamiseks kohaliku omavalitsuse edaspidises tegevuses.

Riigikontrolli soovitused	Auditeeritute vastused
Vastutuse ulatus ja kaasnevad nõuded andmete töötlemisel **29. Riigikontrolli soovitused auditeeritud KOVidele:** ▪ veenduda andmekogu tarkvaralahenduse valimisel, et tarkvaralahendus on vajaduse korral liidestatav X-teega ning et standardlahenduse turbeaste vastaks sinna sisestatavate andmete turbeastmenõudele; ▪ leppida lepingus teenuseosutajaga kokku, millised turvameetmed peavad olema rakendatud ja milline on turvameetmete auditeerimise korraldus. **p-d 15–29**	**Rapla Vallavalitsuse vastus:** Uue kohaliku omavalitsuse üksuse ameti-asutuse moodustamisega kaasneb ka andmekogude tarkvaralahenduse pakkujatega sõlmitud lepingute ülevaatamine ja uute lepingute sõlmimine. Protsessi käigus arvestame Riigikontrolli esitatud soovitustega. **Kohtla-Järve Linnavalitsuse vastus:** Teatame, et püüame viia vastavusse eelnõus esitatud soovitused ning tegeleme puuduste kõrvaldamisega. **Kuusalu Vallavalitsuse vastus:** Kuusalu vallavalitsus arvestab soovitustega uute tarkvaralahenduste valikul ja lepingute sõlmimisel. Peame oluliseks koostööd teiste omavalitsustega nii Eesti Linnade ja Valdade Liidu raames kui ka omavahelisi kontakte. Soovime teenuseosutajaga läbirääkimisi pidades arvestada ka teiste omavalitsuste kogemusega ja teha nendega koostööd. **Valga Vallavalitsuse vastus:** Valga vallale on auditiga välja toodud puudujäägid ja soovitused arusaadavad. Tarkvaralahenduste valimisel jälgime edaspidi, et tegu oleks riiklike andmekogudega X-Tee vahendusel liidestatava süsteemiga; jälgime, et tarkvarateenuse osutajatega oleks sätestatud turbemeetmete rakendamise ja auditeerimise korraldus; ISKE rakendamise kohustusliku osana määrame infoturbejuhi kas oma töötajatest või tellime teenusena sisse. **Haljala Vallavalitsuse vastus:** Haljala vallavalitsus arvestab edaspidi Riigikontrolli ettepanekutega järgida andmekogude kasutuselevõtul või uute andmekogude loomisel, et tarkvaralahenduse pakkuja teenuse turbeaste ja rakendatavad turvameetmed vastaksid andmekogusse sisestatavate andmete turbeastmenõuetele ning et teenuseosutaja pakutav lahendus oleks liidestatav X-teega.
30. Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile: hinnata, kas ministeeriumid saavad seadusega ära määrata ka andmete turvaklassi andmekogu(de) puhul, mille pidamist nõutakse KOVilt kohustusliku ülesande täitmiseks. **p-d 22–23**	**Ettevõtlus- ja infotehnoloogiaministri vastus:** Majandus- ja Kommunikatsiooniministeerium peab mõistlikuks, et sarnaste või ühetaoliste andmekogude turvaklassi määramine lähtuks ühtsetest alustest ning toimuks dubleerivate protseduurideta. Riigi infosüsteemi seisukohalt on optimaalne korraldus, kus infosüsteemid on üleriigilised ning KOVid teevad sinna kandeid. Juhul, kui seadusandja on siiski ette näinud, et iga KOV peab ise mingit registrit pidama, siis tuleb kindlasti hinnata kõikvõimalikke meetmeid, kuidas sellise andmekogu pidamisele kaasa aidata, kaasa arvatud ühtse lähenemise kujundamine turvaklassi määramisele ning turvameetmete rakendamisele.
Infoturbe planeerimise ja rakendamise seis omavalitsustes **46. Riigikontrolli soovitused ettevõtlus- ja infotehnoloogiaministrile:**	**Ettevõtlus- ja infotehnoloogiaministri vastus:** Majandus- ja Kommunikatsiooniministeerium adresseerib Riigikontrolli tõstatud probleeme ISKE määruse uuendamisel ja ISKEga seotud juhendite ja materjalide läbivaatamisel. Küberturvalisuse seadusega laieneb turvameetmete

Riigikontrolli soovitused	Auditeeritute vastused
▪ analüüsida põhjuseid, miks turvameetmete süsteemi rakendamine KOVides on pikalt viibinud ning sellest tulenevalt töötada välja tegevused ISKE rakendamise paindlikumaks muutmiseks (sh kaaluda standardsete tarkvaralahenduste osutajatele ISKE-auditi läbimise kohustuse seadmist) KOVides nii, et see oleks rohkem kohapealseid olusid arvestav. ▪ muuta ISKE-auditi tellimise korraldust (sh ISKE-auditi juhendit) nii, et selle tellimine oleks järjepidevalt tagatud. ▪ algatada Rahandusministeeriumiga ISKE-auditite tellimise rahastuse läbirääkimised. **p-d 31–45**	rakendamise kohustus ka teistele infosüsteemidele lisaks nendele, mida kasutatakse andmekogude pidamisel (01.01.2020). ISKE määrus, juhendid ja materjalid vajavad eelnevat kaasajastamist selle muudatuse realiseerimiseks. Riigikontrolli tõstatud küsimusi on otstarbekas käsitleda koos küberturvalisuse seadusest tingitud muudatustega. MKM nõustub, et senine korraldus KOVide ISKE auditite tellimiseks on ebaõnnestunud.
Omavalitsuste infoturbekultuur **62. Riigikontrolli soovitus auditeeritud KOVidele**: määrata infoturbejuhi ülesannete täitja või tellida infoturbejuhtimine teenusena sisse, et oleks tagatud piisav tähelepanu IT-turvalisusega seotud aspektidele. **p-d 47–61**	**Rapla Vallavalitsuse vastus:** Haldusreformi järel on uus moodustunud kohalik omavalitsus senisest võimekam ja mehitatud valdkonnas pädevate spetsialistidega, saavutamaks auditeeritud valdkonnas senisest tõhusam infoturbe juhtimine, turvameetmete rakendamine, kaitse võimalike intsidentide ja rünnete vastu ning teenistujate parem infoturbeteadlikkus. **Kohtla-Järve Linnavalitsuse vastus:** Teatame, et püüame viia vastavusse eelnõus esitatud soovitused ning tegeleme puuduste kõrvaldamisega. **Kuusalu Vallavalitsuse vastus:** Kuusalu vallavalitsuses on IT-turbe alal toimumas oluline areng. Kuusalu vald osaleb Rahandusministeeriumi Infotehnoloogiakeskuse (RMIT) projektis „KOV-de IKT baastaristute uuendamine ISKE nõuetele“. Projekti käigus võetakse kasutusse ajakohane võrguseadmestik ja RMITis majutatud serveripark ning grupitöölahendus ja e-posti süsteem, samuti KOVi infosüsteemi taastamiseks sobilik taastelahendus. Omavalitsusele luuakse sõltumatult administreeritavad virtuaalserverid, millel toimib keskselt korraldatud IT-haldus (keskne autentimine, keskne grupitöölahendus, keskne arvutite haldus). Koostatakse IKT-taristu ja ISKE dokumentatsioon. Tekivad eeldused taristu haldamises vajadusel teenusepõhisele mudelile üleminekuks. Projekti tegevused on planeeritud läbi viia 2018. aasta jooksul. Kuusalu Vallavalitsuse infoturbe tegevuse teostamine ja korraldamine on ametijuhendi järgi praegu IT-arendusjuhi ülesanne. Projekti „KOV-de IKT baastaristute uuendamine ISKE nõuetele“ täitmise käigus hindame infoturbejuhi ülesannete täitmiseks vajalikku töömahtu ja kompetentsi ja lahendame infoturbejuhi ülesannete täitja valiku parimal võimalikul viisil. **Mustvee Vallavalitsuse vastus:** Mustvee Vallavalitsuses on praeguseks personal komplekteeritud. Teenistujad on osalenud erinevatel infoturbe-koolitustel. Vallavalitsus osaleb pilootprojektis „KOV IKT taristu“, millega arendame ISKE-le vastava turvalise internetivõrgu. Andmevarundus kolib RMITi serverisse. Hetkel on käimas arvutihange, millega viime arvutipargi vastavusse ISKE nõuetega. Koostamisel on infoturbedokumentatsioon. **Valga Vallavalitsuse vastus:** Valga linnas oli tööl üks IT-spetsialist, kes tegeles kogu IT-ga, sealhulgas jõudumööda ISKE nõuete jälgimise ja täitmisega. Suur osa esinenud puudusi on tulenenud aja- ja ressursi-puudusest. Valga vallavalitsuses on ühinemisperioodiks (2017–2018) tähtajaliselt tööl poole kohaga IT-arendusjuht. Tema tööülesandeks on muu hulgas ellu viia ja koordineerida ISKE rakendamist ja infoturbe põhimõtete väljatöötamist. Eeldame, et 2018. a lõpuks on Valga vallas ISKE seisukohalt olukord paranenud ja puudused likvideeritud. **Haljala Vallavalitsuse vastus:** Andmekaitse ja infoturbe korraldamine on hetkel vallasekretäri ametiülesanne (ametijuhend kinnitatud 15.04.2013). Edaspidi peame siiski otstarbekamaks tellida infoturbe ülesannete täitmine sisse teenusena. **Võru Vallavalitsuse vastus:** KOVis on ISKE meetmestiku rakendamine hädavajalik infovarade turvalisuse tagamiseks. Võru Vallavalitsus võtab Riigikontrolli soovitused kuulda ning on asunud olukorda parandama, olles esiteks määranud infoturbega seotud ülesannete täitja ning teadvustanud olukorra tõsidust juhtkonna tasandil. Hetkel on käsil kaasaegse infoturbe-poliitika väljatöötamine ning siit edasi jätkatakse järk-järgult ISKE rakendamist.

Riigikontrolli soovitused	Auditeeritute vastused
Omavalitsuste ja riigi andmekogude vaheline andmete vahetus **77. Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile**: hinnata koostöös Justiitsministeeriumiga avalikule sektorile standardlahenduste pakkujatele registreerimise kohustuse seadmist RIHAs. **p-d 63–76**	**Ettevõtlus- ja infotehnoloogiaministri vastus:** Majandus- ja Kommunikatsiooniministeerium peab oluliseks, et avalikule sektorile pakutavad standardlahendused vastaksid asjakohastele turvanõuetele. Peame samuti oluliseks, et andmekogu pidajate kohustused seoses RIHAga oleksid optimaalsed ja realistlikud. Riigikontrolli ettepanekut on kavas käsitleda RIHA protsessi uuendamisel.
Andmeteenuse osutaja ülesanded **89. Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile**: täpsustada Vabariigi Valitsuse määrust nr 105 „Infosüsteemide andmevahetuskiht“ nii, et oleks üheselt selge, kellele ja mis osas määrus kohaldub, ning veenduda, et sellega ei loodaks andmeteenuse osutajatele ja kasutajatele dubleerivaid kohustusi (mh tuleks arvestada ka olukorraga, kus KOV on andmeteenuse osutaja riigiregistritele). **p-d 78–88**	**Ettevõtlus- ja infotehnoloogiaministri vastus:** Majandus- ja Kommunikatsiooniministeerium võtab arvesse Riigikontrolli soovitust Vabariigi Valitsuse määruse nr 105 „Infosüsteemide andmevahetuskiht“ ajakohastamisel.
Järelevalve turvameetmete süsteemi rakendamise üle omavalitsustes **96. Riigikontrolli soovitus Riigi Infosüsteemi Ameti peadirektorile**: tõhustada kontrolli KOVides turvameetmete süsteemi rakendamise, X-teega liitumise ning RIHAs registreerimise üle. **p-d 90–95**	**Riigi Infosüsteemi Ameti peadirektori vastus:** Riigi Infosüsteemi Amet on turvameetmete rakendamise kontrollimisega (sh X-tee) kohalikes omavalitsustes tegelenud ning jätkab sellega tegelemist vastavalt riskihinnangutest tulenevale prioriteetsusele. Kohalike omavalitsuste kontrollimine haldusreformi järel oli RIA plaanides juba varem, seega võib öelda, et antud soovitus on juba täitmisel.
96. Riigikontrolli soovitus Andmekaitse Inspektsiooni peadirektorile: tõhustada kontrolli KOVides turvameetmete süsteemi rakendamise, X-teega liitumise ning RIHAs registreerimise üle. **p-d 90–95**	**Andmekaitse Inspektsiooni peadirektori vastus:** Tänan selle esitatud soovituse eest, kuid ma pean esmalt märkima, et inspektsiooni pädevuses on järelevalve teostamine nii isikuandmete kaitse seaduse (IKS) kui ka osa avaliku teabe seaduse (AvTS) nõuete täitmise osas. Paljuski on nende kahe seaduse kokkupuutepunkt kattuv: IKSi alusel kontrollime isikuandmete kaitseks rakendatavaid organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid ning AvTS-i alusel kontrollime asutusesiseseks kasutamiseks mõeldud teabe kaitsmist. Märgin, et viimase ülesande täitmist on kohati ka raskendatud teha, kuna senini ei ole Vabariigi Valitsus vastu võtnud AvTS-i § 43 lg 3 alusel määrust, millega kehtestatakse asutusesisese teabe tervikluse, käideldavuse ja konfidentsiaalsuse kaitseks rakendatavate organisatsioonilise, füüsiliste ja infotehniliste turvameetmete loetelu. Selle asemel oleme enda avaliku teabe seaduse üldjuhendis sisustanud ja selgitanud nende nõuete täitmist. Avaliku sektori asutuste osas tegeleme just valdavalt asutusesiseseks kasutamiseks mõeldud teabe kaitse nõuete täitmise kontrollimisega, mitte IKSi alusel, sh ei teosta me järelevalvet ISKE nõuete rakendamise osas. Inspektsiooni tegevusega seonduvalt tuleb arvestada, et nt 2016. aasta lõpus oli Statistikaameti andmetel ligi 160 000 majanduslikult aktiivset majandusüksust ning Justiitsministeeriumi küsitlusuuringu kohaselt töötleb isikuandmeid 85% Eestis tegutsevatest rohkem kui ühe töötajaga ettevõttest. Eeltoodu hulka ei ole arvatud valitsemissektorisse kuuluvaid asutusi ja avaliku sektori osalusega ettevõtteid, keda on kokku 3125. Selle arvu hulgas on ka kohalikud omavalitsused. Haldusreformi tulemusena vähenes omavalitsuste arv 213-1t 79-ni. Samuti on inspektsioonil ka muid järelevalvepädevusi AvTS-i alusel. Kontrollaruandes on välja toodud, et inspektsiooni pädevuses on ka järelevalve teostamine andmekogude osas. AvTS SS 43[3] lõike 3 kohaselt kooskõlastatakse enne andmekogu asutamist, andmekogus kogutavate andmete koosseisu muutmist, andmekogu kasutusele võtmist või andmekogu lõpetamist andmekogu tehniline dokumentatsioon RIHA kaudu inspektsiooniga. Hetkeseisuga on RIHAs registreeritud üle 1500 infosüsteemi ja andmekogu. Eeltoodu annab osaliselt aimu, millega ning mis mastaapides inspektsioon tegeleb. Valdav osa meie järelevalvelisest tööst on seotud inspektsioonile saabuvate pöördumiste menetlemisega, olgu selleks kaebused, märgukirjad võimaliku

Riigikontrolli soovitused	Auditeeritute vastused
	seaduserikkumise osas või vaided teabenõuete täitmisega seotud nõuete rikkumise korral. Sellistel pöördumistel on seadustes ette nähtud ka tähtajad, mida peame järgima, ning valdavalt järgneb sellistele pöördumistele ka mingi järelevalvemenetlus ja/või reageering (nt väärteomenetluse läbiviimine). Selle kõige kõrval on ka meie proaktiivsed tegemised, nt kavandatavad kontrollid ja menetlused erinevates ettevõtetes või avaliku sektori valdkonnas (sh kohalikes omavalitsustes). Meie proaktiivne tegevus on paljuski seotud sellega, kuidas on võimalik asutuse tegemisi planeerida nii, et isikud saaksid oma eelnevalt märgitud pöördumistele ka kvaliteetse vastuse või lahendi. Kui arvestada inspektsiooni ametikoosseisu suurust (18 täidetud ametikohta) ning konkreetsete järelevalve tegijate arvu (8 inspektorit + planeerituna 2 andmeturbeinspektorit; RIHA osas õigusdirektor ja koostöödirektor koos samade andmeturbeinspektoritega), siis tuleb tegeleda sellega, mis on mõjusam nii era- kui ka avalikus sektoris. Kõike eeltoodut ja inspektsiooni töökoormust mõjutavad ka selle aasta mais toimuvad muudatused, kui jõustub isikuandmete kaitse üldmäärus ning koos sellega ka uus isikuandmete kaitse seadus. Nende muudatusega on hõivatud enamik inspektsiooni tööressursist ning seotud meie töö planeerimine, sh järelevalve. Prognoosin, et sellega seotud muudatused mõjutavad vähemalt meie selle aasta toimetusi, sh võimalik, et ka järgmist aastat. Seetõttu tänan Riigikontrolli esitatud soovituse eest tõhustada kontrolli omavalitsustes turvameetmete süsteemi rakendamise ning RIHAs registreerimise üle. Tegelen selle soovituse täitmisega vastavalt võimalustele.
Teavitustegevus infoturbe valdkonnas **103. Riigikontrolli soovitus Riigi Infosüsteemi Ameti peadirektorile**: propageerida IT-spetsialistidele mõeldud koolituste kõrval rohkem KOVi juhtkonnale suunatud koolitusi või teha laiemat teavitust, mh kaaluda uute linna- ja vallajuhtide jaoks koolitusprogrammi väljatöötamist. **p-d 90–95**	**Riigi Infosüsteemi Ameti peadirektori vastus:** Riigi Infosüsteemi Amet tänab selle soovituse eest ning soovime siinkohal rõhutada, et oleme soovituse sisulise poolega igati nõus. Ka RIA on oma toimingute käigus korduvalt leidnud, et asutuste tippjuhtide teadlikkus infoturbest ning sellest tulenevalt ka motiveeritus sellega tegeleda võiksid olla paremad. Samadel põhjustel on tippjuhtide huvi sellistel koolitustel osaleda madal ning seetõttu võiks Riigikontrolli sellekohane soovitus olla pigemini suunatud omavalitsuste juhtidele. Tippjuhtidele suunatud koolitustega on RIA juba alustanud 2017. aastal, mil osalejaid olid peamiselt avaliku sektori juhid. 2018. aastal on plaanis viia läbi infoturbeteadlikkuse tõstmise koolitusi ka kohalikele omavalitsustele ja nende juhtkondadele. ▪ Infoturbe teadlikkuse tõstmise koolitus (erinevad lokatsioonid Eestis) töötajatele, kellel ei ole laialdast tehnilist teadmist infotehnoloogiast ja infoturbest. Sihtgruppi kuuluvad inimesed kõikidest organisatsiooni tasemetest: juhtkond, keskastme juhid, spetsialistid ja tugipersonal. ▪ ISKE koolitus (erinevad lokatsioonid Eestis) töötajatele, kelle ülesanne on ISKE metoodika rakendamine. Koolitusel kasutatakse praktilisi näiteid, mis peamiselt on kogutud lektori 10-aastase ISKE juurutamise kogemuse põhjal. Nii seob koolitaja ISKE rakendamise teoreetilised sammud reaaleluliste probleemkohtadega. ▪ Infoturbe koolitusseminar juhtidele (erinevad lokatsioonid Eestis), et tutvustada asutuste/ettevõtete otsustajate tasemele infoturbe ja infoturbe halduse aluseid, sh vajadust teha investeeringuid selles valdkonnas. Koolitus korraldatakse ELi struktuuritoetuse toetusskeemist „Infoühiskonna teadlikkuse tõstmine" Euroopa Regionaalarengu Fondi rahastusel ning koostöös Tallinna Tehnikaülikooliga. Tegemist on tasuta koolitustega. Koolituse toimumise kohta on jagatud teavet eri kanalite kaudu. Info koolituste toimumise kohta on edastatud muu hulgas linna- ja vallasekretäride e-posti listi ning Eesti Maaomavalitsuste Liidu esindajatele tagamaks, et info jõuaks asjakohaste isikuteni, sh juhtideni. Asetleidvatele koolitustele registreerunute nimekirjades on ka omavalitsuste esindajaid. Koolituse läbinud inimeste tagasisidet analüüsitakse ning koolitusi kohandatakse saadud tagasiside alusel olemasolevate võimaluste piires. Kohalike omavalitsuste külastamine, nõustamine ja paikvaatluste tegemine: 2018. a II poolaastast kuni 2019. a hakkavad RIA küberturvalisuse teenistuse teenuste turvalisuse osakonna töötajad muu hulgas külastama kohalikke omavalitsusi, et suurendada koostööd ja tõsta kohalike omavalitsuste juhtkondade teadlikkust, sh selgitada välja nende vajadused nõustamise, koolitamise jms osas.

Riigikontrolli soovitused	Auditeeritute vastused
	2018. a II poolaastal plaanitakse kohalike omavalitsuste esindajaid kaasata muu hulgas infoturbejuhtide komisjoni töösse, et suurendada koostööd, informatsiooni ja kogemuste vahetamist ISKE rakendajate vahel.
Toetuste jagamine infoturbe valdkonnas **113. Riigikontrolli soovitus ettevõtlus- ja infotehnoloogiaministrile:** toetusmeetmete tingimuste koostamisel võtta arvesse, et need motiveeriks kasutusele võtma lahendusi, mis riik või mõni teine KOV on juba maksumaksja raha eest loonud. **p-d 104–112**	**Ettevõtlus- ja infotehnoloogiaministri vastus:** Majandus- ja Kommunikatsiooniministeerium lähtub juba tänasel päeval üldisest põhimõttest, mille kohaselt eelistatakse IT-lahenduste ühiskasutust ja -arendust. Toetusmeetmete tingimuste koostamisel ja ülevaatamisel lähtub MKM ka edaspidi nendest põhimõtetest.

Auditi iseloomustus

Auditi eesmärk

Auditi eesmärk oli hinnata KOVide tegevust infoturvameetmete rakendamisel ning riigi tegevust KOVide infoturbe olukorra parendamisel. Infoturvameetmete rakendamisel hinnati meetmete tagamise eelduste loomist (sh planeerimine ja nõuete seadmine) ning rakendamist.

Hinnangu andmise kriteeriumid:

- KOV on planeerinud infoturbetegevusi ja loonud dokumentatsiooni selle kohta, kuidas tagatakse X-tee kaudu andmete vahetuse turvalisus.
- KOV rakendab turvameetmeid X-tee kaudu toimuva andmevahetuse turvalisuse tagamiseks.
- Andmete turvalise vahetamise üle tehakse järelevalvet.

Auditi ulatus ja käsitlusviis

Auditi raames viidi KOVides läbi kohapealsed menetlustoimingud Riigikontrolli välja valitud tööjaamade konfiguratsioonide osas, seadmete ja tehniliste ruumide paikvaatlus ning intervjuu vastutavate isikute osalemisel.

Turvameetmete süsteemi rakendamisele anti hinnang ISKE kataloogi moodulitest valitud turvameetmete ulatuses. Moodulite valikul ISKE kataloogist tugineti RIA varasemates kontrollides kasutatud moodulite valikule, mida omakorda kitsendati tuvastatud sagedasemate puudujääkide põhjal. Turvameetmete süsteemi rakendamiseks loodud dokumentatsiooni olemasolu ja nõuetele vastavuse väljaselgitamiseks viidi läbi dokumentide analüüs ning intervjuu. Asutuse vastutavatele isikutele ja/või IT-teenusepakkujale esitati küsimusi infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE ja eelnevalt Riigikontrollile saadetud dokumentatsiooni alusel.

Auditeeritute valikul arvestati KOVide koormatust muude käimasolevate, planeeritavate või hiljuti lõppenud audititega (vt tabel 3).

Tabel 3. Auditeeritud KOVide väljavalimise kriteeriumid

Auditeeritu	Ühinemine	KOVISKE projektis osalenud	Elanike arv > 5000	Riigi andmesidevõrku kuulumine	Maakond
Kuusalu vald	2005	Jah	Jah	Jah	Harjumaa
Rapla vald	2002	Jah	Jah	Ei	Raplamaa
Viljandi vald	2013	Jah	Jah	Jah	Viljandimaa
Paide linn	Ei	Jah	Jah	Jah	Järvamaa
Valga linn	Ei	Jah	Jah	Jah	Valgamaa
Võru vald	Ei	Jah	Jah	Ei	Võrumaa
Audru vald	2013	Ei	Jah	Ei	Pärnumaa
Kohtla-Järve linn	Ei	Ei	Jah	Ei	Ida-Virumaa
Avinurme vald	Ei	Ei	Ei	Ei	Ida-Virumaa
Vihula vald	1999	Ei	Ei	Ei	Lääne-Virumaa

Dokumentaalseid tõendeid KOVide kohta on lisaks auditeeritutele endile esitanud ka riigiasutused, riigiregistrite vastutavad töötlejad ja auditisse kaasatud ekspert.

Eksperditööd

Kohapealseid menetlustoimingud viis läbi Riigikontrolli palgatud ekspert OÜ Primend, kes kogus auditi jaoks vajaliku tõendusmaterjali tööjaamadest ning jäädvustas seadmete füüsilise olukorra. Toimingute tegemiseks kasutati selleks ettenähtud spetsiaalseid tark- ja riistvara lahendusi. Toiminguid viidi läbi igas asutuses kuni 3 arvuti töökohas. Arvutid valiti järgmiste kriteeriumite alusel:

- kasutajal oli juurdepääs riigi andmekogudele;
- kasutajal oli juurdepääs KOVi enda serveris majutatud andmekogule;
- arvuti kasutaja oli juhtkonna liige, valla-/linnasekretär.

Ekspert koostas saadud andmete põhjal raporti, kus hinnati vastavust kriteeriumitele, mis olid eelnevalt Riigikontrolliga kokku lepitud.

Auditi lõpetamise aeg

Peamised toimingud auditi koostamise tarvis tehti maist oktoobrini 2017, andmeid täpsustati kuni jaanuarini 2018.

Auditi meeskond

Auditi meeskonda kuulusid audiitor Meeli Saksing projektijuhi ülesannetes ja audiitor Riina Saaremägi.

Kontaktandmed

Auditi kohta saab lisainfot Riigikontrolli kommunikatsiooniüksusest
tel +372 640 0704 või +372 640 0777, e-post riigikontroll@riigikontroll.ee

Auditiaruande elektrooniline koopia (pdf) on saadaval koduleheküljel www.riigikontroll.ee.

Auditiaruande kokkuvõte on saadaval ka inglise keeles.

Auditiaruande number Riigikontrolli asjaajamissüsteemis on 2-1.9/50094/2.

Riigikontrolli postiaadress on:

Kiriku 2/4
15013 TALLINN
Tel +372 640 0700
Faks +372 661 6012
riigikontroll@riigikontroll.ee

Riigikontrolli varasemaid auditeid info- ja kommunikatsioonitehnoloogia valdkonnas

Alljärgnevates auditites on varem käsiteletud infoturbe halduse teemat muu hulgas ka kohalikes omavalitsustes:

29.09.2006 – **Riigi tugi kohalikele omavalitsustele infoühiskonna arendamisel**

25.11.2008 – **Sisekontrollisüsteemi toimimine andmete kaitsel riiklikes andmekogudes**

26.03.2009 – **Teabele juurdepääsu võimaldamine ja selle piiramine valdades ja linnades**

12.02.2010 – **Riigi infosüsteemide arendusprotsessi tulemuslikkus**

31.10.2013 – **Andmete esitamine riigi andmekogudele valdades ja linnades**

31.01.2017 – **Ülevaade valdades ja linnades peetavatest andmekogudest**

Kõik aruanded on kättesaadavad Riigikontrolli koduleheküljelt www.riigikontroll.ee.

Lisa A. Majandus- ja Kommunikatsiooniministeeriumi, Andmekaitse Inspektsiooni, Riigi Infosüsteemi Ameti ja auditeeritud kohalike omavalitsuste vastuste täistekstid

NB! Mitmel vastusel on märge dokumendi asutusesiseseks kasutamiseks tunnistamise kohta kuni 2023. (2093.) aastani. See piirang on ekslik ning tegelikkuses kehtis piirang kuni käesoleva aruande avalikustamiseni.

Majandus- ja Kommunikatsiooniministeeriumi arvamus kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõu kohta

Riigikontrolli soovitused	Majandus- ja Kommunikatsiooniministeeriumi vastused
1. Hinnata, kas ministeeriumid saavad seadusega ära määrata ka andmete turvaklassi andmekogu(de) puhul, mille pidamist nõutakse KOVilt kohustusliku ülesande täitmiseks.	Majandus- ja Kommunikatsiooniministeerium peab mõistlikuks, et sarnaste või ühetaoliste andmekogude turvaklassi määramine lähtuks ühtsetest alustest ning toimuks dubleerivate protseduurideta. Riigi infosüsteemi seisukohalt on optimaalne korraldus, kus infosüsteemid on üleriigilised ning KOVid teevad sinna kandeid. Juhul, kui seadusandja on siiski ette näinud, et iga KOV peab ise mingit registrit pidama, siis tuleb kindlasti hinnata kõikvõimalikke meetmeid, kuidas sellise andmekogu pidamisele kaasa aidata, kaasa arvatud ühtse lähenemise kujundamine turvaklassi määramisele ning turvameetmete rakendamisele.
2. Analüüsida põhjuseid, miks turvameetmete süsteemi rakendamine KOVides on pikalt viibinud ning sellest tulenevalt töötada välja tegevused ISKE rakendamise paindlikumaks muutmiseks (sh kaaluda standardsete tarkvaralahenduste osutajatele ISKE-auditi läbimise kohustuse seadmist) KOVides nii, et see oleks rohkem kohapealseid olusid arvestav;	Majandus- ja Kommunikatsiooniministeerium adresseerib Riigikontrolli poolt tõstatud probleeme ISKE määruse uuendamisel ja ISKEga seotud juhendite ja materjalide läbivaatamisel. Küberturvalisuse seadusega laieneb turvameetmete rakendamise kohustus ka teistele infosüsteemidele lisaks nendele, mida kasutatakse andmekogude pidamisel (01.01.2020). ISKE määrus, juhendid ja materjalid vajavad eelnevat kaasajastamist selle muudatuse realiseerimiseks. Riigikontrolli poolt tõstatud küsimusi on otstarbekas käsitleda koos küberturvalisuse seadusest tingitud muudatustega. MKM nõustub, et senine korraldus KOVide ISKE auditite tellimiseks on ebaõnnestunud.
3. Muuta ISKE-auditi tellimise korraldust (sh ISKE-auditi juhendit) nii, et selle tellimine oleks järjepidevalt tagatud.	
4. Algatada Rahandusministeeriumiga ISKE-auditite tellimise rahastuse läbirääkimised.	
5. Hinnata koostöös Justiitsministeeriumiga avalikule sektorile standardlahenduste pakkujatele registreerimise kohustuse seadmist RIHAs.	Majandus- ja Kommunikatsiooniministeerium peab oluliseks, et avalikule sektorile pakutavad standardlahendused vastaksid asjakohastele turvanõuetele. Peame samuti oluliseks, et andmekogu pidajate kohustused seoses RIHAga oleksid optimaalsed ja realistlikud. Riigikontrolli ettepanekut on kavas käsitleda RIHA protsessi uuendamisel.
6. Täpsustada Vabariigi Valitsuse määrust nr 105 „Infosüsteemide andmevahetuskiht“ nii, et	Majandus- ja Kommunikatsiooniministeerium võtab arvesse Riigikontrolli soovitust Vabariigi

oleks üheselt selge, kellele ja mis osas määrus kohaldub, ning veenduda, et sellega ei loodaks andmeteenuse osutajatele ja kasutajatele dubleerivaid kohustusi (mh tuleks arvestada ka olukorraga, kus KOV on andmeteenuse osutajaks riigiregistritele).	Valitsuse määruse nr 105 „Infosüsteemide andmevahetuskiht“ kaasajastamisel.
7. Toetusmeetmete tingimuste koostamisel võtta arvesse, et need motiveeriks kasutusele võtma lahendusi, mis riik või mõni teine KOV on juba maksumaksja raha eest loonud.	Majandus- ja Kommunikatsiooniministeerium lähtub juba tänasel päeval üldisest põhimõttest, mille kohaselt eelistatakse IT-lahenduste ühiskasutust ja –arendust. Toetusmeetmete tingimuste koostamisel ja ülevaatamisel lähtub MKM ka edaspidi nendest põhimõtetest.

ANDMEKAITSE INSPEKTSIOON

EESTI VABARIIK 100

ASUTUSESISESEKS KASUTAMISEKS
Teabevaldaja: Andmekaitse Inspektsioon
Märge tehtud: 23.04.2018
Kehtib kuni: kontrollaruande vastuvõtmiseni
Alus: AvTS § 35 lg 2 p 2

Lp Ines Metsalu-Nurminen
peakontrolör
Riigikontroll
riigikontroll@riigikontroll.ee

Teie: 12.04.2018 nr 2-1.9/50094/2

Meie: 24.04.2018 nr 1.2.-4/18/956

Kontrollaruandele arvamuse avaldamine

Tänan, et esitasite mulle arvamuse avaldamiseks „IT-turvameetmete rakendamine kohalikes omavalitsustes“ eelnõu. Kõigepealt tänan, et viisite läbi kõnealuse auditeerimise selles valdkonnas.

Riigikontroll tegi inspektsioonile soovituse tõhustada kontrolli kohalikes omavalitsustes turvameetmete süsteemi rakendamise ning riigi infosüsteemide haldussüsteemis (RIHA) registreerimise üle.

Tänan selle esitatud soovituse eest, kuid ma pean esmalt märkima, et inspektsiooni pädevuses on järelevalve teostamine nii isikuandmete kaitse seaduse (IKS) kui ka osa avaliku teabe seaduse (AvTS) nõuete täitmise osas. Paljuski on nende kahe seaduse kokkupuutepunkt kattuv – IKS-i alusel kontrollime isikuandmete kaitseks rakendatavaid organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid ning AvTS-i alusel kontrollime asutusesiseseks kasutamiseks mõeldud teabe kaitsmist. Märgin, et viimase ülesande täitmist on kohati ka raskendatud teha, kuna senini ei ole Vabariigi Valitsus vastu võtnud AvTS § 43 lg 3 alusel määrust, millega kehtestatakse asutusesisese teabe tervikluse, käideldavuse ja konfidentsiaalsuse kaitseks rakendatavate organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete loetelu. Selle asemel oleme enda avaliku teabe seaduse üldjuhendis sisustanud ja selgitanud nende nõuete täitmist.[1] Avaliku sektori asutuste osas tegeleme just valdavalt asutusesiseseks kasutamiseks mõeldud teabe kaitse nõuete täitmise kontrollimisega, mitte IKS-i alusel, sh ei teosta me järelevalvet ISKE nõuete rakendamise osas.

Inspektsiooni tegevusega seonduvalt tuleb arvestada, et nt 2016. aasta lõpus oli Statistikaameti andmetel ligi 160 000 majanduslikult aktiivset majandusüksust ning Justiitsministeeriumi küsitlusuuringu kohaselt töötleb isikuandmeid 85% Eestis tegutsevatest rohkem kui ühe töötajaga ettevõtetest.[2] Eeltoodu hulka ei ole arvatud valitsemissektorisse kuuluvaid asutusi ja avaliku sektori osalusega ettevõtteid, keda on kokku 3125– selle arvu hulgas on ka kohalikud omavalitsused. [3] Haldusreformi tulemusena vähenes omavalitsuste arv 213-lt 79-ni.[4]

Samuti on inspektsioonil ka muid järelevalvepädevusi AvTS-i alusel. Kontrollaruandes on välja toodud, et inspektsiooni pädevuses on ka järelevalve teostamine andmekogude osas –

[1] Avaliku teab seaduse üldjuhend, peatükk 10 - http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AvTSuldjuhend.pdf.
[2] Vt uue isikuandmete kaitse seaduse eelnõu seletuskiri, lk 56 - http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/iks_sk_21.03.18.pdf.
[3] Sama.
[4] https://haldusreform.fin.ee/.

AvTS § 43^3 lõike 3 kohaselt enne andmekogu asutamist, andmekogus kogutavate andmete koosseisu muutmist, andmekogu kasutusele võtmist või andmekogu lõpetamist kooskõlastatakse andmekogu tehniline dokumentatsioon RIHA kaudu inspektsiooniga. Hetkeseisuga on RIHA-s registreeritud üle 1500 infosüsteemi ja andmekogu.

Eeltoodu annab osaliselt aimu, millega ning mis mastaapides inspektsioon tegeleb. Valdav osa meie järelevalvelisest tööst on seotud inspektsioonile saabuvate pöördumiste menetlemisega – olgu selleks kaebused, märgukirjad võimaliku seaduserikkumise osas või vaided teabenõuete täitmisega seotud nõuete rikkumise korral. Sellistel pöördumistel on seadustes ette nähtud ka tähtajad, mida peame järgima ning valdavalt järgneb sellistele pöördumistele ka mingi järelevalvemenetlus ja/või reageering (nt väärteomenetluse läbiviimine).

Selle kõige kõrval on samuti ka meie proaktiivsed tegevused – nt kavandatavad kontrollid ja menetlused erinevates ettevõtetes või avaliku sektori valdkonnas (sh kohalikes omavalitsustes). Meie proaktiivne tegevus on paljuski seotud sellega, kuidas on võimalik asutuse tegevusi planeerida nii, et isikud saaksid oma eelnevalt märgitud pöördumistele ka kvaliteetse vastuse või lahendi. Kui arvestada inspektsiooni ametikoosseisu suurust (18 täidetud ametikohta) ning konkreetsete järelevalve tegijate arvu (8 inspektorit + planeerituna 2 andmeturbeinspektorit; RIHA osas õigusdirektor ja koostöödirektor koos samade andmeturbeinspektoritega), siis tuleb tegeleda sellega, mis on mõjusam nii era- kui ka avalikus sektoris.

Kõike eeltoodut ning inspektsiooni töökoormust mõjutab ka selle aasta mais toimuvad muudatused, kui jõustub isikuandmete kaitse üldmäärus ning sellega koos ka uus isikuandmete kaitse seadus. Nende muudatusega on hõivatud enamus inspektsiooni tööressursist ning on seotud meie töö planeerimisega, sh järelevalveliste tegevustega. Prognoosin, et sellega seotud muudatused mõjutavad vähemalt meie selle aasta toimetusi, sh võimalik, et ka järgmisel aastal.

Seetõttu tänan Riigikontrolli esitatud soovituse eest tõhustada kontrolli kohalikes omavalitsustes turvameetmete süsteemi rakendamise ning RIHA-s registreerimise üle. Tegelen selle soovituse täitmisega vastavalt võimalustele.

Lugupidamisega

/allkirjastatud digitaalselt/
Viljar Peep
peadirektor

Raavo Palu raavo.palu@aki.ee

RIIGI INFOSÜSTEEMI AMET

Ines Metsalu-Nurminen
Riigikontroll
riigikontroll@riigikontroll.ee

Teie 12.04.2018 nr 2-1.9/50094/2

Meie 24.04.2018 nr 1.1-6/181119

Vastus kontrollaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõule

Austatud Ines Metsalu-Nurminen

Riigikontrolli auditis oli Riigi Infosüsteemi Ameti peadirektorile kaks (2) soovitust, punktid 96 ja 103.

Punkt 96. Riigikontrolli soovitus Riigi Infosüsteemi Ameti peadirektorile ja Andmekaitse Inspektsiooni peadirektorile: tõhustada kontrolli KOV-ides turvameetmete süsteemi rakendamise, X-teega liitumise ning RIHAs registreerimise üle.

Riigi Infosüsteemi Ameti peadirektori vastus:
Riigi Infosüsteemi Amet on turvameetmete rakendamise kontrollimisega (sh. X-tee) kohalikes omavalitsustes tegelenud ning jätkab sellega tegelemist vastavalt riskihinnangutest tulenevale prioriteetsusele. Kohalike omavalitsuste kontrollimine haldusreformi järgselt oli RIA plaanides juba varasemalt, seega võib öelda, et antud soovitus on juba täitmisel.

Punkt 103. Riigikontrolli soovitus Riigi Infosüsteemi Ameti peadirektorile: propageerida IT-spetsialistidele mõeldud koolituste kõrval rohkem KOV-idele suunatud koolitusi või teha laiemat teavitust, mh kaaluda uute linna- ja vallajuhtide jaoks koolitusprogrammi väljatöötamist.

Riigi Infosüsteemi Ameti peadirektori vastus: Riigi Infosüsteemi Amet tänab selle soovituse eest ning soovime siinkohal rõhutada, et oleme soovituse sisulise poolega igati nõus. Ka RIA on oma toimingute käigus korduvalt leidnud, et asutuste tippjuhtide teadlikkus infoturbest ning sellest tulenevalt ka motiveeritus sellega tegeleda võiksid olla paremad. Samadel põhjustel on tippjuhtide huvi sellistel koolitustel osaleda madal ning seetõttu võiks Riigikontrolli sellekohane soovitus olla pigemini suunatud omavalitsuste juhtidele.

Tippjuhtidele suunatud koolitustega on RIA juba alustanud 2017. aastal, mis osalejaid olid peamiselt avaliku sektori juhid. 2018. aastal on plaanis viia läbi infoturbeteadlikkuse tõstmise koolitusi ka kohalikele omavalitsustele ja nende juhtkondadele.

- Infoturbe teadlikkuse tõstmise koolitus (erinevad lokatsioonid Eestis)) – töötajatele, kellel ei ole laialdast tehnilist teadmist infotehnoloogiast ja infoturbest. Sihtgruppi kuuluvad inimesed kõikidest organisatsiooni tasemetest – juhtkond, keskastme juhid, spetsialistid ja tugipersonal.
- ISKE koolitus (erinevad lokatsioonid Eestis) - töötajatele, kelle ülesandeks on ISKE metoodika rakendamine. Koolitusel kasutatakse praktilisi näiteid, mis peamiselt on kogutud lektori 10-aastase ISKE juurutamise kogemuse põhjal. Nii seob koolitaja ISKE teoreetilised rakendamise sammud reaaleluliste probleemkohtadega.
- Infoturbe koolitusseminar juhtidele (erinevad lokatsioonid Eestis) - koolituse eesmärk on tutvustada asutuste/ettevõtete otsustajate tasemele infoturbe ja infoturbe halduse aluseid, sh vajadust teha investeeringuid selles valdkonnas.

Koolitus korraldatakse EL struktuuritoetuse toetusskeemist "Infoühiskonna teadlikkuse tõstmine" Euroopa Regionaalarengu Fondi rahustusel ning koostöös Tallinna Tehnikaülikooliga. Tegemist on tasuta koolitustega.

Koolituse toimumise kohta on jagatud teavet erinevate kanalite kaudu. Informatsioon nimetatud koolituste toimumise kohta on edastatud muuhulgas linna- ja vallasekretäride e-posti listi ning Eesti Maaomavalitsuste Liidu esindajatele tagamaks, et informatsioon jõuaks asjakohaste isikuteni, sh juhtideni. Asetleidvatele koolitustele registreerunute nimekirjades on ka kohalike omavalitsuste esindajaid.

Koolituse läbinud inimeste tagasisidet analüüsitakse ning koolitusi kohandatakse vastavalt saadud tagasisidele olemasolevate võimaluste piires.

Kohalike omavalitsuste külastamine, nõustamine ja paikvaatluste tegemine.
2018 II poolaasta - 2019 hakkavad RIA küberturvalisuse teenistuse teenuste turvalisuse osakonna töötajad muuhulgas külastama erinevaid kohalikke omavalitsusi, et suurendada koostööd ja tõsta kohalike omavalitsuste juhtkondade teadlikkust, sh selgitada välja nende vajadused nõustamise, koolitamise jms osas.

2018 II poolaastal plaanitakse kohalike omavalitsuste esindajaid kaasata muuhulgas infoturbejuhtide komisjoni töösse, et suurendada koostööd, informatsiooni ja kogemuste vahetamist ISKE rakendajate vahel.

Lugupidamisega

/allkirjastatud digitaalselt/

Taimar Peterkop
peadirektor

Martin Mõtus 663 0268
martin.motus@ria.ee

HALJALA VALLAVALITSUS

Riigikontroll
riigikontroll@riigikontroll.ee

Teie : 12.04.2018 nr 2-1.9/50094/2
Meie: 15.05.2018 nr 14-5/199-1

Vastus kontrolliaruandele "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõule

Riigikontrolli aruande eelnõus "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes", milles oli auditeeritavaks endine Vihula vald, 25.oktoobril 2017 moodustus Haljala valla ja Vihula valla ühinemise teel uus omavalitsusüksus Haljala vald, mis on ühinenud omavalitsuste üldõigusjärglane, tehtud ettepanekute osas annab Haljala vallavalitsus oma seisukoha alljärgnevalt:

1. Haljala vallavalitsus arvestab edaspidi Riigikontrolli ettepanekutega järgida andmekogude kasutusele võtul või uute andmekogude loomisel, et tarkvaralahenduse pakkuja teenuse turbeaste ja rakendatavad turvameetmed vastaksid andmekogusse sisestatavate andmete turbeastmenõuetele ning et teenuseosutaja poolt pakutav lahendus oleks liidestatav x-teega.

2. Andmekaitse ja infoturbe korraldamine on hetkel vallasekretäri ametiülesanne, ametijuhend kinnitatud 15.04.2013.a. Edaspidi peame siiski otstarbekamaks tellida infoturbe ülesannete täitmine sisse teenusena.

/allkirjastatud digitaalselt/
Leo Aadel
Vallavanem

Riina Must
327 8223
riina.must@haljala.ee

KOHTLA-JÄRVE LINNAVALITSUS

Riigikontroll
riigikontroll@riigikontroll.ee

Teie:

Meie: 25.04.2018 nr 2-5.1/670-3

Vastus kirjale

Edastasite Kohtla-Järve Linnavalitsusele 13. aprillil 2018. a Riigikontrolli kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõu. Teatame, et püüame viia vastavusse eelnõus esitatud soovitused ning tegeleme puuduste kõrvaldamisega.

Lugupidamisega

/allkirjastatud digitaalselt/

Anna Generalova
linnasekretär

Keskallee 19
30395 Kohtla-Järve
EESTI
registrikood 75001017
tel +372 337 8500
faks +372 337 8503
e-post: linnavalitsus@kjlv.ee
SEB Pank AS
IBAN EE441010552010016001
Swedbank AS
IBANEE402200001120012980

KUUSALU VALLAVALITSUS

Riigikontroll

Teie: 12.04.2018 nr 2-1.9/50094/2

Meie: 26.04.2018 nr 3.2-2/1184-1

Kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõu edastamine: vastuskiri

Kuusalu vallavalitsuses on IT-turbe alal toimumas oluline areng. Kuusalu vald osaleb Rahandusministeeriumi Infotehnoloogiakeskuse (RMIT) projektis „KOV-de IKT baastaristute uuendamine ISKE nõuetele“.

Projekti käigus võetakse kasutusse ajakohasee võrguseadmestik ja RMITis majutatud serveripark, ning grupitöölahendus ja e-posti süsteem, samuti KOV infosüsteemi taastamiseks sobilik taastelahendus. Omavalitsusele luuakse sõltumatult administreeritavad virtuaalserverid, millel toimib keskselt korraldatud IT haldus (keskne autentimine, keskne grupitöölahendus, keskne arvutite haldus). Koostatakse IKT taristu ja ISKE dokumentatsioon. Tekivad eeldused taristu haldamises vajadusel teenusepõhisele mudelile üleminekuks.

Projekti tegevused on planeeritud läbi viia 2018. aasta jooksul.

Kuusalu vallavalitsuse vastused Riigikontrolli soovitustele:

Soovitus:

- veenduda andmekogu tarkvaralahenduse valimisel, et tarkvaralahendus on vajaduse korral liidestatav X-teega ning et standardlahenduse turbeaste vastaks sinna sisestatavate andmete turbeastmenõudele;
- leppida lepingus teenuseosutajaga kokku, millised turvameetmed peavad olema rakendatud ja milline on turvameetmete auditeerimise korraldus.

Vastus:
Kuusalu vallavalitsus arvestab soovitustega uute tarkvaralahenduste valikul ja lepingute sõlmimisel. Peame oluliseks koostööd teiste omavalitsustega nii Eesti Linnade ja Valdade Liidu raames kui ka omavahelisi kontakte. Soovime teenuseosutajaga läbirääkimisi pidades arvestada ka teiste omavalitsuste kogemusega ja teha nendega koostööd.

Kuusalu tee 35b Kuusalu Alevik
74601 Harjumaa
Reg. Kood 75033496

Telefon +372 6066 370
Faks +372 6066 371
E-post vallavalitsus@kuusalu.ee
Veeb http://www.kuusalu.ee

Arvelduskonto EE742200001120050586
Swedbank

Soovitus: määrata infoturbejuhi ülesannete täitja või tellida infoturbejuhtimine teenusena sisse, et oleks tagatud piisav tähelepanu IT-turvalisusega seotud aspektidele.

Vastus:
Kuusalu Vallavalitsuse infoturbe tegevuse teostamine ja korraldamine on ametijuhendi järgi praegu IT-arendusjuhi ülesandeks. Projekti „KOV-de IKT baastaristute uuendamine ISKE nõuetele“ täitmise käigus hindame infoturbejuhi ülesannete täitmiseks vajalikku töömahtu ja kompetentsi ja lahendame infoturbejuhi ülesannete täitja valiku parimal võimalikul viisil.

Lugupidamisega

(allkirjastatud digitaalselt)

Urmas Kirtsi
Vallavanem

Peep Abel 6066394
peep.abel@kuusalu.ee

MUSTVEE VALLAVALITSUS

ASUTUSESISESEKS KASUTAMISEKS
Märge tehtud: 07.05.2018
kehtib kuni: 07.05.2023
Alus: AvTS § 35 lg 2 p 2
Teabevaldaja: Mustvee Vallavalitsus

Riigikontroll
info@riigikontroll.ee

Teie 12.04.2018 nr 2-1.9/50094/2

Meie 07.05.2018 nr 14-3/47-2

Arvamus

Mustvee vald on tutvunud kontrollaruande „IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes“ eelnõuga.

Teiste seas auditeeriti kohalikest omavalitsustest Avinurme valda, mille õigusjärglane peale haldusreformi on Mustvee vald.

Mustvee Vallavalitsuses on praeguseks hetkeks personal komplekteeritud. Teenistujad on osalenud mitmetel erinevatel infoturbe koolitustel. Mustvee Vallavalitsus osaleb pilootprojektis „ KOV IKT taristu“, millega arendame ISKE-le vastava turvalise internetivõrgu. Andmevarundus kolib RMIT serverisse. Hetkel on käimas arvutihange, millega viime arvutipargi vastavusse ISKE nõuetega. Koostamisel on infoturbe alane dokumentatsioon.

Lugupidamisega

/allkirjastatud digitaalselt/

Jüri Morozov
Vallavanem

Daisy Utsar, 332 3663

PAIDE LINNAVALITSUS

Ines Metsalu-Nurminen
Riigikontroll
riigikontroll@riigikontroll.ee
Meeli.Saksing@riigikontroll.ee

Teie 12.04.2018 nr 2-1.9/50094/2

Meie 23.05.2018 nr 15-9/18/1094-2

Vastus kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõule

Austatud Ines Metsalu-Nurminen

25. oktoobril 2017 moodustus Paide linna, Paide valla ja Roosna-Alliku valla ühinemise teel uus omavalitsusüksus Paide linn, mis on kõikide eelpool nimetatute üldõigusjärglane. Alates 01.01.2018 kannab Paide Linnavalitsus, Paide Vallavalitsus ja Roosna-Alliku Vallavalitsus ühist uut nime Paide Linnavalitsus (registrikood 77000246).

Paide Linnavalitsusel puuduvad täiendavad kommentaarid ja parandusettepanekud kontrolliaruande eelnõule.

Lugupidamisega

/allkirjastatud digitaalselt/

Priit Värk
Linnapea

Peeter Läll 383 8606
peeter.lall@paide.ee

PÄRNU LINNAVALITSUS
AUDRU OSAVALLAKESKUS

Riigikontroll
riigikontroll@riigikontroll.ee

Teie 12.04.2018 nr 2-1.9/50094/2
Meie 24.04.2018 nr 4.3-13/4691/2018-1

Kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõu edastamine

Vastuseks Teie kirjale teatame, et oleme kontrolliaruandega tutvunud ja võtame selle teadmiseks. Tänaseks on toimunud Audru valla ja Pärnu linna ühinemine ning IT- turvameetmete süsteeme on oluliselt parendatud mitmetes aruandes viidatud puuduste osas.

Lugupidamisega
/allkirjastatud digitaalselt/

Priit Annus
Audru osavallakeskuse juhataja

Rapla Vallavalitsus

Riigikontroll
Kiriku tn 2/4
15013 Tallinn

Teie 12.04.2018 nr 2-1.9/50094/2

Meie 24.04.2018 nr 12-10/1214-2

info@riigikontroll.ee

Kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõu edastamine: vastuskiri

Rapla Vallavalitsus, tutvunud Riigikontrolli kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" kavandiga, nendib, et auditis käsitletud teemade ring on omavalitsuste tasandil oluline ning annab sisuka ülevaate valdkonna probleemidest, võimalikest põhjustest ning lahendustest.
Nõustume Riigikontrolli seisukohtadega, et kohalikus omavalitsuses on IT-turvameetmetele liialt vähe tähelepanu pööratud ja süsteemi rakendamine jäänud tagaplaanile.
Vallavalitsus on teinud oma järeldused ning alustanud abinõude kavandamist auditeerimise käigus esinenud puuduste kõrvaldamiseks, samuti tehtud soovituste arvestamiseks kohaliku omavalitsuse edaspidises tegevuses.
Haldusreformi järgselt on uus moodustunud kohalik omavalitsus senisest võimekam ja mehitatud valdkonnas pädevate spetsialistidega, saavutamaks auditeeritud valdkonnas senisest tõhusam infoturbe juhtimine, turvameetmete rakendamine, kaitse võimalike intsidentide ja rünnete vastu ning teenistujate parem infoturbealane teadlikkus.
Uue kohaliku omavalitsuse üksuse ametiasutuse moodustamisega kaasneb ka andmekogude tarkvaralahenduse pakkujatega sõlmitud lepingute ülevaatamine ja uute lepingute sõlmimine. Protsessi käigus arvestame Riigikontrolli esitatud soovitustega.

Lugupidamisega

/allkirjastatud digitaalselt/

Piret Minn
vallavanem

Ants Soodla
ants.soodla@rapla.ee
489 0518

VALGA VALLAVALITSUS

Teie nr 2-1.9/50094/2

Riigikontroll
riigikontroll@riigikontroll.ee

Meie kuupäev digiallkirjas
nr 4-5.3/1931-1

Kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes" eelnõu edastamine: vastuskiri

Riigikontroll auditeeris „IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes“ raames Valga linna, mis on tänaseks ühinenud koos Karula, Taheva, Õru ja Tõlliste valdadega uueks omavalitsuseks - Valga vallaks. Andmetöötlustegevused ja infosüsteemid on Valga vallas suuremas osas Valga linna senistega sarnased, seega auditi tulemusel Valga linnal tuvastatud puudusi ja antud soovitusi saame rakendada Valga vallas.

Valga linnas oli tööl üks IT spetsialist, kes tegeles kogu IT-ga, sealhulgas jõudumööda ISKE nõuete jälgimise ja täitmisega. Suur osa esinenud puuduseid on tulenenud aja- ja ressursipuudusest. Valga vallavalitsuses on ühinemisperioodiks (2017-2018) tähtajaliselt tööl poole kohaga IT arendusjuht. Tema tööülesandeks on muuhulgas ellu viia ja koordineerida ISKE rakendamist ja infoturbe põhimõtete väljatöötamist. Eeldame, et 2018 lõpuks on Valga vallas ISKE seisukohalt olukord paranenud ja puudused likvideeritud.

Valga vallale on auditiga välja toodud puudujäägid ja soovitused arusaadavad. Tarkvaralahenduste valimisel jälgime edaspidi, et tegu oleks riiklike andmekogudega X-Tee vahendusel liidestatava süsteemiga; jälgime, et tarkvarateenuse osutajatega oleks sätestatud turbemeetmete rakendamise ja auditeerimise korraldus; ISKE rakendamise kohustusliku osana määrame infoturbejuhi kas oma töötajatest või tellime teenusena sisse.

Austusega

/allkirjastatud digitaalselt/

Margus Lepik
vallavanem

*Valga linna sümboolikat kasutatakse kuni Valga valla sümboolika kinnitamiseni vastavalt Karula valla, Taheva valla, Tõlliste valla, Õru valla ja Valga linna ühinemislepingu punktile 4.8.

Puiestee tn 8
68203 Valga

766 9900, 5348 9118
valgalv@valgalv.ee
www.valga.ee

ak EE491010202000577004
SEB Pank AS

VILJANDI VALLAVALITSUS

Riigikontroll
Kiriku 2/4
15013 TALLINN

meeli.saksing@riigikontroll.ee

Teie: 12.04.2018 nr 2-1.9/50094/2

Meie: 14.05.2018 nr 2-8/1952-1

Vastus kontrollaruandele

Viljandi Vallavalitsusel puuduvad täiendavad kommentaarid ja parandusettepanekud kontrolliaruande eelnõule.

(allkirjastatud digitaalselt)
Alar Karu
vallavanem

VÕRU VALLAVALITSUS

Ines Metsalu-Nurminen
Riigikontroll
riigikontroll@riigikontroll.ee

Teie 12.04.2018 nr 2-1.9/50094/2

Meie 26.04.2018 nr 15-7/1251-1

Arvamus kontrolliaruande "IT-turvameetmete süsteemi rakendamine kohalikes omavalitsustes"

KOVis on ISKE meetmestiku rakendamine hädavajalik infovarade turvalisuse tagamiseks. Võru Vallavalitsus võtab Riigikontrolli poolsed soovitused kuulda ning on asunud olukorda parandama, olles esiteks määranud infoturbega seotud ülesannete täitja ning teadvustanud olukorra tõsidust juhtkonna tasandil. Hetkel on käsil kaasaegse infoturbe poliitika välja töötamine ning siit edasi jätkatakse järk-järgult ISKE rakendamist.

Lugupidamisega

(allkirjastatud digitaalselt)

Karl Kuningas
IT-peaspetsialist

7868801
karl.kuningas@voruvald.ee