TARTU ÜLIKOOL

Pärnu kolledž

Ettevõtlusosakond

Triin Vasli

EESTI INFOTURBESTANDARDI RAKENDAMINE MAAELU TEADMUSKESKUSE NÄITEL

Magistritöö

Juhendaja: Linda Rosenkron, MA

Kaasjuhendaja: Arvi Kuura, PhD

Pärnu 2024

Soovitan suunata kaitsmisele (allkirjastatud digitaalselt)

Linda Rosenkron

(allkirjastatud digitaalselt)

Arvi Kuura

Kaitsmisele lubatud

TÜ Pärnu kolledži programmijuht (allkirjastatud digitaalselt)

Gerda Mihhailova

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

(allkirjastatud digitaalselt)

Triin Vasli

SISUKORD

SISSEJUHATUS

Tänapäeva digitaalses maailmas on infosüsteemid, digiandmed ja infoturve avalike ülesannete täitmiseks vajalike äriprotsesside lahutamatu osa. Küberkuritegevus on aga kasvutrendis ja selle maastik pidevas muutumises, mistõttu on väga oluline küberturvalisuse tagamise eest hoolt kanda.

Küberrünnakud on muutunud järjest sagedasemaks, mitmekesisemaks ja on aina tõsisemate tagajärgedega (ENISA, 2023, lk 4) ning küberkuritegevuse tase kasvab nii maailma mastaabis (Morgan, 2023), Euroopa tasandil (ENISA, 2023, lk 4) kui ka Eestis (Justiitsministeerium, 2022), mistõttu on küberturvalisusega seotud riskide teadlik juhtimine möödapääsmatult oluline.

Küberkuritegevusest eriti ohustatuna nähakse avalikku sektorit, mis omab küberruumis suurtes kogustes isikuandmeid ja tundlikku teavet (Coppolino *et al*, 2018, lk 573). Küberkuritegevus võib mõjutada avalike teenuste toimimist, põhjustada andmelekkeid ja intellektuaalomandi varguseid (Coppolino *et al*, 2018, lk 573; Wirtz & Weyerer, 2017, lk 1085), mis võib omakorda kasvatada kodanike usaldamatust oma riigi vastu (Shandler & Gomez, 2023, lk 359). Eestis nähakse küberturvalisust osana riigikaitsest (Riigi Infosüsteemi Amet, 2023), sest see võib seada ohtu riigi julgeoleku ja inimeste turvalisuse. Seega on avalikke ülesandeid täitval asutusel vaja ühiskonna turvalisuse tagamiseks pöörata infoturbealaste riskide maandamisele erilist tähelepanu.

Teadlik infoturbega tegelemine riigi, organisatsiooni ja indiviidi tasandil võimaldab ennetada ja hallata küberturvalisusega seotud riske, samuti toimunud rünnetele oskuslikumalt reageerida. Infoturbe ülesanne organisatsiooni tasandil on säilitada äriprotsesside käigus töödeldava teabe turvalisus (Riigi Infosüsteemi Amet, 2020). Selle jaoks töötati Eestis 2021. aastal välja uus standard – Eesti infoturbestandard (E-ITS), mis on kohustuslik kõigile Eesti riigi avalikele asutustele, kellele kohaldub küberturvalisuse seadus. Eesti õigusruumile vastav standard pakub senisest terviklikuma

ja protsessipõhise lähenemise küberriskide vastu võitlemiseks. Kokku lepitud infoturbe juhtimise standardi rakendamine on oluline, et tagada riigi ja kodanike turvalisus.

Riigi Infosüsteemi Amet (RIA) on välja töötanud eestikeelse juhendmaterjali standardile üleminekuks, kuid E-ITSi rakendamine tekitab kohuslaste seas siiski probleeme, sest nõuab infoturbe juhtimist protsessipõhiselt. Peamised raskuskohad on seni avaldunud mõistete „protsess“ ja „teenus“ defineerimises ja protsesside tuvastamises, juhendi universaalne sõnastus jääb kohuslaste jaoks kaugeks ja raskusi esineb ka juhendi mõistmisel oma asutuse kontekstis. (Sotsiaalministeeriumi sisedokumentatsioon, 2023) Protsessi- ja teenuspõhine juhtimine on riigis kasutusel sünonüümidena ja ühtne lähenemine definitsioonide osas puudub (Kalbus, 2023, lk 29). Teenuspõhine juhtimismudel on avaliku sektori jaoks harjumuspärane (Sotsiaalministeeriumi sisedokumentatsioon, 2023), kuid protsessipõhine lähenemine, mida nõuab E-ITS, võõras, mis omakorda avaldab mõju ka E-ITSi rakendamisele.

Standardi rakendamine oli aga küberturvalisuse seaduse kohuslastele kohustuslik 2024. aastast, mis näitab probleemi aktuaalsust. Autorile teadaolevalt on Eestis mitmeid avalikke asutusi, kes ei ole seni E-ITSi rakendanud, sealhulgas ka Regionaal- ja Põllumajandusministeeriumi (ReM) valitsemisalasse kuuluv teadus- ja arendusasutus Maaelu Teadmuskeskus (METK), mille näitel käesolev magistritöö tehakse.

Eeltoodust tulenevalt sõnastatakse käesoleva magistritöö uurimisprobleem järgnevalt: E-ITS on kohuslastel rakendamata, mistõttu ei täida asutused seadusega ette antud kohustust ning seeläbi seavad ohtu Eesti riigi ja kodanike küberturvalisuse.

Magistritöö eesmärgiks on tuvastada asjaolud, mis on takistanud METKil E-ITSi seni rakendamast ja teha ettepanekud nende takistuste ületamiseks ning E-ITS rakendamiseks. Eesmärgi saavutamiseks kaardistatakse METKi infoturbealane hetkeolukord ja selle seotus ReMiga ning viiakse läbi standardile kohased ettevalmistused E-ITSi rakendamiseks asutuses.

Töö eesmärgist lähtuvalt püstitab autor alljärgnevad uurimisküsimused:

1. Millised takistused on Maaelu Teadmuskeskusel E-ITSi rakendamisel?
2. Millised on võimalused nende takistuste ületamiseks?

Uurimisküsimustele vastuste leidmiseks kasutab autor peamiste meetoditena dokumendianalüüsi ja poolstruktureeritud intervjuusid.

Käesolev magistritöö koosneb kahest peatükist. Töö teoreetiline osa ehk esimene peatükk käsitleb infoturbe juhtimist avalikus sektoris ja on jaotatud kaheks alapeatükiks. Esimeses alapeatükis annab autor ülevaate infoturbe olemusest ja selle olulisusest avalike ülesannete täitmisel, käsitleb infoturbe standardimist ning infoturbealaste riskide juhtimist. Teises alapeatükis annab autor ülevaate protsessipõhise juhtimise rakendamisest infoturbe terviklikumaks juhtimiseks, protsesside standardimisest ja protsesside ning seotud ressursside mõjust infoturbele.

Olulisemate autoritena leiavad töös kajastamist: M. Dumas, M. Hammer, J. Mendling, M. E. Porter, H. A. Reijers, M. L. Rosa, I. Sommerville, K. Taveter, L. Tredinnick.

Töö empiiriline osa ehk teine peatükk koosneb kolmest alapeatükist ja käsitleb E-ITS rakendamist Maaelu Teadmuskeskuse näitel. Esimeses alapeatükis tutvustab autor E-ITSi olemust, annab ülevaate uuritavast organisatsioonist – Maaelu Teadmuskeskusest ja käesoleva magistritöö raames teostatava uuringu metoodikast.

Teises alapeatükis tutvustab autor töö tulemusi töö etappide põhjal. Lähtuvalt töös püsitatud eesmärgist uurib autor esimeses etapis METKi infoturbealast hetkeolukorda, et selgitada välja võimalikud standardi rakendamist takistavad asjaolud. Teises etapis teeb autor ettevalmistused E-ITSi rakendamiseks asutuses, tuvastades asutuse missioonikriitilised protsessid. Uuringu kolmandas etapis kaardistab ja modelleerib autor asutuse missioonikriitiliste protsesside hetkeolukorra (*as-is*) E-ITSi rakendamiseks vajalikul üldistusastmel ja teostab vastavuskontrolli (Ernst & Young Baltics, 2012, lk 14), veendumaks protsesside vastavuses. Analüüsitud protsessid on E-ITSi edasise rakendamise aluseks METKis.

Kolmandas alapeatükis analüüsib töö autor uuringu tulemusi, kõrvutades neid varasemate teadustöödega ja pakub ettepanekud võimalike takistuste ületamiseks ning E-ITSi rakendamiseks. Lisatulemina pakub töö autor välja ka praktilise ja näitlikustatud meetodi äriprotsesside tuvastamiseks.

Töö peamise sihtrühmana näeb autor METKi juhtkonda ja ReM infoturbejuhti, kes vastutavad infoturbe juhtimise eest ja E-ITSi rakendamise eest METKis. Ettepanekud on suunatud standardi rakendamist takistavate kitsaskohtade ületamiseks ja E-ITSi rakendamiseks METKi näitel. Kõrgem teadlikkus võimaldab asutuse juhtkonnal olla paremini ettevalmistunud võimalikeks küberrünneteks ja tõsta avalike ülesannete täitmiseks vajalike äriprotsesside toimepidevust. Töö tulemused on rakendatavad ka teistele E-ITS kohuslastele, kel esineb takistusi standardile üleminekul ja kes ei ole seda mingil põhjusel veel teinud.

Töö oluliste märksõnadena on autor määratlenud järgmised mõisted: infoturve, avalik sektor, äriprotsess, protsessipõhine juhtimine, standardimine, sotsiotehniline süsteem.

1. INFOTURBE JUHTIMINE AVALIKUS SEKTORIS

1.1. Infoturbe olemus ja olulisus avalikus sektoris

Digitaliseerimine ja tehnoloogia kiire areng on muutnud maailma meie ümber. Viimastel kümnenditel on infosüsteemid saanud ühiskonna lahutamatuks osaks. Need on seotud iga pakutava teenusega ning teenused sõltuvad nende tööst. Digitaliseerimine on olnud avaliku sektori arengus oluline märksõna ja mõjutab sektori poolt pakutavaid teenuseid. See toob endaga aga kaasa ka infoturberiskid, mida nähakse eriti kriitilise probleemina just avaliku sektori asutuste jaoks. Arvestades sektori keerukust, käsitlevate andmete suurt mahtu ja tundlikku olemust, on ülimalt oluline pöörata infoturbele avalikus sektoris kõrget tähelepanu.

Avalikud teenused liiguvad järjest enam elektroonilistesse kanalitesse ning avalike ülesannete täitmisel toetutakse üha enam tehnoloogiale (Wirtz & Weyerer, 2017, lk 1085). Kuna avalik sektor omab küberruumis tohutus kogustes isikuandmeid ning tundlikku teavet, on see muutunud küberkurjategijatele atraktiivseks sihtmärgiks (Coppolino *et al*, 2018, lk 573). Viimaste aastate uuringud näitavad, et ligi 40% kõigist pahavara rünnakutest on suunatud just avaliku sektori organisatsioonide vastu, mis teeb avalikust sektorist enim rünnatud sihtmärgi küberruumis (Coppolino *et al*, 2018, lk 573; Symantec, 2015; Trend Micro, 2015 viidatud Wirtz & Weyerer, 2017, lk 1085 kaudu). Tagamaks avalike teenuste toimimise, on seega ülimalt oluline küberruumi kaitsta.

Küberintsidente peetakse avaliku sektori jaoks väga ohtlikuks, sest rünnakutel võivad olla ulatuslikud ühiskondlikud tagajärjed (Moon, *et al*., 2018, lk 54). Ründe tõttu võib kahjustuda riigi kriitiline infrastruktuur, ohtu võib sattuda avalik kord või inimeste turvalisus, ajutiselt võivad katkeda riigi teenused, toimuda andmelekked ja intellektuaalomandi vargused (Coppolino *et al*, 2018, lk 573; Wirtz & Weyerer, 2017, lk 1085). See võib kasvatada kodanike usaldamatust oma riigi vastu (Riigi Infosüsteemi

Amet, 2020; Shandler & Gomez, 2023, lk 359). Võimalikud kahjud riigile on väga suured.

Euroopa Võrgu-ja Infoturbe Agentuuri (ENISA) 2023. aasta küberruumi ohupildi aruandest selgub, et möödunud aasta küberruumi ohud võis jagada kaheksasse peamisesse kategooriasse:

1. lunavara;
2. pahavara;
3. sotsiaalne manipuleerimine;
4. ohud andmete vastu;
5. ohud kättesaadavuse vastu: teenustõkestusrünnakud;
6. ohud kättesaadavuse vastu: internetipõhised ohud (nt liikluse ümbersuunamine, katkestused või infrastruktuuri hävitamine);
7. informatsiooniga manipuleerimine ja valeinfo levitamine;
8. rünnakud tarneahelate vastu (lk 4).

Lunavararünnakuid ehk rünnakuid, milles nõuti vastutasuks lunaraha, ja teenusetõkestusrünnakuid (DdoS-rünnak) oli 2023. aastal enim (ENISA, 2023, lk 4). 2022. aasta juulis toimus ka Euroopa ajaloo suurim DdoS-rünnak (ENISA, 2022). Viimaste aastate trend näitab, et teenusetõkestusrünnakud muutuvad üha mitmekesisemaks ja keerulisemaks, liikudes järjest enam mobiilsidevõrkude ja asjade interneti suunas, mida nüüd kübersõjas aktiivselt kasutatakse (ENISA, 2023, lk 96). Kuna küberkuritegevus toimub elektroonilises keskkonnas – küberruumis – infosüsteemide ja arvutivõrkude sees, nende abil või nende vastu (Spalevic, 2014, lk 687), on küberkuritegevuse vastu võitlemiseks vajagi küberruumi kaitsta.

Kasvavad turvanõuded ning suuremad riskid on pannud eksperte vaatama infoturvet laiemalt kui lihtsalt infosüsteemide turvalisusena. Kuna infosüsteemid ja kriitilised infrastruktuurid on omavahel läbi põimunud (Moon, *et al*., 2018, lk 54; Wirtz & Weyerer, 2017, lk 1085), on üks võimalik viis vaadata küberturvalisust läbi sotsiotehnilise prisma. Laybats ja Tredinnick väidavad, et infoturve ongi oma olemuselt hoopis inimeste ja nende ettearvamatu loomuse probleem (2016, lk 79). Inimene on ahela nõrgim lüli. Ta on emotsionaalne olend, kes käitub sageli ettearvamatult ja

seletamatult (Laybats & Tredinnick, 2016, lk 79). Inimestel lasub vastutus järgida infoturbepoliitikat, kuid sageli eksivad just nemad, mistõttu on inimfaktori mõjule küberturvalisuse tagamisel kirjanduses ka olulist rõhku pandud (Soomro *et al*., 2015, lk 223).

Inimesed kipuvad eelistama mugavamaid või sisseharjunud teguviise, hoolimata sellest, et nad teavad, et nii ei tohiks (Laybats & Tredinnick, 2016, lk 79) või ei pruugi nad tehnoloogiat kasutada viisil nagu seda on eeldatud (Bella et al, 2015, lk 2). Näiteks võivad inimesed üles kirjutada keerukaid paroole, mida infosüsteemid sageli nõuavad, mis avab ukse uutele riskidele (Bella et al, 2015, lk 2). Küberkurjategijad üritavad inimesi tabada ka õngitsuskirjade kaudu, et haarata seejärel enda valdusesse töötaja kasutajakonto (Pihlak, 2024). Umbkaudu 95% kümberrünnetest toimubki inimeste vastu, mängides lihtsalt inimlike nõrkustega (Kont, 2022, viidatud Tammet, 2023, lk 27 kaudu). Seetõttu tuleb teadlikult pöörata tähelepanu inimese rollile küberturvalisuse tagamisel – tema emotsionaalsele loomusele ja tema harimisele.

Sotsiotehniline süsteem võimaldabki arvesse võtta terviku – inimeste ja süsteemide vastastikuse mõju, rõhutamata üht rohkem kui teist (Malatji *et al*., 2018, lk 256). Ainult heas omavahelises suhtluses ja koostöös saab see süsteem kujuneda väga edukaks (Walker *et al*., 2008, lk 3-4). Ebakõlasid süsteemi sotsiaalse ja tehnilise mõõtme vahel nimetatakse sotsiotehniliseks lõheks (Whitworth 2009, lk 395). Need lõhed peidavad endas infoturberiske (Malatji *et al*., 2018, lk 234). Kuivõrd inimesed kannavad küberturvalisuse tagamisel väga olulist või isegi määravat rolli, on selge, et keskenduda ei saa vaid infosüsteemidele. Tehnoloogia ise ei ole võimeline turvalisust garanteerima. Sommerville (2015, lk 412) toob välja järgmised küberturvalisust negatiivselt mõjutavad tegrid, mis kõik sisaldavad endas inimfaktori mõju:

- teadmatus probleemi tõsidusest;
- turvaprotseduuride ebapiisav rakendamine;
- inimlik muretus ja vähene tähelepanu;
- ebamõistlikud kompromissid kasutusmugavuse vs turvalisuse osas.

Inimfaktor mängib küberturvalisuse tagamisel olulist rolli. Kayworthi ja Whitteni 2010 aastal läbi viidud uuring näitas, et organisatsiooni strateegiline ja tulemuslik infoturbe

strateegia koosnebki kahest elemendist, lisaks infosüsteemide ja tehnoloogia turvalisusele arvestab see ka organisatsiooni sotsiaalseid aspekte (lk 163). Infoturvet tuleb vaadata terviklikult, hinnates äriprotsesside kaudu kogu sotsiotehnilist süsteemi ja seotud riske.

Enamus infoturbealaseid käsitlusi vaatleb infoturvet läbi üldtuntud CIA mudeli: konfidentsiaalsus (*confidentiality),* terviklus (*integrity)* ja käideldavus (*availability)* – tuntud ka kui CIA kolmik (Laybats & Tredinnick, 2016, lk 78; Nweke, 2017, lk 1; Samonas & Coss, 2014, lk 29; Sommerville, 2015, lk 413; ISO/IEC 27001:2022; Eesti infoturbestandard, 2024), kusjuures mudelit on täiendanud infoturbe valdkonna teerajaja, uurija ja konsultant Donn B. Parker, kritiseerides CIA kolmiku tehnoloogilist fookust ja inimfaktori kõrvale jätmist ning rõhutades andmete komplekssemaks muutumist ajas (Pender-Bey, 2016, lk 3,6). Parker täiendas CIA kolmikut kolme elemendiga: autentsus (*authenticity*), omamine/kontroll (*possession/control*) ja kasutatavus (*utility*), pakkudes tänapäeva tingimustesse sobivama ja täielikuma infoturbe mudeli, mis nimetati Parkeri kuuikuks (Pender-Bey, 2016, lk 6). Infoturbe põhikomponentideks on aga endiselt CIA kolmik, mis on aluseks infoturbe terviklikule juhtimisele ja juurutamisele organisatsioonilisel tasandil.

Kui ajalooliselt on küberturvalisust vaadeldud IT-alase probleemina, siis Kayworth ja Whitten (2010) rõhutavad, et tegemist on ärilise probleemiga (lk 164). Organisatsioonides, kus küberturvalisust peetakse endiselt IT-alaseks probleemiks, kipub see jääma madala prioriteediga ja eraldiseisvaks valdkonnaks, mis tegutseb äri poolest sõltumatult ning ei saa juhtkonna poolt piisavalt tähelepanu. Autorid aga rõhutavad, et infoturve peab olema ärilise fookusega ja seda ei saa vaadelda eraldiseisvalt, vastasel juhul võib omavahelise koostöö mittetoimimine kaasa tuua selle, et organisatsiooni infoturbepoliitika ja -eelarve ei ole kooskõlas organisatsiooni tegelike vajadustega. Küberkaitset ei kujundata strateegiliselt, vaid kustutatakse tulekahjusid ja otsused on ajendatud lühiajalistest prioriteetidest. (Kayworth & Whitten, 2010, 164) Samas peidab küberkuritegevus endas selgeid ärilisi riske ning potentsiaalset suurt kahju organisatsioonile.

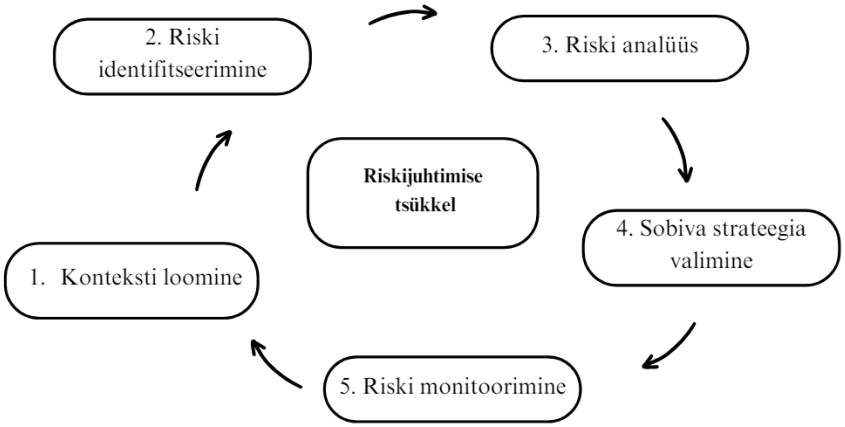
Teave on saanud iga organisatsiooni jaoks kõige väärtuslikumaks varaks (Gebremeskel *et al.*, 2023, lk 44) ja infoturbe ülesanne on hoolitseda selle teabe turvalisuse eest,

tagades seega organisatsiooni toimimise ja teenuste turvalisuse. Infoturbe eesmärgid ei ole eraldiseisvad asutuse eesmärkidest, vaid vajadus infoturbe järele lähtub neist (Eesti infoturbestandard, 2024). Seetõttu, kui varem lasus vastutus küberturvalisuse pärast IT-osakonnal, siis sotsiotehnilisest aspektist vaadatuna nähakse järjest enam määravat rolli infoturbeprotsessis tippjuhtkonnal (Soomro *et al*., 2015, lk 223), kes vastutabki organisatsiooni strateegiliste eesmärkide eest. Juhtkonna pühendumust kui üliolulist aspekti edu tagamiseks, kinnitas ka 2010 aastal Kayworthi ja Whitteni poolt läbi viidud uuring (lk 171).

Lisaks tippjuhtkonna rollile on oluline ära määratleda ka teised olulisemad osapooled ja nende kohustused. Höne ja Eloff (2002) väitel on kindlaks määratud rollid ja nende ülesanded infoturbepoliitika dokumendi üks kõige olulisemaid komponente, aidates vältida vastutuse hajumist, ebaselgust ning mitmeti mõistetavust ülesannetes (lk 404). Oluline on seejuures silmas pidada, et organisatsiooni infoturbealased vajadused saaksid kaetud ja infoturbealased kohustused fikseeritud kõigil töötajatel, kes moel või teisel organisatsiooni teabeallikatega töötavad (Höne & Eloff, 2002, lk 404). Kuna teave ja tehnoloogia on seotud iga protsessiga ja puudutavad tänapäeval suuremal või vähemal määral igaüht, on seega oluline harida kõiki organisatsiooni töötajaid.

Kuna küberruum peidab endas alati riske ja küberkuritegevus on -kaitsest reeglina sammu võrra ees, on küberriskide mõistmisele ja maandamisele vaja pöörata olulist tähelepanu, et missioonikriitilised protsessid ei katkeks ning avalikud teenused toimiksid tõrgeteta. Riskist, sh küberriskist võib mõelda kui millestki, mida organisatsioon ei taha, et juhtuks (Sommerville, 2015, lk 644). Infoturve põhinebki nende potentsiaalsete ohtude mõistmises ja võimalike riskide maandamises (Laybats & Tredinnick, 2016, lk 79). Kusjuures kahju ei pea olema alati rahaline või otseselt rahas mõõdetav. Küberrünne võib ohustada näiteks ka organisatsiooni mainet, selle usaldusväärsust või konkurentsivõimet. Mainekahju võib olla nii tõsine, et organisatsioon ei pruugi sellest enam taastuda. (Fenz *et al*., 2014, lk 420) Seetõttu on tõhusa küberjulgeoleku poliitika väljatöötamine ning edasi arendamine saanud mitmete riikide jaoks prioriteediks, et küberriskidega paremini toime tulla (Spalević, 2014, lk 689). Süsteemne ja terviklik riskijuhtimine küberturvalisuse tagamiseks on vajalik.

Terviklik riskijuhtimine organisatsioonis eeldab selget ja määratletud protsessi (Samimi, 2020, lk 131) ja riskide maandamine peab samuti olema integreeritud organisatsiooni olulisemate protsessidesse (Kayworth & Whitten, 2010, 163). Erinevad autorid (Blank & Gallagher, 2012, lk 4; Eesti infoturbestandard, 2024; Hoo, 2000, lk 7; Kliem, 2000, viidatud Muehlen & Ho, 2005, lk 457 kaudu; Sommerville, 2015, lk 648-649) jagavad riskijuhtimise raamistiku etappideks mõnevõrra erinevalt, kuid põhilised etapid ja nende sisu jäävad üldjoontes siiski samaks ja on välja toodud alljärgneval joonisel 1.



Joonis 1. Riskijuhtimise etapid. Allikad: Blank & Gallagher, 2012, lk 4; Eesti infoturbestandard, 2024; Hoo, 2000, lk 7; Kliem, 2000, viidatud Muehlen & Ho, 2005, lk 457 kaudu; Sommerville, 2015, lk 648-649

Konteksti loomine esimeses etapis aitab mõista raamistikku, milles riskihaldust läbi viiakse. Järgmisena tuleb võimalikud riskid tuvastada ja teostada riskide analüüs, mille käigus riskid järjestada ning hinnata, millised riskid vajavad kiireimat tähelepanu. Organisatsiooni jaoks katastroofilise või tõsise tagajärjega riskidega, mille realiseerumise tõenäosus on mõõdukast suurem, tuleks tegeleda esimesena (Sommerville, 2015, lk 649). Seejärel tulebki valida sobiv toimetulekustrateegia ning olukorda seirata.

Kuivõrd riskid on pidevas muutumises, on väga keeruline ennustada, kust kurjategijad järgmisena ründavad. Ressurss, mida täna ignoreeritakse, võib juba järgmisel päeval küberründe alla sattuda, mistõttu tuleb riskihalduse puhul alati arvestada asjaoluga, et riskid võivad varitseda ootamatutes kohtades (Fenz *et al*., 2014, lk 420). Seda peab meeles pidama ka protsesse kaasajastades, mil infoturvet unustada ei tohi. Uute

haavatavuste tuvastamine peab pidevalt muutuva küberkuritegevuse maastiku tõttu toimuma võimalikult varakult (Hariyanti *et al.*, 2021, lk 1). Protsessi omanik peab oskama märgata ja adresseerida infoturbealaseid riske, mis tema poolt juhitud muutustega kaasa võisid tulla. Tähelepanuta jäänud riskid võivad õõnestada kodanike usaldust tehnoloogia ning avalike teenuste vastu.

Oluline on mitte ainult adresseerida probleemi tõsidust ja olla teadlik kaitsemeetmetest, vaid kaitsemeetmeid organisatsioonis ka rakendada, et kaitsta infrastruktuuri ning oma valduses olevaid andmeid (Coppolino *et al*, 2018, lk 577; Wirtz & Weyerer, 2017, lk 1098). Teisalt tuleb silmas pidada efektiivsuse aspekti, sest mida tugevamad ja mitmekihilisemad on turvaprotseduurid, millest potentsiaalne ründaja peab läbi murdma, seda aeglasemaks muutuvad protsessid ja süsteemid (Sommerville, 2015, lk 414). See omakorda võib aeglustada või lausa takistada igapäevast töö tegemist, pannes töötajad omakorda otsima mugavamaid lahendusi ja turvameetmetest mööda hiilima.

Oluline on leida tasakaal ja teatud juhtudel võibki olla otstarbekam riskiga ka leppida, kui selle elimineerimine on liiga kulukas või muud moodi ebamõistlik. Riske, millega organisatsioon otsustab leppida, võib nimetada jääkriskideks (Eesti infoturbestandard, 2024; ISO/IEC, 2004, viidatud Kaul, 2008, lk 20 kaudu). Infoturbealane riskijuhtimine nõuab arvestamist nii rünnakust tulenevate rahaliste kui ka mainekahjudega, samuti tuleb arvesse võtta turvaprotseduuride ja -tehnoloogiate kulusid, mis võivad neid kahjusid vähendada. Kuivõrd tegemist on äriliste kaalutluste ja otsustega, ongi see üks põhjustest, miks on infoturbe juhtimine äriline, mitte tehniline ülesanne. (Sommerville, 2015, lk 380) Sobiv strateegia riskiga toimetulekuks on asutuse juhtkonna otsustada.

Riskihaldus on pidev protsess. Seda lihtsustab asjaolu, et kõik ohud ei ole organisatsioonispetsiifilised. Veldre tõi oma diplomitöös „Eesti infoturbestandardi protsessimudeli evalveerimine“ välja, et „ ... olukorras, kus enamik organisatsioone kasutavad ühetaolist standardtarkvara, tarbivad ühetaolist Internetti, milles enamik ohtusid polegi organisatsioonispetsiifilised, vaid on samuti ühetaolised, sellises olukorras saavad ühetaolised olla ka meetmed, millega neid ohtusid erinevates organisatsioonides tõrjutakse“ (2021, lk 18). Etalonturve ehk tüüpne minimaalne turvameetmestik koondabki need ühetaolised meetmed ja võimaldab organisatsioonil infoturbealaseid teadmiseid ja praktikaid lihtsa vaevaga taaskasutada (Eesti

infoturbestandard, 2024; Cybernetica, 2023; Riigi Infosüsteemi Amet, s. a.-a). Samas tõdeb Sommerville (2015), et oluline on vaadelda infoturbealast riskihaldust laiemalt kui vaid tehnilisest vaatenurgast, sest rünne ei pruugi olla alati tehnoloogiapõhine ja nõrkused võivad asuda ka mujal, näiteks ei pruugi olla asutuse ruumid kõrvaliste isikute eest piisavalt kaitstud (lk 381). Seetõttu on oluline vaadelda riskihaldust organisatsioonis tervikuna.

Küberruumi pidev muutumine, küberkuritegevuse kasv ja ootamatutes kohtades varitsevad riskid on infoturbe valdkonnas viinud standardimise vajaduseni. Valdkondlikud standardid aitavad küberturvalisuse maailmas orienteeruda ja pakuvad välja kokku lepitud protseduurid, suunised, meetodid ja tööriistad, et tagada ajakohane, piisav ja rahvusvaheliste suundumustega kooskõlas olev küberturvalisuse tase (Alexei, 2021, lk 85, 93). Standardiks võib lugeda dokumenti, mis on konsensuse alusel kehtestatud ja pakub kokku lepitud reeglid ja juhised teatud tegevuste või nende tulemite kohta, eesmärgiga saavutada kindlas kontekstis teatav tase (ISO, 1996, viidatud Münstermann & Weitzel, 2008 kaudu; Kanada standardinõukogu, *n.d.*).

Standardimisel nähakse mitmeid kasutegureid. Selge raamistik varade, protsesside ja ressursside kaitsmiseks võimaldab organisatsioonil keskenduda strateegiliste eesmärkide saavutamisele (Syafrizal *et al*., 2020, lk 417) ja aitab aja ja raha säästmise arvelt suurendada tootmist ja kasumit, minimeerida riske ning tõsta äri toimepidevust (Syafrizal *et al*., 2020, lk 418). Purser (2014, lk 98) rõhutab standardimise olulisust rahvusvahelise koostöö tagamisel – riikide vahel kokku lepitud reeglid võimaldavad ulatuslike küberintsidentide korral üheskoos efektiivselt reageerida. Küberruum muutub aga kiiresti ja selleks, et standarditest oleks turvalisuse tagamisel kasu, peavad need uuenema võrreldavas tempos, vastasel juhul võib standard olla välja andmise hetkel juba aegunud või rakendatav vaid osaliselt (Purser, 2014, lk 100). Kuna standardite väljatöötamine on pikaldane protsess, on see ohukoht, millega tuleb arvestada.

Maailmas pidevalt kasvav küberkuritegevus ohustab enim just avaliku sektori asutusi. Kuna kuritegevusel võivad olla ulatuslikud tagajärjed, tuleb küberturvalisuse tagamisele avalikus sektoris pöörata suurt tähelepanu. Ajalooliselt IT-alast probleemi nähakse järjest enam ärilisest vaatenurgast, sest küberrünne peidab endas asutuse jaoks ärilisi riske ja peamist ohtu põhjustavad just inimesed, kelle eest IT-osakond vastutada ei saa.

Oluline on vaadelda organisatsiooni tervikuna, mistõttu kannab asutuse juhtkond küberturvalisuse tagamisel olulist rolli. Kuna küberruum muutub pidevalt ja riskid võivad varitseda ootamatutes kohtades, on infoturbe standardimine ja terviklik riskijuhtimine parema kaitse tagamiseks vajalik. Küberturvalisuse tagamiseks on vaja vaadelda organisatsiooni tervikuna.

1.2. Infoturberiskide haldamine rakendades protsessipõhist juhtimist

Kuivõrd infoturve peidab endas ärilisi riske ja inimene mängib küberturvalisuse tagamisel väga olulist rolli, ei saa infoturvet enam vaadelda ainuüksi infosüsteemide turvalisusena. Üks võimalik viis infoturbe juhtimiseks on protsesside põhine. Protsessipõhine vaade infoturbele võimaldab vaadelda tervikut, hoides fookuses organisatsiooni strateegilised eesmärgid, mida infoturve teenima peab ja mida protsesside kaudu saavutatakse, ning pöörates tähelepanu inimese rollile organisatsiooni olulistes protsessides.

Organisatsioon, mis kasutab protsessipõhist juhtimist, seab töö korraldamisel ja juhtimisel fookusesse protsessid ning nende pideva täiustamise (Dumas *et al*., 2018, lk 8). Protsess on üksikute tegevuste ja otsuste kogum, mis, asetades laiemasse konteksti koos teiste ülesannetega, on kombineerituna tulemuslikum ning loob kliendile väärtust (Dumas *et al*., 2018; lk 27; Hammer, 2010, lk 11). Üks protsessijuhtimise alusprintsiipe on, et igasugune protsess on parem kui protsessi puudumine. Täpselt ära määratletud protsesside puudumisel valitseb kaos ja tulemused ei ole järjepidevad ning neile ei saa loota. Selgelt ära määratletud protsess toob etteaimatava ja järjekindla tulemuse ja võimaldab luua arendusteks vastava pinnase (Hammer, 2010, lk 11). Hammer (2007, lk 3) on sõnastanud efektiivse protsessi viis kriitilist edutegurit:

1. protsessi täidetavate üksikute ülesannete järjekord peab olema hästi läbi mõeldud - kelle poolt, millal, kus, millistel tingimustel, millise infoga jne;
2. protsessil peavad olema mõõdikud;
3. protsessil peab olema omanik;
4. protsessil peavad olema kindlaks määratud rollidega täitjad;

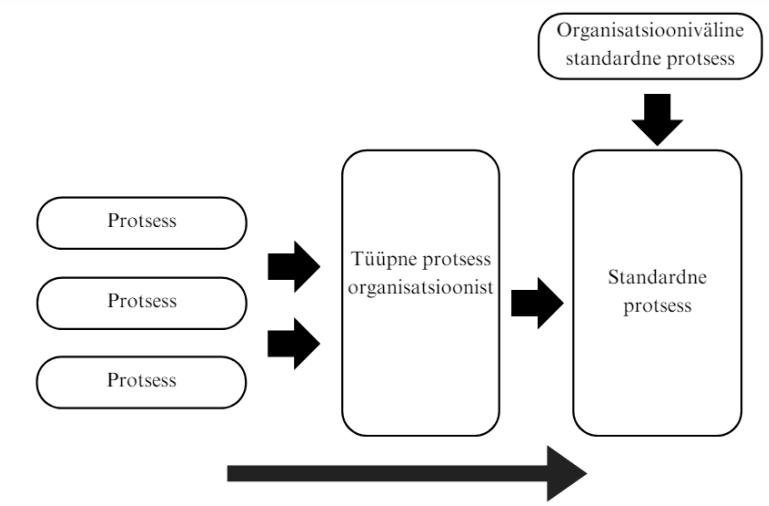
5. peab olema selge protsessi toetav infrastruktuur ehk erinevad tugisüsteemid ja tugiprotsessid.

Seega annab selgelt defineeritud protsess ülevaate omavahel seotud tegevustest, mis on protsessi kvaliteedi tagamiseks olulised, ressurssidest, mis on protsessiga seotud ning ka riskidest, mida on vaja maandada. Kui protsessid ei ole selged, pole ülevaadet ka riskidest, mis neid protsesse ohustavad.

Standardimine aitab riske maandada ja protsesse tõhustada. Protsesside standardimise eesmärk on saavutada järjepidevus organisatsiooni põhilistes protsessides, võimaldades optimeerida kulusid ja tagada kõrge kvaliteet (Goel *et al*., 2023, lk 195). Standardimine võimaldab luua stabiilsust ja vajadus selle järele on olnud praktiline – lihtsustada seal, kus variatiivsus ei loo väärtust ja tagada kvaliteet tarbijatele ning võrdsus tootjatele (Maistre, 1931, lk 329-330). Protsesside standardimist uurinud Münstermann & Weitzel (2008) nimetasid protsesside standardimise põhiliste kasuteguritena:

- protsessi jõudluse paranemise;
- kõrgema valmisoleku muutustele reageerimiseks;
- protsesside eraldamise neid toetavatest IT-lahendustest ja seega parema valmisoleku kasutada standardseid IT-lahendusi;
- vigade vähenemise ja kõrgema kvaliteedi tagamise ning usaldusväärsuse saavutamise.

Münstermann & Weitzel (2008) pakuvad protsesside standardimiseks välja kahesammulise protsessi, ühtlustades protsessid esmalt ühe tüüpse protsessi suhtes ja täiustades selle pinnalt tüüpset protsessi standardseks protsessiks või tuues standardse protsessi organisatsiooni väljastpoolt ning korrigeerides seejärel fookuses olevad protsessid standardse protsessi järgi. Protsesside standardiseerimist on visualiseeritud alljärgneval joonisel 2.



Joonis 2. Protsesside standardimine. Autori koostatud Münstermann & Weitzel 2008 põhjal.

Goel *et al*. (2023, lk 204-206) analüüsisid 60 protsesside standardimise valdkonna artiklit, mille tulemusel pakkusid protsesside standardimiseks seitsmesammulise valemi:

1. üksikute protsessivariantide dokumenteerimine;
2. protsessi jagamine olulisemateks sammudeks ja alamprotsessideks;
3. põhiprotsessi (*master process*) tuvastamine;
4. erisuste välja sõelumine;
5. võimalike parenduste sisse viimine põhiprotsessi;
6. täiustatud põhiprotsessi aktsepteerimine standardse protsessina;
7. protsessivariantide kohandamine standardse protsessi järgi.

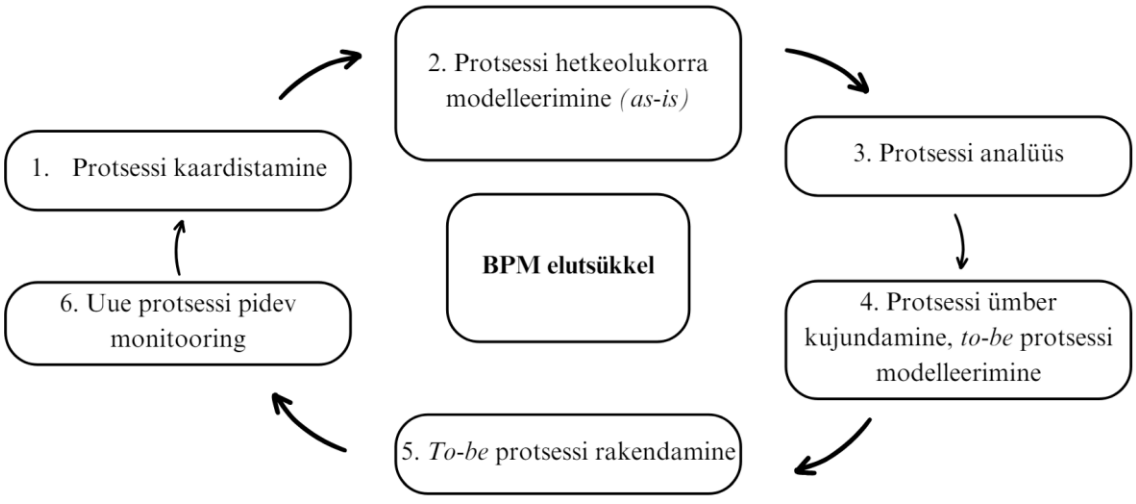
Protsesside standardimine hõlmab endas mitmeid kasutegureid. Kuna standarditud protsessid tagavad järjepidevalt samasuguse tulemuse, võimaldab standardimine omada täielikku ülevaadet protsessile rakenduvatest küberriskidest, mis vastasel juhul oleks puudulik. Täielik ülevaade küberriskidest aitab omakorda tagada organisatsiooni piisava küberturvalisuse taseme. Protsesside standardimine on oluline osa protsessipõhisest juhtimisest.

Protsessipõhise juhtimisega alustades tuleb organisatsioonil arvestada, et töö protsessidega ei ole ühekordne tegevus. See ei ole lineaarne, vaid pidev tsükkel, mis põhineb Demingi laialdaselt tunnustatud pideva parendamise ringil – PDCA tsüklil.

Demingi ring koosneb neljast etapist: planeerimine (*plan*), teostamine (*do*), kontrollimine (*check*) ja reageerimine (*act*). (Ernst & Young Baltics, 2012, lk 40-41; Hammer, 2010, lk 6; Kalbus, 2023, lk 13). Kuigi erinevad autorid käsitlevad protsessijuhtimise elutsükli etappe mõnevõrra erinevalt, jääb sisu siiski samaks ning üldistatult võib eristada kuute olulisimat etappi (Dumas et al, 2018, lk 22-24; Pereira *et al*., 2019, viidatud Geller, 2021, lk 12 kaudu; Sulis & Taveter, 2022, lk 21):

1. kaardistamine ja probleemi defineerimine;
2. hetkeolukorra (*as-is*) modelleerimine;
3. analüüs, mille käigus tuvastatakse protsessi probleemkohad;
4. ümberkujundamine, mille käigus tuvastatakse võimalikud parenduskohad ja modelleeritakse parendatud (*to-be*) protsess;
5. uue protsessi rakendamine, mille käigus tehakse vajalikud muudatused, et ümberkujundatud protsessi oleks võimalik edukalt täita;
6. ümber kujundatud protsessi pidev monitooring, mille käigus jälgitakse uuendatud protsessi tulemuslikkust.

Andmaks edasi protsessipõhise juhtimise elutsüklit, on etapid üldistatult visualiseeritud alljärgneval joonisel 3. Tegemist on üldtunnustatud, kuid käesoleva töö vaatest olulise mudeliga, mistõttu on see töös visualiseeritud.



Joonis 3. Protsessipõhise juhtimise elutsükkel. Allikas: Dumas *et al*, 2018, lk 22-24

Kuna käesoleva magistritöö fookus on äriprotsesside hetkeolukorra (*as-is*) ülevaatel ja töös ei käsitleta protsesside parendamist (*to-be*), mida ei nõua ka Eesti infoturbestandard, on autor käesoleva töö teoreetilises raamistikus võtnud vaatluse alla protsessipõhise juhtimise esimesed kolm etappi.

Protsessipõhisele juhtimisele üleminek algab hetkeolukorra kaardistamisest. Iga muudatus on ressursimahukas, mistõttu on vaja organisatsioonis esmalt mõista, millist probleemi ning millisel eesmärgil sellega lahendada püütakse (Dumas & et al, 2018, lk 17). Kuna protsess peab looma väärtust kliendile ja olema kooskõlas organisatsiooni eesmärkidega, on protsessipõhise juhtimisega algust tehes vaja sõnastada organisatsiooni eesmärk ja alameesmärgid (Muehlen & Ho, 2005, lk 457; Sulis & Taveter, 2022, lk 77).

Seejärel on oluline tuvastada protsessid, mis on sõnastatud eesmärkide elluviimiseks olulised ning panna paika ka protsesside skoop ja protsesside omavahelised seosed ning seotud rollid (Dumas & et al, 2018, lk 17). Protsesside määratlemine ja parendamine on ressursimahukas töö, mistõttu on soovituslik alustada prioriteetsetest ehk strateegiliselt olulistest ja suurimat mõju avaldavatest protsessidest (Dumas et al, 2018, lk 35). Protsessid, mis toetavad organisatsiooni eesmärkide saavutamist ning on organisatsiooni ellujäämise seisukohast olulise tähtsusega ongi prioriteetsed protsessid (Dumas et al, 2018, lk 35) ehk missioonikriitilised äriprotsessid (Eesti infoturbestandard, 2024).

Missioonikriitiliste äriprotsesside tuvastamiseks võib esmalt modelleerida protsesside maastiku (*process landscape model*), mis on laialt levinud mudel protsessidest tervikliku ülevaate saamiseks (Dumas et al, 2018, lk 48). Teine võimalus on kasutatada aga eesmärgipõhist lähenemist ja esimese mudelina eesmärgimudelit, sest infoturve lähtub organisatsiooni eesmärkidest. Alustades eesmärgimudelist, on tegemist hierarhilise abstraktsiooniga – ülalt alla lähenemisviisiga, raamistades esmalt tervikpildi organisatsioonist ning liikudes seejärel sügavamale (Sulis & Taveter, 2022, lk 77). Eesmärgimudel võimaldab visualiseerida asutuse strateegilised eesmärgid, mis on protsesside kaardistamisel oluliseks esmaseks sisendiks.

Organisatsioon on sotsiotehniline süsteem, mis on loodud selleks, et teatud eesmärke saavutada või ülesandeid ellu viia (Sommerville, 2015, lk 303). Eesmärgimudel sobib

keerulise sotsiotehnilise süsteemi raamistamiseks, kus suhtlevad omavahel erinevad osapooled – nii sotsiaalsed kui ka tehnilised (Sterling & Taveter, 2009, 3). See mudel aitab mõista ja visualiseerida asutuse eesmärke ja nende täitmiseks vajalikke äriprotsesse, andes ülevaate sellest, mida infoturve teenima peab. Mudel toob prioriteetsed protsessid esile, aidates mõista protsesside seotust organisatsiooni operatiivtasandi ja strateegilise tasandi eesmärkidega (Guizzardi & Reis, 2015, lk 1).

Samuti toob eesmärgimudel esile, kas protsessid ja tegevused on üldse kooskõlas asutusele seatud eesmärkidega (Guizzardi & Reis, 2015, lk 1) ja millised rollid on protsessidega seotud ning vajalikud eesmärkide saavutamiseks (Sterling & Taveter, 2009, 65; Sulis & Taveter, 2022, lk 79). Mudelis eristatakse kahesuguseid eesmärke: funktsionaalsed eesmärgid ja kvaliteedieesmärgid. Funktsionaalsed eesmärgid viitavad sellele, mida sotsiotehniline süsteem peab saavutama ja kvaliteedieesmärgid koos olulisemate tulemusnäitajatega kirjeldavad süsteemi olemust, milline see olema peab (Sulis & Taveter, 2022, lk 79; lk 85).

Funktsionaalseid eesmärke võib mudelis defineerida kui soovitud olukorda tulevikus, mille nimel tuleb näha vaeva. Need põhinevad motiividel ja on mõõdetavad. (Sterling & Taveter, 2009, 30) Eesmärkidel võivad olla ka alameesmärgid, kus iga alameesmärk panustab kõrgema taseme eesmärgi teatud aspekti saavutamisse (Sterling & Taveter, 2009, 31; Sulis & Taveter, 2022, lk 84). Mudelis seotakse funktsionaalsed eesmärgid rollide, kvaliteedieesmärkide ja olulisemate tulemusnäitajatega. Defineeritud funktsionaalsed eesmärgid viitavadki organisatsiooni prioriteetsetele äriprotsessidele, määratledes eesmärkide saavutamise järjekorra (Sulis & Taveter, 2022, lk 83). Seega ühilduvad eesmärgimudeli funktsionaalsed eesmärgid vastava üldistustasemega äriprotsessidega.

Rolle võib mudelis defineerida kui mingit kindlat kompetentsi või positsiooni, mida on konkreetse eesmärgi täitmiseks vaja (Sterling & Taveter, 2009, 32). Rollid peegeldavad ülesandeid ja vastutust, mis protsessis osalevatele inimestele on antud, et eesmärk saavutada (Sommerville, 2015, lk 44; Sterling & Taveter, 2009, 3). Rollide vastutuse määratlemine annab omakorda sisendi protsesside modelleerimisse, kus vastutust on võimalik ümber sõnastada sooritatud ülesannetena (Sulis & Taveter, 2022, lk 87). Rollide määratlemisel on mõistlik otsida ühisosasid ja võimalusi üldistamiseks ning

grupeerimiseks, kus see on võimalik (Sommerville, 2015, lk 152). Tervikpildi säilitamise huvides ei ole mõistlik laskuda liigsesse detailsusesse.

Eesmärgimudeli kasutamise puhul on oluline mõista, et selle ülesanne ei ole olla uuritava süsteemi alternatiivne esitus, vaid keerulise süsteemi abstraktsioon (Sommerville, 2015, lk 139). Mudel on kõrge abstraktsiooniastmega ja selle väärtus seisnebki mudeli lihtsasti mõistetavuses erinevatele osapooltele, ka IT-kaugele inimesele (Lopez-Lorca, *et al.,* 2018, lk 30; Sterling & Taveter, 2009, 65; Sommerville, 2015, lk 139). Lihtsuse huvides ei kajastata eesmärkide saavutamisel ajalist järgnevust (Rosenkron, 2022, lk 9). See mudel on sobilik kasutamiseks esimese mudelina, mis annab raamistiku, et eesmärkide saavutamiseks vajalike protsesside kaardistamisega vajadusel süvitsi minna.

Eesmärgimudel erineb teistest eesmärgipõhises nõuete analüüsis (*Goal-oriented requirements engineering – GORE*) kasutatud mudelitest nagu näiteks *i** või KAOS selle poolest, et see mudel võimaldab lihtsustamist ja sobib hästi kasutamiseks just mittetehniliste osapooltega suhtlemisel, sest kirjapandut on lihtne hoomata (Lopez-Lorca *et al.,* 2018, lk 30). Selle loomisel on oluline küsida sisendit osapooltelt, kel on ülevaade organisatsiooni strateegilistest eesmärkidest ning suundadest. Töötajate kaasamisele eesmärgimudeli loomisel aitab kaasa juhtkonna tugi (Lopez-Lorca, *et al.,* 2018, lk 32). Eesmärgimudeli notatsioon on esitatud tabelina töö lisas 1.

Kuivõrd organisatsioonis on protsesse palju, aitab ka protsesside kategoriseerimine luua selgust. Äriprotsesside kategoriseerimise võimalusi on erinevaid. Üks kõige levinumaid kategoriseerimisviise on Porteri poolt 1985. aastal tutvustatud väärtusahela mudel (lk 38), mis jaotab protsessid kaheks: tuumikprotsessid (*core process*) ja tugiprotsessid (*support proccess*). Kolmanda kategooriana lisati hiljem juurde ka juhtimisprotsessid (*management proccess*). Nende kolme kategooria eristamine on organisatsiooni jaoks strateegilise tähtsusega (Dumas *et al.,* 2018, lk 41). Organisatsiooni tuumikprotsessideks nimetab Porter protsesse, mis loovad väärtust väliskliendile, olles seega äritegevuse jaoks hädavajalikud. Avaliku sektori puhul võib seega tuumikprotsessideks pidada äriprotsesse, mis aitavad ellu viia organisatsioonile määratud avalikke ülesandeid. Tugiprotsessid toetavad tuumikprotsesside täitmist ja loovad väärtust sisekliendile (Hammer, 2010, lk 11; Muehlen & Ho, 2005; lk 455).

Nendeks võib nimetada näiteks kommunikatsiooni, värbamist, arendustegevusi, finantsjuhtimist jne.

Protsesse on lähtuvalt vajadusest võimalik kaardistada väga erineval detailsusastmel. Sõltuvalt eesmärgist ja vajadusest peab iga organisatsioon ise otsustama, kui üldiselt või detailselt on vaja protsessid kaardistada, millisel tasemel on võimalik probleemkohti defineerida ja need likvideerida. Kui kaardistust tehakse esmakordselt, on otstarbekas kaardistada kõigepealt üldpilt ning panna paika raamistik. Ameerika produktiivsuse ja kvaliteedi keskuse (APQC) välja töötatud ja üldtunnustatud protsesside kvalifikatsiooni raamistik eristab viite üldistustaset (2023):

- I tasand – kategooria/valdkonna tasand (määratleb organisatsiooni protsessid kõige üldisemal valdkondlikul tasemel, protsesside maastik);
- II tasand – protsesside grupi tasand (tähistab erinevaid alamprotsesse protsesse, mis moodustavad ühe suurema grupi);
- III tasand – alamprotsessi tasand (detailsem tasand, mis võtab fookusesse ühe protsessi, hõlmates ühes protsessis kõiki I tasandi protsessi hädavajalikke elemente);
- IV tasand – tegevuste tasand (näitab III tasandi protsessi edukaks täitmiseks vajalikke võtmetegevusi);
- V tasand – ülesande tasand (üksikute ülesannete üles loetlemine on kõige detailsem tasand protsesside kaardistamises).

Protsessile tuleb määrata ka omanik, kes protsessi eest vastutab, selle hetkeolukorda regulaarselt seirab ja võimalikke parenduskohti otsib. Oluline on paika panna ka omaniku kohustused, millest olulisemate hulka kuuluvad (APQC, 2024, lk 3; Ernst & Young Baltics, 2012, lk 12):

- protsessi eesmärkide ja mõõdikute määratlemine;
- võtmetähtsusega edutegurite tuvastamine;
- vastutamine protsessi eesmärkide saavutamise eest ning mõõdikute jälgimine;
- protsessiga seonduva õigusruumi jälgimine ja muudatustega kursis olemine;
- protsessi regulaarne seire ja seotud muudatuste juhtimine;
- protsessiga seotud dokumentatsiooni ajakohasena hoidmine;
- protsessi, seotud eesmärkide ja tegevuste tutvustamine osapooltele.

Kui prioriteetsed äriprotsessid on kaardistatud ning omanikud määratletud, on kasulik protsesside hetkeolukord (*as-is*) ka modelleerida. Protsesse visualiseerides on võimalik juba detailselt ära kaardistada iga protsessiga seotud rollid ja ressursid, selgelt adresseerida probleemkohti ning näha ka võimalikke parenduskohti. Protsesside visualiseerimine aitab märgata ka seoseid erinevate protsesside vahel.

Sulis ja Taveter (2022, lk 77-78) jagavad äriprotsesside modelleerimisviisid kolme kategooriasse:

1. Tegevuspõhine *(activity-oriented)* lähenemisviis – rõhuasetus on üksikutel tegevustel ning nende järjestusel.
2. Kasutajapõhine *(agent-oriented)* lähenemisviis – rõhuasetus on protsessis osalevatel rollidel ja nende ülesannetel, keskendutakse protsessi elluviijatele.
3. Tootepõhine *(product-oriented)* lähenemisviis – rõhuasetus on toodetel ja toodete muutumisel ajas.

Olgugi, et protsesside modelleerimiseks on erinevaid keeli, domineerib tänapäeval tegevuspõhine lähenemisviis. Üks tunnustatumaid ja enim kasutatud tegevuspõhiseid äriportsesside modelleerimise notatsioone on BPMN-notatsioon, mis on saanud standardkeeleks protsesside visualiseerimisel ja analüüsil (Aagesen & Krogstie, 2010, lk 213; Dumas et al, 2018, 17; Hariyanti et al., 2021, lk 3; Sulis & Taveter, 2022, lk 89). Seda notatsiooni kasutab protsesside modelleerimiseks paljuski ka Eesti avalik sektor (Ernst & Young Baltics, 2012, lk 7), mistõttu kasutatakse BPMN notatsiooni ka käesolevas töös. BPMN-notatsiooni põhilised elemendid on tabelina välja toodud lisas 2.

Hoolimata tegevuspõhisest lähenemisviisist, on ka protsesse modelleerides oluline säilitada kasutajast lähtuv mõtteviis (Sulis & Taveter, 2022, lk 78). Kuivõrd protsesside kaardistamine ja modelleerimine hõlmab väga suurt osa organisatsioonist, on juhtkonna tugi selles projektis olulise tähtsusega. Sõltuvalt sellest, millisel üldistustasemel soovib organisatsioon protsesside kaardistamist ja modelleerimist läbi viia, võib kaaluda ka vastutava meeskonna moodustamist organisatsioonis, kelle ülesannete hulka võivad kuuluda:

- protsesside kaardistamiseks ja modelleerimiseks vajaliku info koondamine;

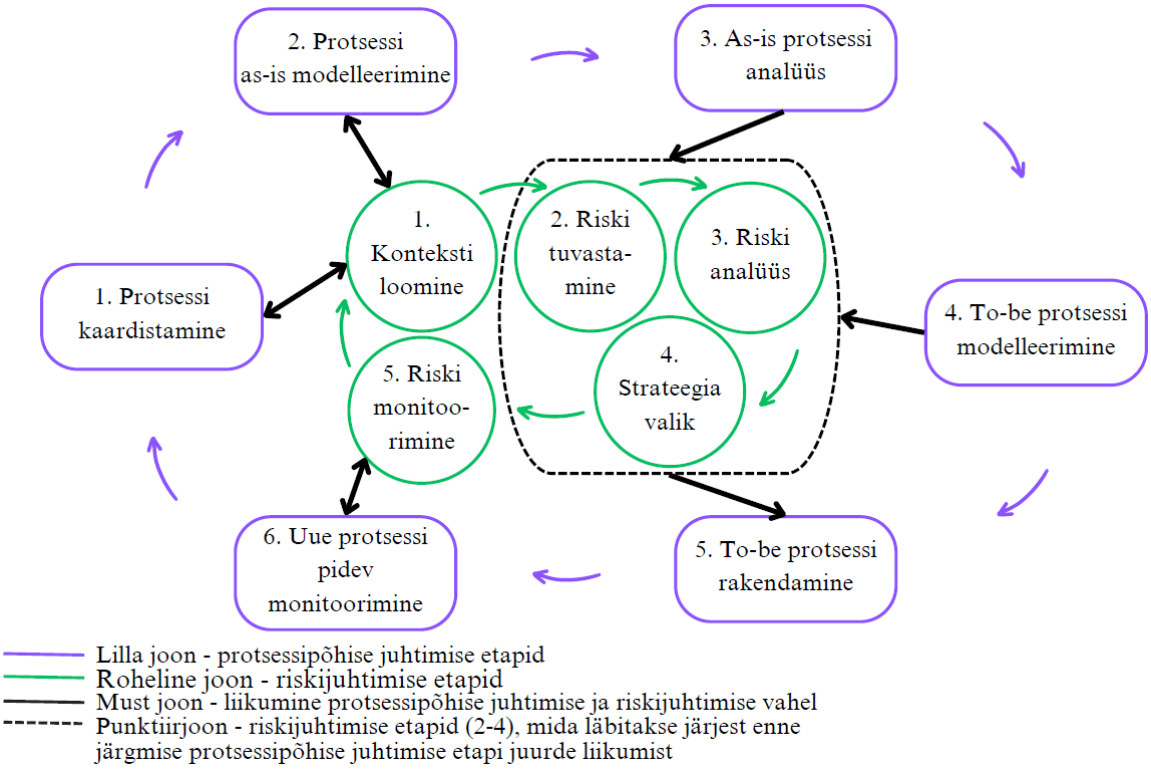
- töövahendite ja -metoodika valik;
- protsesside nimekirja ja kirjelduste koostamine ühtsetel alustel;
- protsesside modelleerimine (Ernst & Young Baltics, 2012, lk 12).

Kuna avalikke ülesandeid täidetakse läbi teatud protsesside, on üks võimalus juhtida ka infoturvet protsessipõhiselt, käsitledes ja kaitstes organisatsiooni protsesse tervikuna. Kasutamaks ära digitaliseerimise potentsiaali on vaja muuta avalike teenustega seotud äriprotsessid turvaliseks (Gebremeskel *et al*., 2023, lk 44). Protsessipõhine lähenemine aitab mõista, millised protsessid on avalike ülesannete täitmiseks olulised, millised ressursid on nende protsessidega seotud ning millised võimalikud infoturbealased riskid protsesse ohustavad. Protsessipõhine lähenemine võtab infoturbe juhtimisel arvesse terve sotsiotehnilise süsteemi ning seab vastutuse organisatsiooni juhtkonnale, mitte enam IT-osakonnale.

Prioriteetsete protsesside kaardistamisel infoturbe eesmärgil, tuleb kaasatud ressurssidele pöörata väga olulist tähelepanu, sest nemad avaldavad mõju ka protsessi küberturvalisusele. Kaardistamine ja modelleerimine aitab asutusel paremini mõista ka infosüsteemide ja tehnoloogia rolli protsessides ning adresseerida ja analüüsida võimalikke infoturbealaseid riske, mis protsessile rakenduvad. Kuna äriprotsessidesse on põimitud infotehnoloogia ja infosüsteemid hõlmavad endas alati interaktsiooni – sisend- ja väljundandmeid, et soovitud tulem tekiks – on infoturbealase olukorra kaardistamisel oluline saada aru, kuidas siseneb informatsioon äriprotsessidesse ning kus kohas protsessides peituvad haavatavused (Sommerville, 2015, lk 144). Ebakõlad sotsiaalse ja tehnilise mõõtme vahel (Laybats & Tredinnick, 2016, lk 79) või sotsiotehnilised lõhed, nagu Whitworth (2009, lk 395) neid nimetanud on. Sotsiotehniliste lõhede avastamiseks on oluline tuvastada äriprotsessidega seotud rollid ja rakendused, andmekogud ning -baasid. Muuhulgas nähakse infotehnoloogial ka võtmetähtsusega rolli äriprotsesside parendamisel (Dumas et al, 2018, lk 24), mistõttu ei saa tehnoloogiast ning infoturbest protsessipõhise juhtimise rakendamisel üle ega ümber.

Kuna protsessipõhise juhtimise elutsüklit rakendades (vt joonis 3, lk 19) on oluline tähelepanu pöörata ka infoturbealastele riskidele, mis protsessile rakenduvad või mis protsessi parendades ilmneda võivad (Hariyanti *et al*., 2021, lk 1), peab riskide

juhtimine (vt joonis 1, lk 13) olema osa protsessi juhtimisest ja seda ei saa vaadelda eraldiseisvana. Joonisel 4 visualiseeritud mudel võtab protsessipõhist elutsüklit järgides arvesse ka riskijuhtimise etapid – arvestab protsessile rakenduvate riskidega ning tegeleb nende maandamisega. Tegemist on autori poolt koostatud mudeliga, mis põhineb alljärgnevatel allikatel.



Joonis 4. Protsessipõhise juhtimise elutsükkel, mis arvestab ka protsessile rakenduvate riskide juhtimist. Allikad: Blank & Gallagher, 2012, lk 4; Dumas *et al*, 2018, lk 22-24; Eesti infoturbestandard, 2024; Hariyanti *et al.*, 2021, lk 1; Hoo, 2000, lk 7; Kliem, 2000, viidatud Muehlen & Ho, 2005, lk 457 kaudu; Sommerville, 2015, lk 648-649

Protsessipõhise juhtimise esimeses kahes etapis luuakse riskijuhtimiseks vajalik kontekst, mille järgselt liigutakse protsessipõhise juhtimise kolmandasse – protsessi hetkeolukorra analüüsi etappi ja tuvastatakse ning analüüsitakse ka protsessile rakenduvaid riske ning valitakse sobiv strateegia riskide maandamiseks ehk liigutakse läbi riskijuhtimise 2-4 etapi. Seejärel liigutakse protsessipõhise juhtimise neljandasse – protsessi parendamise etappi. Kuna oluline on teadvustada ja maandada ka infoturbealaseid riske, mis kaasnevad protsessi parendamisega (Hariyanti *et al*., 2021, lk

1), korratakse seejärel riskijuhtimise 2-4 etappi. Edasi liigutakse parendatud (*to-be*) protsessi rakendamise juurde ja viimaks tegeletakse uue protsessi ja protsessile rakenduvate riskide pideva monitoorimisega.

Kokkuvõtvalt võib öelda, et kuna inimesed kannavad küberturvalisuse tagamisel väga olulist rolli, ei saa infoturbe juhtimine keskenduda vaid infosüsteemidele. Infoturvet tuleb vaadata terviklikult, mis on viinud vajaduseni arendada seda protsessipõhiselt. Protsessipõhine lähenemine infoturbe juhtimisele võimaldab hoida fookuses organisatsiooni strateegilised eesmärgid ning seab vastutuse juhtkonnale, mitte enam IT-osakonnale.

Ülevaade protsesside hetkeolukorrast aitab organisatsioonil mõista, millised on tuumikprotsessid, millised ressursid on nendega seotud ja millised võimalikud infoturbealased ohud protsesse ohustavad. Alles seejärel saab tegeleda nende riskide maandamisega. Kuna terviklik riskijuhtimine eeldab selget protsessi ja riskide maandamine peab samuti olema integreeritud organisatsiooni olulistesse protsessidesse, tuleb protsesside ja riskide juhtimist vaadelda tervikuna.

Terviklik lähenemine ja ärilise fookuse seadmine aitab juhtida infoturvet strateegiliselt ning – arvestades nii tehnoloogilisi haavatavusi kui ka inimmõju – tagada avalike ülesannete täitmiseks vajalike tuumikprotsesside kaitse.

Kuna inimesed kannavad küberturvalisuse tagamisel olulist rolli, on vaja selgelt määratleda ka infoturbe juhtimisega seotud rollid ja vastutus organisatsioonis ning töötajaid harida.

2. EESTI INFOTURBESTANDARDI RAKENDAMINE MAAELU TEADMUSKESKUSES

2.1. Infoturve Eestis, ülevaade Maaelu Teadmuskeskusest ja uuringu metoodikast

Magistritöö käigus viidi läbi empiiriline uuring ReM haldusalas asuvas riiklikus teadus-arendusasutuses Maaelu Teadmuskeskus (METK), mida autor töö teises peatükis tutvustab. Käesolevas alapeatükis annab autor ülevaate Eestis kehtivast infoturbestandardist E-ITS ja selle peamistest erinevustest võrreldes 2022. aastani kehtinud ISKE standardiga, samuti uuritavast organisatsioonist – METKist, kel on kohustus standardit rakendada. Autor tutvustab ka uuringu ülesehitust ja selle etappe.

Eestis mõisteti küberturvalisuse olulisust juba 2008. aastal, mil Eestist sai esimene Euroopa Liidu liikmesriik, kus töötati välja riiklik küberjulgeoleku strateegia. Strateegia töötati välja vastuseks 2007. aastal Pronksiööle järgnenud küberkriisile, mil mastaapsete teenusetõkestusrünnete ehk DDoS-rünnete tõttu said kurjategijad ligi valitsusasutuste veebilehtedele, ajutiselt suleti välissministeeriumi ja justiitsministeeriumi kodulehed, blokeeriti hädaabiliin 112 ja pihta said ka erakondade, pankade ning Eesti meediaväljaannete veebilehed (Traynor, 2007; Vaks, 2018, lk 2).

2022. aastal ületas RIA poolt registreeritud küberrünnakute arv 2007. aasta oma kohati juba 100-kordselt, mis näitab küberkuritegevuse aktiivsust ja suurt kasvu ka Eesti riigis (Riigi Infosüsteemi Amet, 2023, lk 10). Kuivõrd küberkuritegevus ohustab avalikku sektorit ja julgeolekurisk on ilmne, on vaja avalikke teenuseid kaitsta ja infoturvet avalikus sektoris prioritiseerida. Tagamaks riigiüleselt infoturbe ühtse taseme ja teenuste turvalisuse, on riigid välja töötanud infoturbestandardeid. Eestis kehtib 2023. aastast alates Eesti infoturbestandard (E-ITS).

E-ITS on Eestile kohaldatud ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks, mis lepib riiklikult kokku reeglid küberturvalisuse tagamiseks ja põhineb rahvusvahelisel standardil ISO/IEC 27001 (Eesti infoturbestandard, 2024). Rahvusvahelise Standardimisorganisatsiooni ehk ISO poolt välja antud infoturbestandard ISO/IEC 27001 on maailma tuntuim ja enim kasutatud rahvusvaheline infoturbe juhtimise standard, mis annab juhised infoturbe juhtimisüsteemi loomiseks ja selle pidevaks haldamiseks (Rahvusvaheline Standardimisorganisatsioon, 2022). E-ITS asendab aastatel 2003-2022 kehtinud infosüsteemide kolmeastmelise etalonturbe süsteemi ehk ISKE (Riigi Infosüsteemi Amet, s. a.-b). E-ITS ei ole Eesti Standardimis- ja Akrediteerimiskeskuse poolt heaks kiidetud standard, eesmärgiga vältida standardi tasuliseks muutumist ja ametlike standardite pikka välja töötamise ning uuendamise tsüklit (Purser, 2014, lk 100), võimaldades seega standardi paindlikuma uuendamise RIA poolt (Tammet, 2023, lk 25).

E-ITS põhineb riskijuhtimisel, vaatleb organisatsiooni tervikuna ja selle eesmärk on tagada avalike ülesannete täitmiseks vajalike äriprotsesside ja infosüsteemide kõikehõlmav kaitse, et hoida avalikud teenused turvalised, andmed kaitstud ja tagada protsesside jätkusuutlik toimimine. Standardi loojaks ja omanikuks on RIA ja selle järgimine on kohustuslik kõigile avalikke ülesandeid täitvatele asutustele. Standardile üleminekuks oli aega kolm aastat. Alates 2024. aastast on selle rakendamine kohustuslik.

Kehtivuse lõpetanud ISKE ja hetkel kehtiva E-ITSi olulisimad aspektid ja peamised erinevused on välja toodud alljärgnevas tabelis 1.

Tabel 1. ISKE ja E-ITS standardi võrdlus

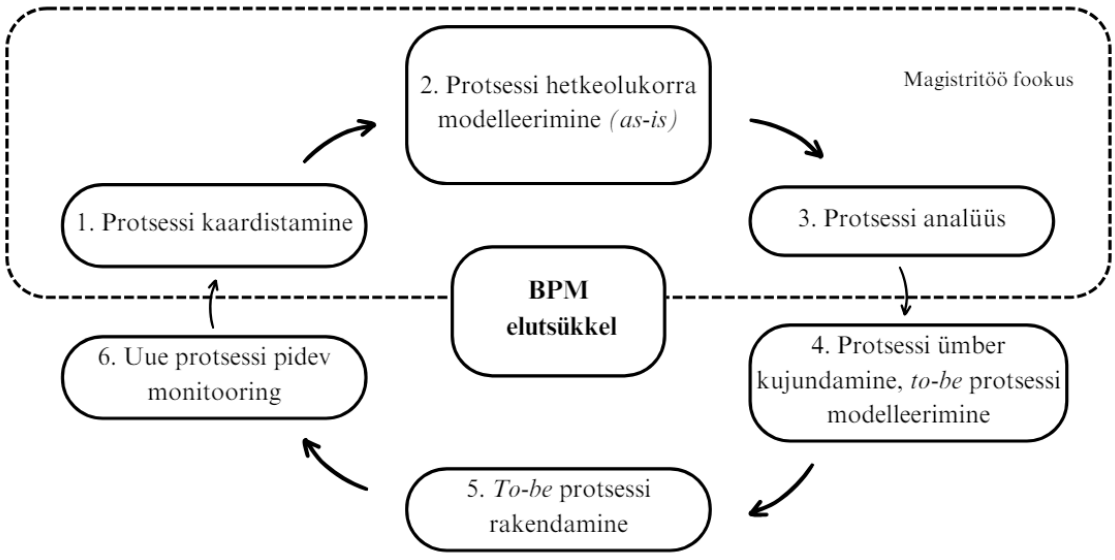
Valdkond	**ISKE**	**E-ITS**
Periood	Riiklik infoturbe juhtimise standard aastatel 2003-2022	Alates 2023. aastast kehtiv riiklik infoturbe juhtimise standard
Rakendajad	Eesti avaliku sektori asutused, kohalikud omavalitsused, IT-majad	Eesti avaliku sektori asutused, kohalikud omavalitsused, avalik-õiguslikud juriidilised isikud, põhiseaduslikud institutsioonid - kõik, kellele kohaldub küberturvalisuse seadus. Kasutamiseks ka erafirmadele.
Vastavus ISO/IEC 27001:2022 standardiga	Ei ole seotud	Seos olemas
Turvameetmestik	Etalonturve	Etalonturve ja riskipõhine
Kaitseala	Andmekogu	Äriprotsess
Vastutus	IT-osakond	Juhtkond
Riskihaldus	Tähelepanuta jäid süsteemide mittetüüpsed lahendused, mis oleksid vajanud eraldi riskihaldust.	Mittetüüpsete lahenduste või kõrge kaitsetarbe puhul on võimalik väline riskihaldus.
Murekohad	Standardi keerukus ja mahukus rakendajatele hirmutav ja eemaletõukav, ressursside puuduse tõttu paljud turvameetmed rakendamata, töömaht võis osutuda ebarealistlikuks.	Protsessi ja teenuse definitsioonid kokku leppimata, protsesside tuvastamine keeruline, standardi universaalsus jääb kaugeks ja raske mõista oma asutuse kontekstis.

Allikad: Eesti infoturbestandard, 2024; Riigi Infosüsteemi Amet, s.a.-a, s. a.-b; Seeba, 2019, lk 12; Sotsiaalministeeriumi sisedokumentatsioon, 2023; Veldre, 2021, lk 24

E-ITSi ja ISKE standardi peamine erinevus seisneb kaitseala määratlemises ja vastutuse jagunemises. Kui ISKE puhul oli kaitsealaks andmekogu, siis E-ITSi puhul lähtutakse kaitsetarbe määramisel äriprotsessidest ehk asutust vaadatakse tervikuna. E-ITSi puhul langeb vastutus asutuse juhile ja standard annab juhile suurema otsustusvabaduse kaitsemeetmete rakendamisel. Kui ISKE puhul lasus vastutus sageli IT-teenust pakkuval partneril, näiteks Maaelu Teadmuskeskuse puhul ReM-il, siis E-ITSi puhul vastutab asutuse juht äriprotsesside turvalisuse ja sellega seonduvate riskide eest. Seetõttu on standardi edukal rakendamisel väga oluline juhtkonna teadlikkus, kaasatus ning teema olulisuse teadvustamine. Juhtkonna kõrval rõhutab E-ITS ka infoturbejuhi rolli, kelle ülesanne on hoida juhtkonda olukorra ja vajadustega kursis. Väiksemates

organisatsioonides võib infoturbejuhi kohustusi täita mõne teise ametikoha esindaja, näiteks andmekaitsespetsialist (Eesti infoturbestandard, 2024).

Standardi rakendamine annab asutusele parema arusaama avalike ülesannete täitmiseks kasutatavatest äriprotsessidest ja protsessidega seotud riskidest. Selge ülevaade omakorda aitab tõsta organisatsiooni toimepidevust. (Eesti infoturbestandard, 2024) E-ITSi vaatest on protsessid väga kõrgel tasemel üldistatud ning jäävad pigem abstraktseks. Standard ei nõua protsessidega süvitsi minemist, kui just organisatsioon ise selleks vajadust ei näe. E-ITSi vaatest võib organisatsioonil olla ka vaid üks põhiline protsess, mille ülesanded, rollid ja ressursid kaardistatakse. Samas jätab standard organisatsioonile vabaduse vajaduse korral rohkem protsesse luua ja hallata. (Sotsiaalministeeriumi sisedokumentatsioon, 2023) Standard ei nõua protsesside parendamist, vaid oluline on äriprotsesside hetkeolukorra (*as-is*) vaade ja selle dokumenteerimine. Sellest lähtuvalt on käesoleva magistritöö fookus protsessipõhise juhtimise kolmel esimesel etapil, mis on joonisel 5 tähistatud punktiirjoonega. Käesolev joonis põhineb protsessipõhise juhtimise üldtunnustatud etappidel (vt joonis 3, lk 19).



Joonis 5. Protsessipõhise juhtimise elutsükkel (Dumas *et al*, 2018, lk 22-24) ja käesoleva magistritöö fookus.

Sotsiaalministeeriumi poolt tellitud E-ITSi pilootprojekt näitas, et standardile ülemineku tuumikmeeskond võiks olla võimalusel kolmeliikmeline ja koosneda kolme valdkonna esindajatest (Sotsiaalministeeriumi sisedokumentatsioon, 2023):

1. IT esindaja (näiteks IT-juht, infoturbejuht või teisi sarnaseid ülesandeid täitev isik);
2. Äri valdkonna esindaja (näiteks kvaliteedijuht, arendusjuht või teisi sarnaseid ülesandeid täitev isik);
3. Juriidiline tugi (näiteks jurist, andmekaitsespetsialist või teise ametinimetusega sarnaseid ülesandeid täitev isik).

Tuumikmeeskonna moodustamisel on rõhk vajaminevatel kompetentsidel, mitte niivõrd konkreetsetel ametikohtadel. Äriprotsesside hetkeolukorra kaardistamisel on oluline, et meeskonnas oleks olemas teadmine äriprotsessidest kui sellistest ning võimekus neid protsesse analüüsida. Samuti on oluline IT-alane kompetents. Olgugi, et E-ITS ei kohusta juriidilise toe kaasamist projekti, näitas pilootprojekt, et juriidilised teadmised on niivõrd spetsiifilised ja enim probleeme esineb just õigusvaldkonnas, mistõttu on võimaluse korral mõistlik kaasata vastutav isik õigusalastes küsimustes. (Sotsiaalministeeriumi sisedokumentatsioon, 2023)

E-ITS on rakendamiseks kohustuslik ka ReMi haldusalasse kuuluvale METKile, millel käesolev uuring põhineb. METK loodi 1. jaanuaril 2023. aastal, mil ühendati Eesti Taimekasvatuse Instituut ja Põllumajandusuuringute Keskus. METKi loomise eesmärk oli „... tekitada teadus-arendus kompetents, mis ühendab omavahel sordiaretuse, taimekasvatuse, mulla, agrokeemia, keskkonnaseire ning sotsiaalmajanduslike uuringute valdkonnad“ (Pajumägi, 2022). Üldistatult võib öelda, et METK tegeleb valdkondliku teaduse loome, erinevate uuringute, katsete ja analüüside teostamise ning teadmuse jagamisega. METKi põhimääruses (2023) on asutuse tegevusvaldkondadena välja toodud neli põhisuunda:

1. „põllumajanduse, maaelu ja maamajanduse valdkonna uuringud, seire, hindamine ja analüüsid, sealhulgas laboratoorsed analüüsid;
2. põllumajanduskultuuride sordiaretus ja põldkatsed;
3. põllumajandus- ja maaeluvaldkonna teadmussiirde-, nõuande- ja innovatsiooniteenused;
4. Euroopa Liidu ühise põllumajanduspoliitika rakendamiseks vajalikud tegevused“.

Keskuse tööd juhib direktor, kelle alla kuulub kolm asedirektorit: innovatsiooni ja ettevõtluse valdkonna asedirektor, teaduse valdkonna asedirektor ning laborite ja

katsekeskuste valdkonna asedirektor. (Maaelu Teadmuskeskuse põhimäärus, 2023) Maaelu Teadmuskeskuse teadus-arendustegevuste tööd koordineerib asutuse juures tegutsev 11-liikmeline teadusnõukogu (Kõiv, 2023). METKi labori- ja katsekeskuse pakutavad teenused on osa riiklikust taimetervise, sööda- ja toiduohutuse alasest kontrollisüsteemist ning on akrediteeritud. Laborid on akrediteeritud vastavalt standardile EVS EN ISO/IEC 17025:2017 ja katsekeskused on sertifitseeritud vastavalt standardile ISO 9001 (Maaelu Teadmuskeskus, 2023). Tulenevalt standardi nõuetest on METKi laborite ja katsekeskuste protsessid üksikasjalikult kaardistatud, kuid terviklik ülevaade METKi äriprotsessidest puudub ja asutuseülest kaardistust varasemalt tehtud ei ole. Samuti ei ole määratud protsesside eest vastutajaid ega kaardistatud rolle, kes ja millistesse protsessidesse panustab.

METKi IT- ja infoturbe juhtimise vastutus on jagatud ReMi ja asutuse vahel. ReM IT-osakonna põhiline ülesanne on korraldada infosüsteemide arendamine, haldamine, majutamine, hooldus ning pakkuda IT-alast tuge. Samuti vastutab ministeerium infotehnoloogilise turvapoliitika väljatöötamise ja rakendamise eest valitsemisala üleselt. Asutusepõhine infoturbe juhtimine kuulub asutuse juhi pädevusse. (ReM sisedokumentatsioon, 2020) METK on E-ITSi kohuslane, kuid asutuses ei ole uuele infoturbe juhtimise standardile üleminekut alustatud, mis ajendas käesolevat uuringut METKis läbi viima.

Empiiriline uuring põhineb magistritöö teoreetilisel osal ja RIA poolt E-ITSi rakendamise nõuetel. Töö autor viis 2024. aasta veebruari- ja aprillikuu jooksul läbi kolmeetapilise uuringu, mille tulemusel tegi omapoolsed ettepanekud standardi rakendamist takistavate asjaolude ületamiseks ning standardi rakendamiseks. Selle jaoks kaardistati METKi infoturbealane hetkeolukord ja tehti ettevalmistavad tegevused E-ITSi rakendamiseks asutuses. Uuring koosnes järgmistest etappidest:

1. etapp: infoturbealase hetkeolukorra kaardistamine;
2. etapp: ettevalmistavad tegevused E-ITSi rakendamiseks: missioonikriitiliste äriprotsesside tuvastamine läbi asutuse strateegiliste eesmärkide (eesmärgimudel);
3. etapp: ettevalmistavad tegevused E-ITSi rakendamiseks: missioonikriitiliste protsesside modelleerimine ja sidumine ressurssidega.

Uuringu vältel kasutatavateks põhilisteks andmekogumismeetoditeks olid dokumendianalüüs ja poolstruktureeritud intervjuud. Uuringu läbiviimise etapid, andmekogumise meetodid ja ajakava on kokkuvõtvalt välja toodud magistritöö lisas 7.

Selleks, et selgitada välja, millistele dokumentidele tugineb ja milliste põhimõtete alusel toimub infoturbe juhtimine METKis, teostas autor veebruarikuus esmalt dokumendianalüüsi, mis põhines järgmistel METKi ja ReMi sisemistel dokumentidel:

- Maaelu Teadmuskeskuse põhimäärus;
- Regionaal-ja Põllumajandusministeeriumi infotehnoloogia (IT) osakonna põhimäärus (aastast 2020);
- Maaeluministeeriumi ja ministeeriumi infosüsteemiga liitunud ministeeriumi valitsemisala asutuste infoturbe poliitika (aastast 2020);
- kvartaalsete IT-kohtumiste memod ministeeriumi ja asutuse vahel (2023-2024).

Dokumendianalüüs andis esmase ülevaate asutuse infoturbealasest hetkeolukorrast, mille pinnalt viis autor läbi poolstruktureeritud intervjuud ReMi infoturbejuhiga ning METKi direktoriga, et saada parem ülevaade tegelikust hetkeolukorrast infoturbe juhtimisel, kaardistada olulisemate teemadena rollijaotus, ministeeriumi- ja asutusevaheline koostöö, E-ITSile üleminek ning mõlema osapoole ootused infoturbele. Tuginedes teooriale ja dokumendianalüüsile kannavad mõlemad osapooled olulist rolli infoturbe juhtimisel, mistõttu nad uuringusse kaasati.

Autor viis intervjuud läbi märtsikuus ja need toimusid videokonverentsiplatvormi Skype vahendusel ning kestsid orienteeruvalt tunni. Intervjuud salvestati osalejate eelneval nõusolekul märkmete tegemise tarbeks. Intervjuu ReM infoturbejuhiga (intervjuukava leitav lisast 3) toimus 11. märtsil ning intervjuu METKi direktoriga (intervjuukava leitav lisast 4) 15. märtsil. Poolstruktureeritud intervjuud andsid autorile võimaluse keskenduda olulisimatele teemadele, säilitades samas piisava paindlikkuse, et hetkeolukorda hinnates intervjuu kulgu vastavalt muuta või küsida vajadusel täpsustavaid küsimusi. Intervjuu tulemusi analüüsiti kvalitatiivsel sisuanalüüsi meetodil (Õunapuu, 2014, lk 171-172), mis võimaldas võtta arvesse osapoolte arvamused, hinnangud ning hoiakud. Intervjuukavad on välja toodud käesoleva töö lisades 3 ja 4. Uuringu käigus läbi viidud dokumendianalüüs ja poolstruktureeritud intervjuud aitasid

autoril leida ühisosa ja puudujääke infoturbealase teoreetilise käsitluse ning päriselu vahel.

Uuringu teises etapis teostas autor dokumendianalüüsi eesmärgiga saada ülevaade METKile antud avalikest ülesannetest, asutuse funktsionaalsetest ja kvaliteedieesmärkidest ning mõõdikutest. Dokumendianalüüs põhines asutuse sisedokumentatsioonil, mh põhimäärusel, arengukaval, huvide konflikti ohuolukordi maandavad meetmed METKi sordi ja seemnekasvatuse valdkonnas (HUKO) ning muudel strateegilist vaadet käsitlevatel dokumentidel (vt lisa 7). Neist kõige olulisemaks sisendiks eesmärgimudeli konstrueerimisel peab autor asutuse vastvalminud arengukava (2024-2035). Dokumendianalüüsi pinnalt konstrueeris autor esialgse eesmärgimudeli Drawio vabavaralise tarkvara abil, mida valideeriti ja täiendati asutuse strateegiajuhiga läbi viidud poolstruktureeritud intervjuude käigus. Strateegiajuhile suunatud intervjuukava on leitav lisast 5.

Intervjuusid strateegiajuhiga viidi läbi kaks tükki, mille tulemusel valmis lõplik asutuse eesmärgimudel. Teise intervjuu käigus teostati eesmärgimudeli vastavuskontroll ning täiendati mudelit vajadusest lähtuvalt. Eesmärgimudeli konstrueerimiseks vajalikud intervjuud asutuse strateegiajuhiga toimusid märtsikuu jooksul videokonverentsiplatvormi Skype vahendusel ning kestsid kumbki 1,5 tundi. Intervjuud salvestati osaleja eelneval nõusolekul märkmete tegemise tarbeks, need transkribeeriti ja teostati kvalitatiivne sisuanalüüs (Õunapuu, 2014, lk 171-172). Eesmärgimudel võimaldas autoril tuvastada asutuse missioonikriitilised protsessid.

Uuringu kolmandas etapis, võttes aluseks eesmärgimudeli kaudu tuvastatud missioonikriitilised äriprotsessid, viis autor läbi poolstruktureeritud intervjuu, et kaardistada ja modelleerida üldisel tasandil METKi missioonikriitiline äriprotsess, mis on aluseks E-ITSi rakendamisel. Intervjuu viidi läbi põllumajandusuuringute osakonna juhatajaga (intervjuukava on leitav lisast 6), kel on hea teadmine äriprotsessidest kui sellistest, terviklik ülevaade asutuse eesmärkidest ja protsessidest ning võimekus näha tervikpilti, protsesse kõrgel tasemel üldistada ja analüüsida (Sotsiaalministeeriumi sisedokumentatsioon, 2023). Samuti on tema vastutusalas mitmeid kriitilise tähtsusega andmebaase, mille kaardistamine on E-ITSi rakendamise seisukohast oluline. Protsess

modelleeriti intervjuu pinnalt BPMN notatsiooni toetava Camunda vabavaralise protsesside modelleerimise tarkvara abil.

Saadud tulemuste pinnalt viis autor läbi vastavuskontrolli, et veenduda modelleeritud protsessi ja tegeliku protsessi vastavuses (Ernst & Young Baltics, 2012, lk 14). Kirjalik vastavuskontroll viidi läbi põllumajandusuuringute osakonna juhatajaga ja intervjuud METKi teadustegevuse valdkonna ja laborite ning katsetegevuse valdkonna asedirektoriga, kel mõlemal on oluline vastutusala tuvastatud äriprotsessis.

Vastavuskontrolli intervjuud viis autor läbi mudeli graafilise esitluse põhjal, mille käigus tutvustas töö autor modelleeritud äriprotsessi ja seotud ressursse. Intervjuud asedirektoritega toimusid videokonverentsiplatvormi Skype vahendusel, kestsid kumbki 30-60 minutit ja need salvestati osalejate eelnevalt nõusolekul märkmete tegemise tarbeks. Intervjuudest saadud tagasiside alusel tehti modelleeritud protsessi vajalikud parandused. Kokku viidi uuringu käigus läbi seitse intervjuud ja parema ülevaate saamise huvides on uuringusse kaasatud osapooled on välja toodud allolevas tabelis 2.

Tabel 2. Uuringusse kaasatud osapooled

Uuringu osapool	**Valdkond**	**Uuringu etapp**	**Eesmärk**
ReM infoturbejuht	IT-esindaja	I etapp	Hetkeolukorra kaardistamine ministeeriumi vaatest
METK direktor	Äri esindaja	I etapp	Hetkeolukorra kaardistamine asutuse vaatest
METK strateegiajuht	Äri esindaja	II etapp	Ülevaade asutuse strateegilistest eesmärkidest, rollidest, kvaliteedieesmärkidest ja mõõdikutest, sisend missioonikriitiliste äriprotsesside tuvastamiseks
METK põllumajandusuuringute osakonna juhataja	Äri esindaja	III etapp	Üldise tasandi missioonikriitilise protsessi kaardistus ja modelleerimine
METK teadustegevuse valdkonna asedirektor	Äri esindaja	III etapp	Modelleeritud protsessi ja tegeliku protsessi vastavuskontroll ning protsessi täpsustamine
METK laborite ja katsekeskuste valdkonna asedirektor	Äri esindaja	III etapp	Modelleeritud protsessi ja tegeliku protsessi vastavuskontroll ning protsessi täpsustamine

Autor kõrvutas läbi viidud uuringut teooriaga ning sünteesi tulemusel tegi järeldused ja ettepanekud METKi näitel E-ITSi rakendamise võimalike takistuste ületamiseks ja

standardi rakendamiseks asutuses. Lisatulemina pakkus töö autor METKi näitel välja praktilise näite äriprotsesside tuvastamiseks. Samuti andis autor omapoolsed ettepanekud ka järgnevate uuringute tarbeks, mida käesoleva töö pinnalt oleks vajalik edasi uurida.

2.2. Eesti infoturbestandardi rakendamise uuringu tulemused

Käesolevas alapeatükis annab autor ülevaate dokumendianalüüsil ja poolstruktureeritud intervjuudel põhineva uuringu tulemustest. Autor tutvustab Maaelu Teadmuskeskuse infoturbealast hetkeolukorda, andes ülevaate rollijaotustest, koostööst ReMi ja asutuse vahel ning kitsaskohtadest, millega täna silmitsi seistakse. Samuti annab autor ülevaate E-ITSi rakendamiseks vajalikest tegevustest, mis käesoleva uuringu raames ära tehti ning mille tulemit on võimalik ReM IT-osakonnal kasutada äripoolse sisendina E-ITSi rakendamisel METKis.

Dokumendianalüüs andis esmase ülevaate asutuse infoturbealasest hetkeolukorrast. ReM IT-osakonna põhimäärusest (2020) selgus, et asutuse infoturbealase korralduse eest kannab hoolt ReM IT-osakond, kes töötab välja infotehnoloogilise turvapoliitika, sellele vastava infoturbe korra ja juhendi ning korraldab nende rakendamise ja täitmise. Asutusesiseseks kasutamiseks mõeldud Maaeluministeeriumi (ReM endine nimi) ja ministeeriumi infosüsteemiga liitunud ministeeriumi valitsemisala asutuste kehtiv infoturbe poliitika (2020) paneb paika ministeeriumi ja infoturbe haldusala infoturbe eesmärgid, üldalused ja vastutuse jagunemise. Dokumendist lähtub, et ReM ja ministeeriumi haldusala kasutab infoturbe juhtimiseks ISKE standardit ja infosüsteemidel on volitatud peakasutajad. Infosüsteemi peakasutaja on ühtlasi ka ISKE rakendusjuhendi tähenduses andmete omanik.

ReM tasandil töötatakse välja infoturbe juhtimise põhimõtted ja nõuded, mis on järgimiseks kohustuslikud ning koordineeritakse üldist infoturbe juhtimist. Asutusepõhine infoturbe juhtimine kuulub asutuste juhtide pädevusse. Sellel tasandil töötatakse välja asutuse infovarade füüsilist kaitset käsitlevad ja asutuse personaliga seotud infoturbe korrad ning korraldatakse nende rakendamine ja viimase üle arvestuse pidamine. Infoturbe koordineerimiseks on moodustatud ka töökeskkonna ning infoturbe korraldamise juhtkomisjon (TIK), kuhu kuuluvad ReM ja ministeeriumi haldusala

asutuste esindajad. Infoturbe poliitika dokument annab selge ülevaate rollidest ja neile määratud ülesannetest asutuse tasandil, konkreetne vastutus ja ülesanded on nii asutuse juhil, ISKE koordinaatoril kui ka infosüsteemide peakasutajatel. Kuivõrd tegu on asutusesiseseks kasutamiseks mõeldud dokumendiga, siis seda käesolevas töös detailsemalt ei käsitleta. Kokkuvõtvalt on dokumente võrreldud hetkeolukorraga tabelis 3.

Intervjuudest METKi direktoriga ja ReMi infoturbejuhiga selgus, et infoturbe poliitika ja infotehnoloogia osakonna põhimääruse dokumendid on paljuski aegunud ja hetkeolukord ei vasta dokumentides kirja pandule. Seoses infoturbejuhi vahetumisega 2023. aasta jaanuaris on paljud eelnevalt toiminud koostöövormid, näiteks TIK, jäänud soiku ning neid ülesandeid ei ole uuele infoturbejuhile üle antud. Samuti on infoturbealast olukorda ja töökorraldust oluliselt mõjutanud ReMi valitsemisala laienemine 2023. aastal, mil Maaeluministeerium ja Regionaalministeerium liideti, ja ReMi kolimine ühendministeeriumi hoonesse 2024. aasta alguses.

Olgugi, et käesoleva aasta alguses oleks pidanud nii ReM kui ka haldusala asutused olema üle läinud uuele infoturbestandardile E-ITS, on see ulatuslike muudatuste tõttu haldusalas jäänud tagaplaanile. Probleeme näevad ja tunnistavad nii ReM infoturbejuht kui ka METKi direktor. Peamiste probleemkohtadena jääb intervjuust infoturbejuhiga kõlama tõsine tööjõuressursi puudus ja infoturbe alatähtsustamine. Valitsemisala on suur, koosnedes kolmest valitsusasutusest, kahest hallatavast riigiasutusest ning kaheksast juriidilisest kehast. Infoturve on korraldatud keskselt kolmes valitsemisala asutuses, ühes osaliselt. Infoturbejuhi sõnul iseloomustab hetkeolukorda segadus, tegemata tööd on palju ja olukord on pigem murettekitav. Infoturbejuht tegeleb enda sõnul pidevalt “tulekahjude kustutamise” ja “pseudoprobleemidega”, mis võtab 70-80% tööajast.

Kuivõrd dokumendianalüüs ja läbi viidud intervjuud tõid esile ulatuslikud erinevused rollijaotuse, ülesannete ja kommunikatsiooni osas, on peamised vastuolud toodud selguse huvides välja alljärgnevas tabelis 3.

Tabel 3. Peamised vastuolud infoturbe juhtimisel METKis.

Kategooria	Dokumendianalüüsist lähtuv	ReMi vaade (intervjuu)	Asutuse vaade (intervjuu)
Rollijaotus ja ülesanded	Ministeeriumi tasand: infoturbe juhtimise põhimõtted, nõuded, IT-erinõuded. Asutuse tasand: asutuse juhi pädevus, asutuse infovarade füüsilist kaitset käsitlevad ja personaliga seotud infoturbe korrad, rakendamine, arvestuse pidamine. Infoturvet juhib TIK.	Vastutuse jagunemine asutuse ja ministeeriumi vahel hägune. Infoturve jäetakse IT-teemadest kõrvale, on ebapopulaarne ja kardetud. ISKE peakasutajad määratud osaliselt, ebapiisavalt. ReM vastutab.	Infoturvet juhib ministeerium. Direktor endal infoturbe juhtimise alaseid ülesandeid ei näe. ISKE koordinaatorit ja infosüsteemide peakasutajaid määratud ei ole.
Kommuni-katsioon ja koostöö	Moodustatud on TIK. Ministeeriumi IT-osakond juhib IT-nõukogu tööd. Regulaarne kommunikatsioon ministeeriumi ja asutuste vahel toimub läbi ISKE koordinaatori ja infosüsteemide peakasutajate.	Äri- ja IT-vaheline suhtlus ei toimi süsteemselt. Kvartaalsed IT-kohtumised toimuvad, kuid infoturbejuhti ei kaasata. Puudub otsene kontaktisik METKiga.	Puudub otsene infoturbealane kontakt ReMiga. Koostöö ReM IT-osakonnaga toimub läbi kvartaalsete kohtumiste ja IT nõukogu, kuid on probleemne.
E-ITS standard	Põhineb ISKE standardil. E-ITSil põhinevaid dokumente ei ole.	Standardile üleminek ei ole prioriteet. Üleminekut ei ole ReM infoturbejuhi poolt asutustele tutvustatud.	Konkreetsed suunised ministeeriumi poolt puuduvad.
Peamised kitsaskohad	Ei ole dokumenteeritud.	Üks infoturbejuht, suur valitsemisala ja töökoormus. Infosulg, pikad kooskõlastus-ringid, ebapiisav kaasatus.	IT-osakonna passiivsus ja suur info puudujääk, protsessid venivad.

Intervjuust METKi direktoriga lähtub, et infoturbealane tervikvaade ning ülevaade riskidest asutusel puudub. Selge ei ole ka rollijaotus ning vastutus infoturbe juhtimise eest langeb suuresti ainult ministeeriumi õlgadele. METKi direktor endal infoturbe juhtimise alaseid ülesandeid ei näe ja tunneb, et temal ei ole selles vallas sõnaõigust, sest ka infoturvet reguleerivad ja asutuse töötajatele järgmiseks mõeldud korrad on ette antud ministeeriumi poolt. Dokumentide järgi asutusele sätestatud rollid ning kaasnev vastutus, mis on välja toodud alljärgnevas tabelis 4, ei toimi. METKi direktori sõnul ei ole asutuses määratud ISKE koordinaatorit ega infosüsteemide peakasutajaid.

Tabel 4. Dokumendianalüüsist lähtuvad olulisimad rollid asutuse vaatest.

Roll	Ülesanded
Asutuse juht	korraldab ISKE meetmete rakendamist asutuses, sh määrab ISKE koordinaatori ja infosüsteemide peakasutajad, nende õigused ja kohustused ja kinnitab süsteemide turvaklassid.
ISKE koordinaator	koordineerib meetmete rakendamist ja nõustab, peab ISKE meetmete üle arvestust, osaleb auditi läbiviimisel.
Peakasutaja	määrab turvaklassi, osaleb infosüsteemi arendamise protsessis ja selle kasutuskorra välja töötamisel, haldab kasutajaõigusi, teavitab infoturbejuhti võimalike intsidentide kahtlusest.

Infoturvet seostab direktor peamiselt tööks vajalike programmide hankimisega, mida ministeerium peab kooskõlastama. „Muus osas infoturve meieni naljalt ei jõuagi," tõdeb direktor intervjuus. Peamiste kitsaskohtadena koostöös toob ta välja IT-osakonna passiivsuse, tugeva infosulu ning protsesside venimise. Puudulikku infovahetust ja infoturbe ebapiisavat kaasatust IT-alastes küsimustes toob esile ka infoturbejuht. Info liikumine on probleemne nii ministeeriumis kui ka ministeeriumi ja haldusala asutuste vahel. Koostöö allasutustega on kehv ja puudub konkreetne asutusepoolne kontaktisik. Intervjueeritavate sõnul toimuvad asutuse ja ministeeriumi IT-osakonna vahel kvartaalsed kohtumised, kuid infoturbejuhi sõnul teda sinna ei kaasata.

Infoturbejuhi hinnangul peetakse infoturvet endiselt IT-alaseks probleemiks ja äri- ning IT-vaheline suhtlus on väga kehv. Ka asutuse juhil on keeruline mõista infoturvet kui ärilise fookusega probleemi. Ta tõdeb, et asutus ei tee äri, mistõttu ei ole infoturbest äriliste riskide kontekstis mõelnud. Viimase viie aasta jooksul ei ole asutuses juhtunud ühtegi tõsisemat infoturbeintsidenti, mistõttu peab direktor tõsiste tagajärgedega intsidendi juhtumist üsna ebatõenäoliseks.

Uuele infoturbe juhtimise standardile üleminek ei ole seni olnud prioriteetne teema. Intervjuust ReM infoturbejuhiga selgub, et E-ITSile üleminekut asutustele tutvustatud ei ole, seda eelkõige infoturbejuhi ülekoormatuse tõttu. METKi direktori sõnul on üleminekut uuele standardile küll mainitud, kuid kuivõrd IT on konsolideeritud ReMi, on direktoril arusaam, et asutust uus infoturbe juhtimise standard otseselt ei puuduta. Ta tõdeb, et ei ole ministeeriumi poolt vähemasti saanud konkreetseid suuniseid, millist rolli asutus peaks selles protsessis täitma ja mida seoses uue standardi tulekuga tegema.

Intervjuust kõlama jäänud peamiste infoturbealaste ohukohtadena toob asutuse juht välja teadmatuse. Asutusel puudub teadmine, millist kahju on võimalik riigile teha

asutuse valduses olevate andmetega „Mis on meile võibolla kõige suurem oht, on see, et me ei saa aru, mis võib teistele olla huvitav.“ Näitlikustades oma mõtet mullastiku andmete ära kasutamisega sõjalises kontekstis. Kõige suurema ohukohana toob direktor välja asutuse töötaja, kes peab oskama küberohte märgata ja vastavalt käituda. Samas ei oska direktor välja tuua ühtegi näidet viimasest aastast, mida on asutuse töötajate infoturbealase teadlikkuse tõstmiseks ära tehtud.

METKi direktor tõdeb, et tal ei ole tegelikult head ülevaadet asutust ohustatavatest infoturbealastest riskidest. „See on jälle see koht, kus ma eeldan, et kuna see on konsolideeritud ministeeriumisse, siis ministeeriumi mure on selle eest hoolitseda,“ tõdeb ta intervjuus. Direktori hinnangul on asutusel vähe võimalusi, mida riskide maandamiseks ise ära teha, hoovad on rohkem ministeeriumi käes. Samas selgub intervjuust, et ReM ei ole METKi direktoriga infoturbealaseid riske ja nende maandamismeetmeid arutanud. Ülevaadet, milline on asutuse infoturbealane hetkeolukord ja organisatsiooni ohustavad riskid, ei ole METKi direktorini IT-osakonna kaudu jõudnud või ei ole ta sellest teadlik.

Kokkuvõtvalt võib öelda, et käesoleva uuringu esimesest etapist ehk infoturbealase hetkeolukorra ülevaatest selgusid olulised vastuolud dokumentides kirjeldatu ja reaalse töökorralduse vahel. Uuringu käigus analüüsitud põhilised infoturvet juhtivad dokumendid põhinevad ISKE standardil ja on seega aegunud. Intervjuud näitasid, et töökorraldus ei vasta tegelikult dokumentides sätestatule ja ebaselgus rollides ning tööülesannetes esines juba enne infoturbe standardi vahetumist. Suurimate probleemidena jäi kõlama tugev ressursipuudus, infoturbe alatähtsustamine, ebaselgus rollides ja ülesannetes ning tugevad kommunikatsiooniprobleemd. E-ITSile üleminek on valitsemisalas olnud samuti tagaplaanil eelkõige ressursipuuduse ja valitsemisala ulatuslike muudatuste tõttu.

Uuringu teises etapis teostas autor dokumendianalüüsi ja intervjuud asutuse strateegijajuhiga, eesmärgiga tuvastada asutuse missioonikriitilised äriprotsessid asutuse strateegiliste eesmärkide kaudu, mida infoturve teenima peab. Dokumendianalüüsi ja poolstruktureeritud intervjuude alusel konstrueeris autor METKi eesmärgimudeli. Dokumendianalüüsist lähtus, et METKi peamine eesmärk on teadmuspõhiste lahenduste pakkumine, mis aitaksid kujundada jätkusuutlikku põllumajandust ja maaelu Eestis.

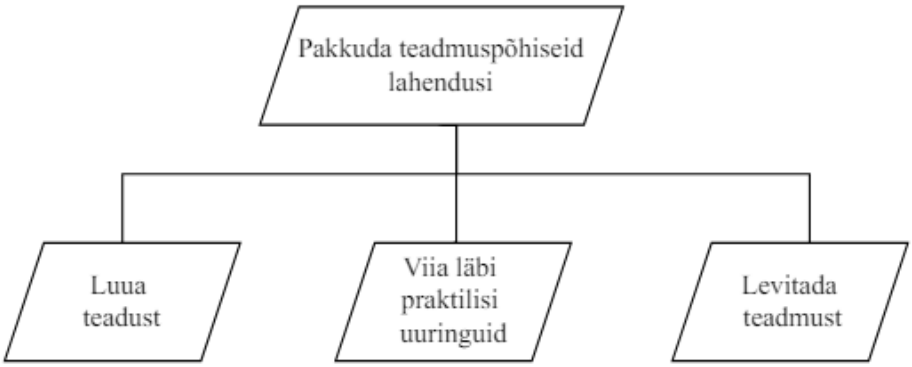
Dokumendianalüüsi pinnalt konstrueeris autor esialgse eesmärgimudeli koos olulisemate rollidega, kes organisatsiooni strateegilistesse eesmärkidesse panustavad.

Intervjuust strateegiajuhiga täpsustus asutuse eesmärgimudel. Peamise eesmärgi saab jagada kolmeks suuremaks alameesmärgiks, milleks on teaduse loome, erinevate valdkondlike uuringute, katsete ning analüüside läbi viimine ja teaduse ning praktilise kogemuse pinnalt loodud teadmuse jagamine eesmärgiga viia see laiemasse praktilisse kasutusse. Olulisimad kvaliteedinäitajad asutuse eesmärkide saavutamisel on usaldusväärsus, kliendikesksus, ajakohasus ning teadmuse praktiline teostatavus Eestis.

Teises intervjuus asutuse strateegiajuhiga täpsustati olulisimaid rolle, mis eesmärkide täitmise eest vastutavad ning peamiseid tulemusnäitajad, millega kvaliteeti mõõdetakse. Kuivõrd tegemist on 2023. aastal loodud organisatsiooniga ei ole iga kvaliteedieesmärgi kohta tulemusnäitajaid veel paika pandud ning töö selles suunas alles käib.

Kõige olulisemate rollidena panustavad eesmärkide saavutamisse lisaks juhtkonnale asutuse teadurid, agronoomid, katsetehnikud, valdkondlikud spetsialistid, laboritöötajad ja tugiteenuse pakkujad. Olulisemate tulemusnäitajatena võib välja tuua nii klientide kui ka partnerite ja töötajate rahulolu ja akrediteerituse säilitamise.

Uuringu käigus koostatud eesmärgimudel võimaldas saada ülevaate asutuse põhilistest eesmärkidest, mida infoturve teenima peab, tuues esile organisatsiooni prioriteetsed protsessid (Sulis & Taveter, 2022, lk 83), mille kaudu strateegilisi eesmärke saavutatakse. Uuringu käigus konstrueeritud asutuse eesmärgimudel kajastab hetkeseisu (*as-is*), mitte soovitud seisu (*to-be*), mis jääb käesoleva töö skoobist välja. Joonisel 5 on välja toodud mudeli lihtsustatud versioon, kus kajastuvad kolm peamist funktsionaalset eesmärki, mis aitavad täita teadmuspõhiste lahenduste pakkumise eesmärki ja on EITSi rakendamise aluseks. Organisatsiooni terviklik eesmärgimudel on parema loetavuse huvides leitav lisast 8.



Joonis 5. METKi funktsionaalsed eesmärgid, mis on E-ITSi rakendamise aluseks (mudeli lihtsustatud versioon)

Teaduse loome, praktiliste uuringute läbiviimise ja teadmuse levitamise saab jagada alameesmärkideks, mis on välja toodud lisas 8 asuval eesmärgimudelil. Teaduse loomel on kolm alameesmärki: korraldada sordiaretust, kaitsta taimi ja teostada põllumajanduse uuringuid. Kuna teadusloome protsess hõlmab METKis erinevaid valdkondi ja töös kasutatakse erinevaid andmebaase ning infosüsteeme, mis võivad mõjutada protsessi kaitsetarvet, kaardistas autor käesolevas töös näitena ära ka teaduse loome kolmanda funktsionaalsete eesmärkide taseme. Alameesmärgid on välja toodud lisas 8 asuval METKi eesmärgimudelil.

Sordiaretuse korraldusel on viis funktsionaalset alameesmärki, mis kõik panustavad ühe eesmärgi täitmisse – korraldada sordiaretust. Kuna sorte aretatakse eesmärgiga, et neid Eesti põldudel kasvatataks, on sordiaretuse korraldamise olulisim kvaliteedieesmärk vastavus klientide ootustele.

Taimede kaitsmise võib jagada kolmeks alameesmärgiks, milleks on taimekahjustajate uurimine, seire ja uuringute teostamine. Taimekaitse peab olema nõuetele vastav ja keskkonnasõbralik, säilitades samas saagitootlikkuse ning kliendiootustele vastavuse, mis on ära määratletud olulisemate kvaliteedieesmärkidena.

Põllumajandusuuringute teostamisel võib eristada nelja funktsionaalset eesmärki. Põllumajandusuuringud peavad olema teaduspõhised ja usaldusväärsed, aga ka kiired, et võimaldada põllumajandusettevõtetel uuringutulemusi arvesse võttes vastavalt tegutseda, mistõttu on need olulisemate kvaliteedieesmärkidena mudelis määratletud.

Uuringu III etapis teostas autor äriprotsessi analüüsi. Kuivõrd kaardistust tehti METKis esmakordselt ja E-ITSi rakendamine ei vaja protsessidega süvitsi minemist, vaid jääb soovituslikult üldisele tasandile, kaardistas autor esmalt METKi üldpildi ühe äriprotsessina ehk I tasandi protsessina (APQC, 2023). Eesmärgimudel, mis tõi esile asutuse funktsionaalsed eesmärgid, mida infoturve teenima peab, võimaldas lihtsasti määratleda asutuse kõige olulisema protsessi (Sulis & Taveter, 2022, lk 83), milleks on teadmuspõhiste lahenduste pakkumine. See protsess koosneb omakorda kolmest tuumikprotsessist: teaduse loomine, uuringute läbiviimine ja teadmuse levitamine, mis on METKi jaoks missioonikriitilise tähtsusega protsessid.

Eesmärgimudel loob soodsa pinnase protsesside kaardistamisega tulevikus detailsemaks minna, kui asutus seda soovib. Kuna tugiprotsesside eesmärk on toetada asutuse strateegiliste eesmärkide toimimist, ei ole need eesmärgiks iseenesest, mistõttu tugiprotsesse käesoleva töö raames ei kaardistatud. Tugiprotsessid on seotud iga protsessiga ja turvet vajavad nad siiski, mistõttu märgiti tugiprotsessid asutuse eesmärgimudelis vastava rollina. Tugiprotsessidele laieneb METKi olulisima äriprotsessi kaitsetarve.

Uuringu kolmandas etapis modelleeriti METKi olulisim protsess – teadmuspõhiste lahenduste pakkumine (vt lisa 9), mille jaoks saadi esmane sisend dokumendianalüüsist ja eesmärgimudelist. Saadud sisendi pinnalt ja tuginedes teoreetilisele käsitlusele viidi läbi poolstruktureeritud intervjuu põllumajandusuuringute osakonna juhatajaga. Intervjuust selgus, et teadmuspõhiste lahenduste pakkumise protsess algab METKi teaduse valdkonnas probleemi määratlemisega, mille järgselt valmistatakse ette uuringu plaan ja taotletakse selleks rahastust. Positiivse rahastusotsuse saamisel viiakse uuring läbi ning publitseeritakse teadustöö. Kuna uuringud on sageli pikad ja võivad kesta aastaid, tegeletakse paralleelselt uuringu läbiviimisele ka teadmuse levitamisega. Teadmust levitatakse sektorisse, et viia see praktilisse kasutusse ja anda teostatavast uuringust ajakohast ülevaadet. See on eestkätt võrgustiku osakonna roll. Protsess lõppeb, kui teadustöö on publitseeritud.

Teadmuspõhiste lahenduste pakkumise hetkeolukorra (*as-is*) protsess METKis on parema loetavuse huvides välja toodud lisas 9. Tegemist on METKi kõige olulisema protsessiga, mis on tervikliku ülevaate säilimise huvides kõrgel tasemel üldistatud.

Teadmuspõhiste lahenduste pakkumise protsessi igas etapis tuginetakse IT-keskkondadele. Intervjuust selgus, et olulist rolli mängivad nii erinevad METKi/ReMi keskkonnad kui ka litsentsiõigusega ja avalikud keskkonnad. Kuna infoturbe vaatenurgast lähtudes on oluline missioonikriitilise protsessiga seotud IT-alased keskkonnad ära kaardistada, pöörati neile protsessi kaardistades tähelepanu ning need on välja toodud tabelis 5.

Tabel 5. Levinumad METKis kasutusel olevad sisemised, väilised ja avalikud keskkonnad

Nimetus	
Avalik keskkond	Google pilvepõhised lahendused; videokonverentsiplatvormid nagu Teams, Zoom, Skype; Põllumajandusliku raamatupidamise andmebaas FADN; Eesti Teadusinfosüsteem – ETIS; keskkonnaotsuste infosüsteem – KOTKAS; statistikaprogramm
Litsentsiõigusega keskkond	Microsoft Sharepoint; Microsoft Office; statistikaprogramm; taimekasvatuse tarkvara – Agrobase
METKi/ReMi keskkond	Laborite infosüsteem LIS; mullastiku andmebaas Spectrum; väetiseregister; taimekaitsevahendite register; sordiregister; riigi toidu ja sööda käitlejate register; maaparandussüsteemide register; taimetervise register; mahepõllumajanduse register;

Avalike keskkondadena on määratletud keskkonnad, mille osas METKil puudub igasugune kontroll. Litsentsiõigusega keskkondade all mõistetakse litsentsi alusel kasutusel olevaid väliseid keskkondasid. METKi/ReMi keskkondadena mõistetakse ReM kontrolli all olevaid keskkondasid, kes ühtlasi vastutab ka METKi keskkondade turvalisuse eest.

Lisaks tabelis välja toodud keskkondadele on oluline ära mainida ka tugiteenuste andmebaasid nagu näiteks dokumendihaldussüsteem, millele tuleb E-ITSi rakendamisel tähelepanu pöörata, kuid kuivõrd need ei ole protsesside spetsiifilised, vaid mõjutavad kõiki protsesse ühtemoodi, ei ole neid käesoleva töö raames välja toodud.

Kuna uuringu läbiviimise etapp on käesolevas protsessis kõige olulisem ja mahukam samm ning kätkeb endas rohkelt tööd erinevate andmebaasidega, vaadati käesoleva magistritöö raames sinna detailsemalt sisse, kaardistades uuringu läbiviimise alamprotsessi, mis on parema loetavuse huvides välja toodud lisas 10.

Uuringu läbi viimine METKis algab uuringu ettevalmistamisest, mis hõlmab endas kõikvõimalike töökorralduslike kokkulepete, lepingute jms tegemist nii uurimisrühma sees kui ka rahastajaga.

Kui uuringu ettevalmistavad tegevused on tehtud, on järgmiseks oluliseks sammuks andmete kogumine, mis võib hõlmata endas nii olemasolevate andmete pärimist METKi/ReMi andmebaasidest või teistest keskkondadest kui ka andmete kogumist „põllult“. Kogutavad andmed võivad uuringuti erineda, näiteks andmed mullastiku, ilmastiku, sortide või taimekahjustajate kohta, samuti võivad andmete iseloomust sõltuvalt erineda ka andmete kogumise meetodid.

Andmete kogumise järel toimub andmete töötlemine, milleks kasutatakse taas litsentsipõhist või avalikku keskkonda, sageli vabavaralist statistikaprogrammi. Paralleelselt edastatakse andmed avatud teaduse põhimõtteid järgides avalikuks kasutamiseks teadusandmete repositooriumi, samuti kohustub METK avaldama asjakohased andmed Euroopa-üleseses põllumajandusliku raamatupidamise andmebaasis FADN.

Seejärel analüüsitakse uuringu käigus kogutud ja töödeldud andmed ja tehakse nende pinnalt järeldused. Uuringu läbiviimise alamprotsessi viimane etapp on tulemuste esitlemine rahastajale ja protsess lõppeb, kui teadustöö tulemused rahastajale on esitatud. Levinumad protsessis kasutatavad keskkonnad ja infosüsteemid toodi välja tabelis 5. Uuringu läbiviimise hetkeolukorra (*as-is*) protsess on välja toodud lisas 10.

Empiirilise uuringu käigus kaardistati detailsemalt ka andmete kogumise protsess (vt lisa 11). Kuna see hõlmab endas mitut otsustuskohta, visualiseeriti protsess parema ülevaate saamiseks eraldiseisval joonisel.

Andmete kogumise protsessis kannavad olulist rolli nii METKi laborid kui ka katsekeskused. Sõltuvalt sellest, kas uuringu jaoks on vajalikud laboratoorsed mõõtmised või katsete teostamine, vahel ka mõlemad, võib protsess liikuda edasi METKi laboritesse, kus vajalikud mõõtmised teostatakse ja andmed kantakse laborite infosüsteemi LIS, või katsekeskustesse, kus teostatakse uuringu jaoks vajalikud katsed. Katsetegevuse jooksul kogutakse andmed reeglina Microsoft Office programmi Excel ja

need talletatakse töötaja tööarvutis, välisel kõvakettal või välises keskkonnas (Microsoft Sharepoint). Laboratoorsed mõõtmised ja katsetegevuse käigus kogutud andmed annavad uuringusse uut sisendit, mistõttu liigub protsess tagasi andmete kogumise faasi. Kui katseid või laboratoorseid mõõtmiseid ei ole vaja enam teostada, siis andmete kogumise protsess lõppeb. METKi andmete kogumise hetkeolukorra *(as-is)* protsess on parema loetavuse huvides välja toodud lisas 11.

Intervjuust põllumajandusuuringute osakonna juhatajaga selgus, et teadurite tööd raskendavad infoturbealased piirangud teatud koostöökeskkondade või programmide kasutamiseks. Nii vähese materjali põhjal ei saa kindlalt väita, et mure puudutab kõiki organisatsiooni teadureid, kuid probleemile viitas ka METKi direktor, mistõttu võib eeldada, et nende ring, keda probleem puudutab, on laiem. Asutuses ei ole välja töötatud selget andmehalduspoliitikat ja puuduvad selged asutuseülesed kokkulepped, milliseid teadmuspõhiste lahenduste pakkumise protsessi käigus tekkivaid andmeid ja millistel alustel ning millises keskkonnas säilitatakse, töödeldakse ja analüüsitakse ning milliste rollide kandjad, millistele andmetele ligi pääsevad.

Samuti ei ole kindlaks määratud pilvepõhiseid koostöökeskkondasid, mis võimaldaksid edukat koostööd erinevate uuringu osapooltega. Seni on sõltuvalt seotud osapooltest ja uuringust kasutusel olnud väga erinevaid keskkondasid ja valik teatud keskkonna kasuks põhineb eelkõige mugavusel ja eelneval kasutuskogemusel, samuti uurimisrühma juhtpartneri valikul. Andmete vahetamiseks erinevate uuringu osapooltega ja uuringu käigus kogutud andmete talletamiseks kasutatakse kõige sagedamini Google ja Microsofti veebipõhiseid rakendusi.

Kokkuvõtvalt tuvastati uuringu käigus 12 tegurit, mis takistavad E-ITSi rakendamist METKis:

- asutuses infoturbe eest vastutava rolli puudumine;
- asutuse juht ei näe probleemi prioriteetsena;
- protsesside kaardistuse, sh vastutajate puudmine;
- infoturvet peetakse endiselt tehniliseks probleemiks;
- asutuse töötajate ebapiisav koolitamine;
- asutuses infoturbealase tervikülevaate puudumine;

- negatiivne meelestatus infoturbe valdkonna osas;
- infoturbealaste rollide ja vastutuse hägusus ja erinev tõlgendamine;
- ebapiisav kommunikatsioon mitmel tasandil;
- eelnevalt kehtinud infoturbe standardi mittetäielik rakendamine;
- ministeeriumi infoturbejuhi ebapiisav kaasatus IT-alastele koosolekutele;
- infoturbealase ressursi ebapiisavus ministeeriumis.

Kokkuvõtvalt võib käesoleva magistritöö empiirilise uuringu tulemuste pinnalt öelda, et infoturbealast hetkeolukorda iseloomustab tugev ressursipuudus, infoturbe alatähtsustamine, ebaselgus rollides ja ülesannetes ning tugevad kommunikatsiooniprobleemid, mis on E-ITSi rakendamist takistavateks teguriteks. Uuringu I etapist lähtus ka, et asutuse juht ei ole saanud konkreetseid suuniseid E-ITSile ülemineku kohta, mistõttu ei ole ta teadlik oma rollist selles protsessis ega oska vajadusi organisatsioonile kommunikeerida.

Uuringu II etapis määratleti eesmärgimudeli abil asutuse kõige olulisem protsess, milleks on teadmuspõhiste lahenduste pakkumine (vt lisa 8) ja uuringu III etapis analüüsiti ning modelleeriti protsess (vt lisa 9), pannes rõhku seotud IT-keskkondadele.

Uuringust lähtus, et E-ITS kaitsetarve tuleb määrata teadmuspõhiste lahenduste pakkumise protsessile, mille lahutamatuteks osadeks on uuringu läbiviimise protsess (vt lisa 10) ja andmete kogumise protsess (vt lisa 11). METKi missioonikriitilise protsessiga seotud varade hulka tuleb arvestada ka tabelis 5 välja toodud METKi/ReMi-sisesed keskkonnad, samuti peab arvesse võtma ka protsessis kasutatavaid litsentsiõigusega ja avalikke keskkondasid.

2.3. Järeldused ja ettepanekud

Tuginedes töö teoreetilisele käsitlusele ja läbi viidud empiirilisele uuringule, annab autor käesolevas peatükis ülevaate töö järeldustest ja esitab omapoolsed ettepanekud E-ITSi rakendamist takistavate asjaolude ületamiseks ning standardi rakendamiseks asutuses.

Tervikliku ülevaate saamiseks on autor toonud ettepanekud kokkuvõtvalt välja tabelis 6. Need on suunatud ministeeriumi infoturbe eest vastutavale isikule ja asutuse juhile, kuna nemad vastutavad infoturbe juhtimise ja E-ITSi rakendamise eest METKis. Ettepanekutest võib olla kasu ka teistele E-ITS rakendajatele, kel esineb takistusi standardile üleminekul ja kes ei ole seda mingil põhjusel veel teinud. Ettepanekud on tabelis järjestatud lähtuvalt nende esitamise järjekorrast järgnevas tekstis. Iga ettepanku juurde on märgitud leheküljenumber, viitamaks sellekohasele analüüsile tabelile järgnevas tekstis.

Tabel 6. Ettepanekud takistuste ületamiseks ja E-ITSi rakendamiseks

Ettepanek	**Sihtrühm**
Tagada süsteemne koostöö ja regulaarne kommunikatsioon IT- ja ärivaldkonna vahel (lk 49-50).	Ministeeriumi infoturbe vastutaja, asutuse juht
Määrata asutuse tasandil kindlaks infoturbealased rollid, vastutus ja ülesanded (lk 50-51).	Asutuse juht
Kaardistada organisatsiooni tegelikud infoturbealased vajadused ja vajalik rahaline ressurss infoturbealaste vajaduste katmiseks (lk 51).	Asutuse juht
Kaasajastada asutust puudutav infoturbealane dokumentatsioon, viies see vastavusse hetkel kehtiva E-ITS standardiga (lk 51-52).	Ministeeriumi infoturbe vastutaja
Korraldada asutuse töötajate regulaarne infoturbealane koolitamine (lk 52).	Asutuse juht
Kaardistada organisatsiooniüleselt vajadused tehniliste lahenduste järele ja leida sobivaimad, võttes arvesse nii turvalisuse kui ka kasutusmugavuse aspekti (lk 52-53).	Asutuse juht
Luua asutuseülene andmehalduspoliitika (lk 53).	Asutuse juht
Luua E-ITSile ülemineku kommunikatsiooniplaan ja konkreetsed suunised haldusala asutustele ning eest vedada kommunikatsiooniplaani rakendamist (lk 53).	Ministeeriumi infoturbe vastutaja
E-ITSile üleminekul kasutada soovitusliku mudelina kaitstavate äriprotsesside tuvastamiseks eesmärgimudelit eriti juhul, kui organisatsiooni protsesse pole varasemalt kaardistatud (lk 53-54).	E-ITSi rakendaja
Kaardistada ja modelleerida asutuse tuumik- ja tugiprotsessid võttes arvesse efektiivse protsessi edutegureid ning määrata protsessiomanike kohustused (lk 54-55).	Asutuse juht
Rakendada asutuses protsessipõhist juhtimist ja standardida asutuse tuumikprotsessid (lk 55).	Asutuse juht

Käesoleva magistritöö raames läbi viidud uuringust selgus, et ReM haldusalas jääb infoturve tagaplaanile, olgugi, et teoreetiline käsitlus rõhutab infoturbe olulisust. See avaldab mõju ka METKile. Avalik sektor on küberkurjategijatele atraktiivne sihtmärk (Coppolino *et al*., 2018, lk 573; Moon, *et al*., 2018, lk 54; Symantec, 2015; Trend

Micro, 2015 viidatud Wirtz & Weyerer, 2017, lk 1085 vahendusel) ja ulatuslike rünnakute tõttu võib ohtu sattuda ka riigi julgeolek ning langeda kodanike usaldus riigi vastu (Shandler & Gomez, 2023, lk 35). Infoturbe olulisust rõhutab ka E-ITS (Eesti infoturbestandard, 2024). Terviklik infoturbe juhtimine organisatsioonis aitab maandada infoturbealaseid riske ja tagada äriprotsesside ning avalike teenuste turvalisuse.

Uuringu I etapi tulemustest järeldus, et infoturbealane koostöö ministeeriumi ja asutuse vahel on nõrk. Kommunikatsiooniprobleeme esineb nii ministeeriumi tasandil, asutuse ja ministeeriumi vahel kui ka asutuse tasandil. Kayworth ja Whitten tõid esile, et infoturve jääbki madala prioriteediga ja eraldiseisvaks probleemiks, mis ei saa juhtkonna poolt piisavalt tähelepanu, kui ei mõisteta selle ärilist fookust ja infoturve tegutseb äri poolest sõltumatult (2010, lk 164). Intervjuude tulemused kinnitasid Kayworthi ja Whitteni järeldust. ReM infoturbejuhi hinnangul ei mõisteta infoturbe ärilist fookust ministeeriumi ega asutuste tasandil, mida kinnitas METKi direktori vaade – infoturbest äriliste riskide kontekstis ta mõelnud ei ole. Avalike teenuste küberturvalisuse tagamiseks on vaja toimivat koostööd ja regulaarset kommunikatsiooni IT- ja ärivaldkonna vahel, planeerides regulaarsed kohtumised konkreetsete päevakorra punktidega ning kaasates kohtumistele kõik seotud osapooled, sh ReM infoturbejuht. Sellest lähtuvalt on autoripoolne ettepanek tagada

Ettepanek 1: Tagada süsteemne koostöö ja regulaarne kommunikatsioon IT- ja ärivaldkonna vahel.

Uuringust lähtus, et asutuse juht ei näe endal vastutust infoturbe juhtimise osas. Samuti puudub tal teadmine teistest rollidest, mis infoturbealase dokumentatsiooni järgi peaksid olema organisatsioonis kehtestatud (vt tabel 4). Edu tagamiseks nähakse tippjuhtkonnal infoturbe juhtimises määravat rolli (Kayworthi ja Whitten, 2010, lk 171; Soomro *et al*., 2015, lk 223), asutuse juht aga tõdes, et tal puudub infoturbealastes küsimustes sõnaõigus.

Nii kirjandus (Soomro *et al*., 2015, lk 223; Kayworth ja Whitten, 2010, lk 171) kui ka E-ITS (Eesti infoturbestandard, 2024) rõhutavad asutuse juhi rolli ja suunavad vastutuse infoturbealastes küsimustes juhtkonnale, andes asutusele seega suurema otsustusvabaduse. ReM valitsemisalas on aga suund teine – kogu IT-d, sh infoturvet

juhib ministeerium mitme asutuse üleselt. Asutuses puudub infoturbe valdkonna eest vastutav roll, kes omaks asutuseülest tervikvaadet ja hoiaks regulaarset suhtlust ka ReM infoturbejuhiga. Kuivõrd rollid ja vastutuse jagunemine asutuse tasandil ei ole selge ja rollide jagunemises esineb vastuolusid teoreetilise käsitluse ning E-ITSiga, tuleb rollid kindlaks määrata.

Ettepanek 2: Määrata asutuse tasandil kindlaks infoturbealased rollid, vastutus ja ülesanded.

Uuringu I etapi tulemused on kooskõlas Kayworthi ja Whitteni väitega, et ärilise fookuse mittemõistmisel ei kujundata küberkaitset strateegiliselt, vaid ajaline ressurss raisatakse esilekerkivate kiireloomuliste ülesannete lahendamiseks ja otsused on ajendatud lühiajalistest prioriteetidest (2010, lk 164). See aga võib omakorda viia selleni, et organisatsiooni infoturbepoliitika ja -eelarve ei ole kooskõlas organisatsiooni tegelike vajadustega (Kayworth ja Whitten, 2010, lk 164). Uuringust selgus, et head ülevaadet asutusel infoturbealastest riskidest tegelikult ei ole, millest võib järeldada, et asutusel puudub ka ülevaade tegelikest infoturbealastest vajadustest. Kuivõrd ebapiisav infotuve peidab endas ulatuslikke ärilisi riske, on selle tagaplaanile jätmisel oht missioonikriitiliste protsesside katkemiseks ja võimalikuks rahaliseks ning mainekahjuks (Sommerville, 2015, lk 380), mistõttu tuleb organisatsiooni tegelikud infoturbealased vajadused üle vaadata, mõeldes juba strateegiliselt ka võimalikele vajadustele lähitulevikus.

Ettepanek 3: Kaardistada organisatsiooni tegelikud infoturbealased vajadused ja vajalik rahaline ressurss infoturbealaste vajaduste katmiseks.

Läbi viidud uuringust selgus, et infoturbe juhtimisega seotud töökorraldus ReM valitsemisalas ei vasta dokumentides sätestatule ja dokumentatsioon on aegunud. Olgugi, et hetkel kehtiv dokumentatsioon määrab (ISKE standardist lähtudes) kindlaks infoturbe juhtimisega seotud põhilised rollid ja nende ülesanded nagu seda rõhutavad Höne ja Eloff (2002, lk 404), ei vasta hetkeolukord dokumentides kirja pandule, mistõttu on oluline kaasajastada asutust puudutav infoturbealane dokumentatsioon.

Ettepanek 4: Kaasajastada asutust puudutav infoturbealane dokumentatsioon, viies see vastavusse hetkel kehtiva E-ITS standardiga.

METKi puudutavas infoturbealases dokumentatsioonis ei ole ära määratletud, kuidas käib töötajate infoturbealane koolitamine ja kes selle eest vastutab. METKi direktor ei osanud välja tuua viimase aasta näiteid, mida on töötajate infoturbealase teadlikkuse tõstmiseks ära tehtud, samas tõi ta samuti suurima ohuna välja just inimfaktori. Teoreetilisest käsitlusest lähtub, et infoturve puudutab igat asutuse töötajat ja inimene on ahela nõrgim lüli, kes infoturbepoliitikat järgima peab ning sageli selles eksib (Bella et al, 2015, lk 2; Laybats & Tredinnick, 2016, lk 79; Soomro *et al*., 2015, lk 223; Kont, 2022, viidatud Tammet, 2023, lk 27 kaudu). Ka Sommerville (2015, lk 412) toob välja erinevad põhjused, kuidas inimfaktor võib küberturvalisust negatiivselt mõjutada, mistõttu on inimeste järjepidevale koolitamisele ja infoturbealase teadlikkuse tõstmisele vaja pöörata suurt tähelepanu, vastasel juhul võib töötaja ebapädevus ja madal teadlikkus infoturbealastes küsimustes viia ebamõistlikke ja organisatsiooni küberturvalisust ohtu seadvate otsusteni.

Ettepanek 5: Korraldada asutuse töötajate regulaarne infoturbealane koolitamine.

Uuringust lähtus, et teadurite tööd raskendavad infoturbealased piirangud teatud koostöökeskkondade või programmide kasutamiseks. Olgugi, et nende kasutamine ei ole lubatud, kasutatakse neid siiski, et töö efektiivselt tehtud saada. Küberturvalisuse tagamise kõrval rõhutab ka Sommerville (2015, lk 414) efektiivsuse aspekti – oluline on arvestada, et mida tugevamad ja mitmekihilisemad on turvaprotseduurid, seda aeglasemaks muutuvad protsessid ja süsteemid. Kuna inimene on emotsionaalne olend ja kipub leidma mugavamaid alternatiive (Laybats & Tredinnick, 2016, lk 79) on oluline leida kompromiss turvalisuse ja kasutusmugavuse vahel, mis tagaks mõistliku turvalisuse taseme, kuid samas võimaldaks inimestel mugavalt töö tehtud saada. Sellest lähtuvalt on oluline kaardistada organisatsiooniüleselt ära töötajate vajadused tehnilistele lahendustele ja valida koostöös ministeeriumi IT-osakonnaga välja kõige sobilikumad lahendused, mis võtavad arvesse nii turvalisuse kui ka kasutusmugavuse aspekti.

Ettepanek 6: Kaardistada organisatsiooniüleselt vajadused tehniliste lahenduste järele ja leida sobivaimad, võttes arvesse nii turvalisuse kui ka kasutusmugavuse aspekti.

Läbi viidud uuringust selgus, et asutuses puuduvad ka organisatsiooniülesed kokkulepped andmehalduse küsimustes. Andmehaldusplaanid koostatakse küll üksikute uuringute läbiviimiseks koostöös uurimisrühmaga, kuid organisatsiooniülene tervikvaade, millele nende koostamisel tugineda, puudub. Teave on aga organisatsiooni kõige väärtuslikum vara (Gebremeskel *et al*., 2023, lk 44) ja avalik sektor, omades küberruumis tohutus kogustes isikuandmeid ning tundlikku teavet, on muutunud küberkurjategijatele atraktiivseks sihtmärgiks (Coppolino *et al*, 2018, lk 573), mistõttu peab autor oluliseks organisatsiooniülest andmehalduspoliitika loomist, et kaitsta organisatsiooni valduses olevaid andmeid ja korraldada nende kasutamist.

Ettepanek 7: Luua asutuseülene andmehalduspoliitika.

Uuringust selgus, et E-ITSile üleminek ei ole valitsemisalas olnud prioriteet, olgugi, et standardi rakendamine on kohustuslik 2024. aastast ja sellele üleminekuks oli aega kolm aastat. Standardimisel nähakse mitmeid kasutegureid (Purser 2014, lk 98; Syafrizal *et al*., 2020, lk 417) ja küberkuritegevus on kasvutrendis kogu maailmas (Morgan, 2023; ENISA, 2023, lk 4; Justiitsministeerium, 2022) ning selle tagajärjed muutuvad aina tõsisemaks (ENISA, 2023, lk 4), mistõttu on Eestile kohaldatud standardi rakendamine möödapääsmatult oluline. Kommunikatsioon E-ITSile ülemineku osas on aga olnud ebapiisav ja lünklik. Asutuse juht ei ole saanud ministeeriumilt konkreetseid suuniseid E-ITSile üleminekul, samuti puudub tal arusaam oma rollist selles protsessis. Sellest lähtuvalt on oluline ReM infoturbejuhil luua E-ITSile ülemineku kommunikatsiooniplaan haldusala asutustele, eest vedada selle rakendamist ning anda asutustele konkreetsed suunised E-ITSile üleminekul.

Ettepanek 8: Luua E-ITSile ülemineku kommunikatsiooniplaan ja konkreetsed suunised haldusala asutustele ning eest vedada kommunikatsiooniplaani rakendamist.

Uuringu II etapis rakendati eesmärgimudelit asutuse missioonikriitiliste äriprotsesside tuvastamiseks. Protsessid olid asutuses varasemast kaardistamata ja mudel aitas edukalt missioonikriitilised protsessid tuvastada. Mudel on kõrge abstraktsiooniastmega ja selle

väärtus seisnebki selle lihtsuses ja arusaadavuses kõigile osapooltele (Sterling & Taveter, 2009, 65; Lopez-Lorca, et al., 2018, lk 30; Sommerville, 2015, lk 139). Olgugi, et E-ITSi rakendamine ei nõua eesmärgimudeli kasutamist, leiab autor, et sellest on suurt kasu juhul, kui asutuses ei ole varem protsesse kaardistatud, sest see võimaldab visualiseerida asutuse strateegilised eesmärgid, tuues seega organisatsiooni prioriteetsed protsessid esile (Guizzardi & Reis, 2015, lk 1; Sulis & Taveter, 2022, lk 83). Mudel toetab E-ITSi üldistatud lähenemist ning toob esile ka olulisimad kvaliteedieesmärgid ja rollid, kes eesmärkide täitmisesse panustavad. Kuna infoturbe eesmärgid lähtuvad asutuse strateegilistest eesmärkidest (Eesti infoturbestandard, 2024), soovitab töö autor E-ITSile üleminekul kasutada esimese mudelina eesmärgimudelit.

Ettepanek 9: E-ITSile üleminekul kasutada soovitusliku mudelina kaitstavate äriprotsesside tuvastamiseks eesmärgimudelit eriti juhul, kui organisatsiooni protsesse ei ole varasemalt kaardistatud.

Asutusel puudub selge ülevaade organisatsiooni missioonikriitilistest protsessidest ja neid ohustatavatest infoturbealastest riskidest. METKis ei ole varem asutuseüleselt protsesse kaardistatud ega modelleeritud, samas hõlmab selge ülevaade ja missioonikriitiliste protsesside standardimine endas organisatsiooni jaoks mitmeid kasutegureid (Hammer, 2010, lk 11; Münstermann & Weitzel, 2008). Sellest lähtuvalt soovitab töö autor kaardistada ja modelleerida METKi missioonikriitilised äriprotsessid vähemalt eesmärgimudelis välja toodud tasemete lõikes, võttes arvesse Hammeri (2007, lk 3) efektiivse protsessi edutegureid.

Kasuks tuleb ka organisatsiooni olulisemate tugiprotsesside kaardistamine ja modelleerimine, sest need toetavad missioonikriitiliste protsesside täitmist (Hammer, 2010, lk 11; Muehlen & Ho, 2005; lk 455), ja tuumik- ja tugiprotsesside omanike kohustuste määratlemine (APQC, 2024, lk 3; Ernst & Young Baltics, 2012, lk 12).

Sõltuvalt sellest, millisel üldistustasemel protsesse kaardistada, võib selleks moodustada vastutava meeskonna ja määrata selle ülesanded (Ernst & Young Baltics, 2012, lk 12). Kaardistatud ja modelleeritud protsessid annavad asutusele ka ülevaate infoturbealastest riskidest, mis täna on puudulik.

Ettepanek 10: Kaardistada ja modelleerida asutuse tuumik- ja tugiprotsessid võttes arvesse efektiivse protsessi edutegureid ning määrata protsessiomanike kohustused.

Protsessipõhine juhtimine ei ole ühekordne tegevus, vaid pidev juhtimistsükkel, mille puhul on fookus protsessidel ja nende pideval täiustamisel (Dumas *et al*., 2018, lk 8). METK ei ole seni protsessipõhist juhtimist rakendanud, kuid teoreetiline käsitlus toob välja selle mitmeid kasutegureid (Hammer, 2010, lk 11). Protsessipõhist lähenemist toetab ka E-ITS, mis küll ei eelda protsessidega süvitsi minemist, kuid nõuab ülevaadet prioriteetsetest äriprotsessidest (Dumas *et al*, 2018, lk 35), mis on organisatsiooni strateegiliste eesmärkide saavutamise seisukohast kriitilise tähtsusega.

Kuna standard eeldab protsessipõhist riskihaldust ja riskid tuleb üle vaadata protsessis muudatusi tehes (Hariyanti *et al.,* 2021, lk 1), on soovituslik protsessid standardida (Münstermann & Weitzel, 2008), et tagada järjepidevad tulemused ning ühtlane kvaliteet (vt joonis 2, lk 18).

Protsessipõhise juhtimise rakendamiseks asutuses soovitab autor kasutada üldtunnustatud protsessipõhise juhtimise elutsüklit, põimides seda riskijuhtimise elutsükliga (vt joonis 4, lk 26). Selline lähenemine võimaldab märgata riske võimalikult varakult ning valida sobiv strateegia nendega toimetulekuks.

Protsessipõhise juhtimismudeli rakendamine organisatsioonis võimaldab infoturvet edukamalt korraldada, tagades organisatsiooni jätkusuutlikkuse ja kohanemisvõime pidevalt muutuva küberruumiga ning parema küberturvalisuse taseme.

Ettepanek 11: Rakendada asutuses protsessipõhist juhtimist ja standardida asutuse tuumikprotsessid.

Käesoleva magistritöö ja läbi viidud kolmeetapilise uuringu pinnalt tegi autor üksteist ettepanekut E-ITSi rakendamist takistavate asjaolude ületamiseks ning E-ITSi rakendamiseks asutuses. Välja toodud ettepanekute seas on neid, mille rakendamine ei nõua suurt lisaressurssi, aga on ka suuremaid muutuseid nõudvaid ettepanekuid. Kõige prioriteetsema ettepanekuna näeb autor infoturbealaste rollide, vastutuse ja ülesannete määramist asutuse tasandil, mis võimaldaks üsna lihtsa vaevaga oluliselt parendada infoturbealast hetkeolukorda ja kommunikatsiooni asutuse ning ministeeriumi vahel,

sest rollid ja vastutus on võimalik ära jagada ka olemasolevate töötajate vahel. Kuna asutuses ei ole varem protsesse kaardistatud, usub autor, et kõige suuremat kasu võiks asutus saada protsesside kaardistamisest ning protsessipõhise juhtimissüsteemi rakendamisest.

Autor usub, et võttes arvesse välja toodud ettepanekuid ja neid rakendades, on võimalik METKi infoturbealast olukorda parendada ja E-ITSi rakendamise takistused ületada, tagades parema kaitse küberkuritegevuse vastu. Oluline on siinkohal rõhutada, et koostöös ReM infoturbe eest vastutava isikuga on vaja edasi tegeleda ka E-ITSi rakendamisega organisatsioonis, kuna standardi rakendamine E-ITSi kohuslastele on kohustuslik alates 2024. aastast.

KOKKUVÕTE

Käesoleva magistritöö fookuses oli tuvastada asjaolud, mis on takistanud Eesti infoturbestandardi rakendamist ja leida viisid nende ületamiseks. Selleks kaardistati Maaelu Teadmuskeskuse näitel asutuse infoturbealane hetkeolukord ja tehti standardikohased ettevalmistused E-ITSi rakendamiseks asutuses.

Magistritöö teoreetiline raamistik käsitles terviklikku infoturbe juhtimist avalikus sektoris, seades fookuse protsessidele. Teooriast lähtus, et avalik sektor on küberruumi kõige ohustatum sihtmärk ja kuna rünnakud võivad ohtu seada riigi julgeoleku ja kodanike turvalisuse, on küberturvalisuse tagamisele vaja avalikus sektoris pöörata suurt tähelepanu.

Infoturvet nähakse järjest enam ärilise probleemina ja kuna infoturve peab olema ajendatud organisatsiooni strateegilistest eesmärkidest, rõhutab teoreetiline käsitlus asutuse juhi rolli infoturbe juhtimisel. Oluline on IT- ja ärivaldkonna koostöö küberturvalisuse tagamisel, vastasel juhul ei kujundata küberkaitset strateegiliselt ja organisatsiooni infoturbepoliitika ja -eelarve ei pruugi olla kooskõlas organisatsiooni tegelike vajadustega.

Küberkuritegevus võib ohtu seada organisatsiooni eksistentsi, mistõttu on oluline kaitsta organisatsiooni missioonikriitilisi protsesse. Protsessipõhine vaade infoturbele võimaldab näha organisatsiooni sotsiotehnilise süsteemina, pöörates tähelepanu inimese rollile organisatsiooni olulistes protsessides. Kuna inimene on ahela nõrgim lüli ja küberkurjategijad mängivad inimlike nõrkustega, tuleb infoturvet vaadelda laiemalt kui infosüsteemide turvalisusena. Protsessipõhine lähenemine infoturbele võimaldab märgata riske varakult ja tagada seega avalike teenuste turvalisus ning organisatsiooni jätkusuutlikkus.

Käesoleva töö empiirilises osas tutvustati infoturbe olukorda Eestis ja anti ülevaade uuritavast organisatsioonist – Maaelu Teadmuskeskusest – ning uuringu metoodikast. Empiirilises osas läbi viidud uuring põhines kolmel etapil, mille käigus uuriti E-ITSi rakendamise takistusi, tuvastati asutuse missioonikriitilised protsessid ja kaardistati ning modelleeriti asutuse kõige olulisem protsess – teadmuspõhiste lahenduste pakkumine, millele tuleb E-ITS kaitsetarve määrata ja protsessi turvalisus tagada. Kuna äriprotsesside tuvastamine on olnud E-ITSi kohuslastele raskuskohaks, pakkus töö autor lisatulemina välja praktilise näite nende tuvastamiseks. Protsess modelleeriti Ameerika produktiivsuse ja kvaliteedi keskuse (APQC) välja töötatud ja üldtunnustatud protsesside kvalifikatsiooni raamistiku esimesel üldistustasemel.

Uuringu käigus seoti protsessiga olulisimad andmebaasid, infosüsteemid ja keskkonnad, mida protsessis kasutatakse ning analüüsiti nii uuringu läbiviimise protsessi kui ka andmete kogumise protsessi, mis on teadmuspõhiste lahenduste pakkumise protsessi lahutamatuteks osadeks.

Uuringu meetoditena kasutati dokumendianalüüsi ja poolstruktureeritud intervjuusid, eesmärgimudelile ja modelleeritud äriprotsessile teostati ka vastavuskontroll. Protsessi parendamisega ehk *to-be* vaatega käesoleva magistritöö raames ei tegeletud, kuna see ei ole E-ITSi rakendamise seisukohast vajalik.

Töö autori hinnangul said magistritöö uurimisküsimused ja töö eesmärk täidetud. Olulisemate uuringu tulemustena selgusid järgmised E-ITSi rakendamise takistused METKis:

- asutuses infoturbe eest vastutava rolli puudumine;
- asutuse juht ei näe probleemi prioriteetsena;
- protsesside kaardistuse, sh vastutajate puudmine;
- infoturvet peetakse endiselt tehniliseks probleemiks;
- asutuse töötajate ebapiisav koolitamine;
- asutuses infoturbealase tervikülevaate puudumine;
- negatiivne meelestatus infoturbe valdkonna osas;
- infoturbealaste rollide ja vastutuse hägusus ning erinev tõlgendamine;
- ebapiisav kommunikatsioon mitmel tasandil;

- eelnevalt kehtinud infoturbe standardi mittetäielik rakendamine;
- ministeeriumi infoturbejuhi ebapiisav kaasatus IT-alastele koosolekutele;
- infoturbealase ressursi ebapiisavus ministeeriumis.

Uuringust lähtus, et infoturbealane hetkeolukord METKis ei võimalda standardi rakendamist, sest üleminekut toetav süsteem selleks puudub. Asutuse juht ei ole teadlik oma rollist selles protsessis ega ole saanud ReMilt ka konkreetseid suuniseid E-ITSile ülemineku kohta. Hetkeolukorda iseloomustab tugev ressursipuudus, infoturbe alatähtsustamine, ebaselgus rollides ja ülesannetes ning tugevad kommunikatsiooni-probleemid, mistõttu on E-ITSi rakendamine asutuses viibinud. Esmalt tuleb tegeleda hetkeolukorra korrastamisega.

Magistritöö raames käsitletud teoreetilise kirjanduse ja läbi viidud empiirilise uuringu põhjal tegi töö autor üksteist ettepanekut E-ITSi rakendamist takistavate asjaolude ületamiseks ning standardi rakendamiseks. Ettepanekud on koostatud Maaelu Teadmuskeskuse näitel ja suunatud METKi infoturbe juhtimise ja E-ITSi rakendamise eest vastutavatele isikutele, kuid võivad pakkuda huvi ja on kohaldatavad ka teistele E-ITS kohuslastele, kuivõrd mitmed tuvastatud probleemid ja nende lahendused on oma olemuselt universaalsed.

Käesoleva töö pinnalt tehti järgmised ettepanekud:

- Tagada süsteemne infoturbealane koostöö ja regulaarne kommunikatsioon IT- ja ärivaldkonna vahel.
- Määrata asutuse tasandil kindlaks infoturbealased rollid, vastutus ja ülesanded.
- Kaardistada organisatsiooni tegelikud infoturbealased vajadused ja vajalik rahaline ressurss infoturbealaste vajaduste katmiseks.
- Kaasajastada asutust puudutav infoturbealane dokumentatsioon, viies see vastavusse hetkel kehtiva E-ITS standardiga.
- Korraldada asutuse töötajate regulaarne infoturbealane koolitamine.
- Kaardistada organisatsiooniüleselt vajadused tehniliste lahenduste järele ja leida sobivaimad, võttes arvesse nii turvalisuse kui ka kasutusmugavuse aspekti.
- Luua asutuseülene andmehalduspoliitika.

- Luua E-ITSile ülemineku kommunikatsiooniplaan ja konkreetsed suunised haldusala asutustele ning eest vedada kommunikatsiooniplaani rakendamist.
- E-ITSile üleminekul kasutada soovitusliku mudelina kaitstavate äriprotsesside tuvastamiseks eesmärgimudelit eriti juhul, kui organisatsiooni protsesse pole varasemalt kaardistatud.
- Kaardistada ja modelleerida asutuse tuumik- ja tugiprotsessid võttes arvesse efektiivse protsessi edutegureid ning määrata protsessiomanike kohustused.
- Rakendada asutuses protsessipõhist juhtimist ja standardida asutuse tuumikprotsessid.

Magistritööd ja selle tulemeid saab kasutada E-ITSi rakendamisel asutuses ja need antakse üle ReM IT-osakonnale ärivaldkonnapoolse sisendina. Käesoleva töö pinnalt saab määrata koostöös ReM infoturbe eest vastutava isikuga kaardistatud protsessile kaitsetarve ja vajalikud kaitsemeetmed, vaadata üle seotud varad ja teostada vajadusel väline riskihindamine. E-ITSi edasised rakendusetapid jäid käesoleva töö skoobist välja.

Käesoleva töö raames uuriti E-ITSi rakendamist takistavaid asjaolusid infoturbe vaatenurgast lähtuvalt, mida võib lugeda töö piiranguks ja ka võimalikuks jätku-uuringu teemaks, sest takistusi võib esineda ka väljaspool infoturbe valdkonda. Käesoleva töö raames tegeleti E-ITSi rakendamise takistuste uurimise ja infoturbealase hetkeolukorra kaardistamisega METKi näitel, kuid jätku-uuringuna võiks seda uurida valitsemisalaüleselt, samuti teistes valitsemisalades, mõistmaks riigiülest olukorda. Kuna inimene mängib küberturvalisuse tagamisel olulist rolli ja tema harimine on tähtis, näeb autor ühe jätku-uuringu teemana ka infoturbealase teadlikkuse alast uuringut avalikus sektoris laiemalt.

VIIDATUD ALLIKAD

Aagesen, G. & Krogstie, J. (2010). What is business process management? In J. Vom Brocke, & M. Rosemann (Eds.), *Handbook on Business Process Management: Introduction, Methods and Information Systems, vol. 1* (pp. 213-235), Springer.

Alexei, A. (2021). Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. *Journal of Social Sciences, 4*(1), 84-94.

American Productivity & Quality Center (APQC). (2024). *How Process Frameworks Enable Automation: National Bank of Moldova Case Study.* https://www.apqc.org/resource-library/resource-listing/how-process-frameworks-enable-automation-national-bank-moldova

American Productivity & Quality Center (APQC). (2023). Process Classification Framework - City Government. https://www.apqc.org/resource-library/resource-listing/apqc-process-classification-framework-pcf-city-government-pdf

Bella, G., Curzon, P. & Lenzini, G. (2015). Service Security and Privacy as a Socio-Technical Problem. *Journal of Computer Security 23*(5), 563-585. https://doi.org/10.3233/JCS-150536

Blank, R. & Gallagher, P. (2012). *Guide for Conducting Risk Assessments* (NIST SP 800-30). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Coppolino, L., Salvatore, A., D., Mazzeo, G., Romano, L. & Sgaglione, L. (2018). *How to Protect Public Administration from Cybersecurity Threats: the COMPACT Project*. https://doi.org/10.1109/WAINA.2018.00147

Cyberenetica (2023). Andmekaitse ja infoturbe portaal. https://akit.cyber.ee/

Dumas, M., La Rosa, M., Mendling, J & Reijers, H., A. (2018). *Fundamentals of Business Process Management*. Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-56509-4

Eesti infoturbestandard. (2024). *Riigi Infosüsteemi Amet*. https://eits.ria.ee/

Ernst & Young Baltic AS. (2012). *Avaliku sektori äriprotsessid. Protsessianalüüsi käsiraamat.* Majandus- ja Kommunikatsiooniministeerium. http://dspace.ut.ee/handle/10062/45124

Euroopa Komisjon. (2022). *Digital Economy and Society Index (DESI) 2022. Digital Public Services.* https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022

Euroopa võrgu-ja infoturbe agentuur (ENISA). (2023). *ENISA Threat Landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Euroopa võrgu-ja infoturbe agentuur (ENISA). (2022). *Threat Landscape.* https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

Fenz, S., Heurix, J., Neubauer, T. & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security, 22(5), 410-430.* https://doi.org/10.1108/IMCS-07-2013-0053

Gebremeskel, B., K., Jonathan, G., M. & Yalew, S., D. (2023). Information Security Challenges During Digital Transformation. *Procedia Computer Science 219,* 44–51. https://doi.org/10.1016/j.procs.2023.01.262

Geller, S. (2021). *Protsesside juhtimise rakendamine professionaalseid teenuseid pakkuvas ettevõttes*. [Magistritöö. Tallinna Tehnikaülikool]. https://digikogu.taltech.ee/et/Item/f0790133-729b-4e02-aa0b-b5dc5b073a00

Goel, K., Bandara, W., & Gable, G. (2023). Conceptualizing business process standardization: a review and synthesis. *Schmalenbach Journal of Business Research, 75*(2), 195-237. https://doi.org/10.1007/s41471-023-00158-y

Guizzardi, R. S., Guizzardi, G., Almeida, J. P. A., & Cardoso, E. C. (2010). Bridging the Gap between Goals, Agents and Business Processes. *In iStar,* 46-51.

Guizzardi, R. & Reis, A., N. (2015). A Method to Align Goals and Business Processes. In P. Johannesson, M., L., Lee, S., W., Liddle, A., L., Opdahl & Ó., P., López (Eds.), *Lecture Notes in Computer Science: Vol. 9381. International Conference on Conceptual Modeling* (pp. 79-93). Springer. https://doi.org/10.1007/978-3-319-25264-3_6

Hammer, M. (2007). The process audit. *Harvard business review*, *85*(4), 1-17.

Hammer, M. (2010). What is business process management, in J., Brocke, & M. Rosemann (Eds.), *Handbook on Business Process Management: Introduction, Methods and Information Systems, vol. 1* (pp. 3-16). Springer.

Hariyanti, E., Djunaidy, A., & Siahaan, D. (2021). Information security vulnerability prediction based on business process model using machine learning approach. *Computers & Security, 110,* 1-16. https://doi.org/10.1016/j.cose.2021.102422

Hoo, K. J. S. (2000). *How much is enough? A risk management approach to computer security.* Stanford University.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. *Computers & security, 21*(5), 402-409. https://doi.org/10.1016/S0167-4048(02)00504-7

International Organization for Standardization. (2022). *ISO/IEC 27001:2022.* https://www.iso.org/standard/27001

Justiitsministeerium. (2022). *Kuritegevus Eestis 2022*. https://www.kriminaalpoliitika.ee/kuritegevus2022/arvutikuriteod/

Kalbus, S. (2023). *Protsessipõhise juhtimise parendamine teenusedisaini toel Maaeluministeeriumi tervikteenuste näitel.* [Magistritöö. Tartu Ülikool, Pärnu Kolledž]. https://hdl.handle.net/10062/92199

Kanada standardinõukogu. (n.d.). *Types of standards.* https://www.scc.ca/en/types-standards

Kaul, K. (2008). *IT riskide hindamise metoodika väikeettevõtetele.* [Magistritöö. Tallinna Ülikool] www.cs.tlu.ee/instituut/opilaste_tood/magistri_tood/kevad_2008/Kristo_Kaul/Kristo_Kaul_Magistri_Too.pdf

Kayworth, T. & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive, 9(3),* 162-176.

Kõiv, K. (2023, mai 18). *Esmakordselt kogunes METK teadusnõukogu*. Maaelu Teadmuskeskus. https://metk.agri.ee/uudised/esmakordselt-kogunes-metk-teadusnoukogu

Laybats, C. & Tredinnick, L. (2016). Information security, *Business Information Review, 33*(2), 76-80. https://doi.org/10.1177/0266382116653061

Lopez-Lorca, A., Burrows, R., & Sterling, L. (2018). Teaching Motivational Models in Agile Requirements Engineering. In *Proceedings of an International Workshop on Requirements Engineering Education and Training held in Banff, AB, Canada 21 August 2018* (pp. 30-39). https://doi.org/10.13140/RG.2.2.33988.68489

Maaelu Teadmuskeskus (2023, aprill). *Akrediteeritus.* https://metk.agri.ee/laboriteenused-poldkatsed/olulised-dokumendid/akrediteeritus

Maaelu Teadmuskeskuse põhimäärus. (2022). *Riigi Teataja I,* 27.09.2022, 1*; Riigi Teataja I,* 04.07.2023, 24. https://www.riigiteataja.ee/akt/127092022001?leiaKehtiv

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security, 27*(2), 233-272. https://doi.org/10.1108/ICS-03-2018-0031

Moon, Y., J., Choi, M. & Armstrong, D., J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management 40,* 54–66. https://doi.org/10.1016/j.ijinfomgt.2018.01.001

Morgan, S. (2023). *Boardroom Cybersecurity Report 2023*. *Cybersecurity Ventures*. https://www.secureworks.com/centers/boardroom-cybersecurity-report-2023

Muehlen, M. Z., & Ho, D. T. Y. (2005). Risk management in the BPM lifecycle. In C. Bussler & A. Haller (Eds.), *Lecture Notes in Computer Science: Vol. 3812. Business Process Management Workshops* (pp. 454-466). Springer. https://doi.org/10.1007/11678564_42

Münstermann, B. & Weitzel, T. (2008). What Is Process Standardization? *Proceedings of an international conference on Information Resources Management held in Niagara Falls, Ontario, Canada, 18-20 May 2008.* Association for Information Systems. http://aisel.aisnet.org/confirm2008/64

Nweke, L. O. (2017). Using the CIA and AAA models to explain cybersecurity activities. *PM World Journal, 6*(12), *1-3.*

Pajumägi, K. (2022, 17. august). *Valitsuse 18.8 istungi kommenteeritud päevakord.* Vabariigi valitsus. https://valitsus.ee/uudised/valitsuse-188-istungi-kommenteeritud-paevakord

Pender-Bey, G. (2016). The parkerian hexad. *Information Security Program at Lewis University*.

Pihlak, A. (2024, 4. aprill). Suur andmekahju kerge vaevaga: ligi 700 000 Apotheka ja PetCity kliendi andmed varastati. *Delfi Meedia.* https://www.delfi.ee/artikkel/120282843/suur-andmekahju-kerge-vaevaga-ligi-700-000-apotheka-ja-petcity-kliendi-andmed-varastati

Porter, M. E. (1985). *The Competitive Advantage: Creating and Sustaining Superior Performance*. The Free Press.

Purser, S. (2014). Standards for Cyber Security. In M. E. Hathaway (Eds.), *Best Practices in Computer Network Defense: Incident Detection and Response* (pp. 97-106). IOS Press.

Rahvusvaheline Standardimisorganisatsioon. (2022). *ISO/IEC 27001*. https://www.iso.org/standard/27001

Regionaal-ja Põllumajandusministeeriumi sisedokumentatsioon. (2020).

Riigi Infosüsteemi Amet. (2023). *Küberturvalisuse aastaraamat 2023*. https://ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid#kuberturbe-aastaraamatud

Riigi Infosüsteemi Amet. (2022, 9. detsember). *Valitsus kehtestas Eesti infoturbestandardi, mis aitab juhtida riske ja kaitsta infosüsteeme.* https://www.ria.ee/uudised/valitsus-kehtestas-eesti-infoturbestandardi-mis-aitab-juhtida-riske-ja-kaitsta-infosusteeme

Riigi Infosüsteemi Amet. (2020). *EITS koolitus.* https://www.youtube.com/watch?v=0e-rDN-ntj4&ab_channel=RiigiInfos%C3%BCsteemiAmetNCSC-EE

Riigi Infosüsteemi Amet. (s. a.-a). *Avalikule sektorile.* https://www.itvaatlik.ee/avalikule-sektorile/

Riigi Infosüsteemi Amet. (s. a.-b). *Infosüsteemide turvameetmete süsteem ISKE*. https://www.ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/infosusteemide-turvameetmete-susteem-iske

Samimi, A. (2020). Risk management in information technology. *Progress in Chemical and Biochemical Research, 3*(2), 130-134.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3), 21-45.

Seeba, M. (2019). *A Specification of Layer-Based Information Security Management System for the Issue Tracking System*. [Magistritöö. Tartu Ülikool]. http://hdl.handle.net/10062/66393

Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology & Politics, 20*(4), 359-374. https://doi.org/10.1080/19331681.2022.2112796

Sommerville, I. (2015). *Software engineering, 10th edition.* Pearson.

Soomro, Z., A., Shah, M., H. & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management 36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Sotsiaalministeeriumi sisedokumentatsioon. (2023).

Spalević, Ž. (2014). Cyber security as a global challenge today. *Singidunum Journal of Applied Sciences, 687-692*. https://doi.org/10.15308/SInteZa-2014-687-692

Sulis, E., & Taveter, K. (2022). *Agent-Based Business Process Simulation*. *A Primer with Applications and Examples.* Springer. https://doi.org/10.1007/978-3-030-98816-6

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417-432. https://doi.org/10.17762/ijcnis.v12i3.4817

Tammet, K. (2023). *Eesti infoturbestandardi (E-ITS) haldusprotsess lähtudes parimast praktikast*. [Magistritöö. Tallinna Tehnikaülikool]. https://digikogu.taltech.ee/et/Item/0510a7b2-14ea-4f9f-abd3-0ee813419c74

Traynor, Ian. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Vaks, T. (2018). *Küberjulgeoleku strateegia mõju küberturvalisuse arengule Eestis 2008-2018.* [Magistritöö. Tallinna Tehnikaülikool]. https://digikogu.taltech.ee/et/item/e14f0293-e40f-4fac-ab92-62af3febd040

Veldre, A. (2021). *Eesti infoturbestandardi protsessimudeli evalveerimine*. [Diplomitöö. Tallinna Tehnikaülikool]. https://digikogu.taltech.ee/et/item/1e4a4d90-e66e-4ef8-ae01-11b311cd7e02

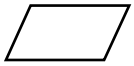
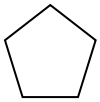
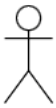
Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A review of sociotechnical systems theory: a classic concept for new command and control paradigms. *Theoretical issues in ergonomics science, 9*(6), 479-499. https://doi.org/10.1080/14639220701635470

Whitworth, B. (2009). A brief introduction to sociotechnical systems. In M. Khosrow-Pour (Eds.), *Encyclopedia of Information Science and Technology, Second Edition,* (pp. 394-400). IGI Global. https://doi.org/10.4018/978-1-60566-026-4

Wirtz, B. W., & Weyerer, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration, 40*(13), 1085-1100. https://doi.org/10.1080/01900692.2016.1242614

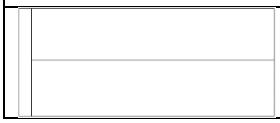
Õunapuu, L. (2014). *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes.* http://dspace.ut.ee/bitstream/handle/10062/36419/ounapuu_kvalitatiivne.pdf

Lisa 1. Eesmärgimudeli notatsioon

Sümbol	**Tähendus**
	Funktsionaalne eesmärk
	Kvaliteedieesmärk
	Tulemusmõõdik
----------	Suhe funktsionaalse eesmärgi ja kvaliteedieesmärgi vahel
_____	Eesmärkide vaheline suhe
	Roll

Allikad: Lopez-Lorca, et al., 2018, lk 36; Sterling & Taveter, 2009, lk 67

Lisa 2. BPMN notatsiooni põhilised elemendid

Sümbol	**Tähendus**
	Erinevat liiki sündmused – erineva ringikujulise sümbolina tähistatakse protsessi algust (vasakul) ja lõppu (keskel). Sõnumi märk tähistab sõnumiga lõppevat voogu (paremal).
	Erinevat liiki tegevused – üksikud protsessi jooksul tehtavad toimingud.
	Lüüs – otsustuskoht, kus toimub protsessis hargnevus. Sümbolina on tähistatud välistav (vasakul) ja paralleelne (paremal) lüüs.
	Andmebaas
	Järgnevusvoog
	Sõnumivoog
	Seos
	Rada (tähistab protsessis osalevat rolli)
	Bassein (tähistab protsessi)

Allikad: Aagesen & Krogstie, 2010, lk 217; Ernst & Young Baltics, 2012, lk 15-18; Sulis & Taveter, 2022, lk 17

Lisa 3. Poolstruktureeritud intervjuukava Regionaal- ja Põllumajandusministeeriumi infoturbejuhile

1. Palun kirjelda lühidalt hetkeolukorda, kuidas on täna valitsemisalas infoturve juhitud?
2. Palun kirjelda ka ministeeriumi ja haldusala asutuste omavahelist koostööd ja rollide jaotust ning vastutuse jagunemist METKI näitel, mis on infoturbe juhtimise korraldamiseks loodud:

    - Infoturbe koordineerimiseks ministeeriumis ja infoturbe haldusalas on moodustatud ministeeriumi töökeskkonna ning infoturbe korraldamise juhtkomisjon (edaspidi TIK). Mis on selle komisjoni roll ja milliste põhimõtete alusel loodud, st kes sinna kuuluvad? Kas keegi ka METKist?

    - Millisena näeb ministerium infoturbealast vastutust, mis lasub täna asutuse juhile? Kirjelda asutuse juhi rolli ja ülesandeid.

    - ISKE koordinaator täidab oma asutuses infoturbealaseid ülesandeid vastavalt õigusaktide nõuetele, ametijuhendile või töölepingule kooskõlas infoturbe poliitikaga. Kas ma saan õigesti aru, et igas asutuses on oma ISKE koordinaator? Mis on selle inimese roll ja kes see koordinaator METKis on? Kas E-ITSI puhul jääb see sama inimene nüüd lihtsalt E-ITSI koordineerima? Kas koordinaatorid teevad ka juhtkomiskoniga koostööd?

    - ITO põhimääruses on kirjas, et ITO "töötab välja ministeeriumi valitsemisala arengukavast lähtudes ministeeriumi ja ministeeriumi infosüsteemiga liitunud asutuse infotehnoloogia strateegia" – kas see dokument on olemas? Kellele on see suunatud?

3. Kuidas näed tänast infoturbealast koostööd ministeeriumi ja METKi vahel? Kuidas hindad tänast süsteemi?
4. Milline on sinu hinnang METKi hetkeolukorrale infoturbe vaatest, kui hästi oleme küberrünnete eest kaitstud ja kust sinu arvates meil king kõige rohkem pigistab? Millised oleksid sinu soovitused METKile?
5. Kirjelda lühidalt, milliseid muutusi on oodata asutustel seoses E-ITSi tulekuga?
6. Kas valitsemisala asutustele on uut E-ITS standardit tutvustatud ja ülemineku protsessi kommunikeeritud? Kui ei, millal on see planeeritud? Kui jah, siis millal sai asutus üleminekust teadlikuks?
7. Palun kirjelda lühidalt protsessi järgmisi samme, kuidas üleminek on kavandatud? Millal peab asutus standardile üle minema?
8. Milline saab olema uue standardiga vastutuse jagunemine ministeeriumi ja METKi vahel?

Lisa 4. Poolstruktureeritud intervjuukava Maaelu Teadmuskeskuse direktorile

1. Kirjelda lühidalt, mida tähendab sinu jaoks infoturve, kui oluliseks seda pead ja millised on esimesed infoturbega tekkinud seosed sinu peas?
2. Mida teed ise igapäevaselt infoturbealaste riskide maandamiseks?
3. Teooria ütleb, et infoturve on muutumas tehnilisest pigem äriliseks probleemiks. Milline on sinu nägemus sellest ja kas asutused on selleks valmis? Kuidas lahendada?
4. Ole hea ja kirjelda, kuidas on täna infoturve METKis juhitud ja milline on rollijaotus?
   - milline on sinu roll ja ülesanded asutuse infoturbe juhtimisel? Kuidas jagunevad teised rollid ja vastutused?
5. Kirjelda lühidalt standardi olemust, mille alusel käib hetkel infoturbe juhtimine METKis.
6. Millist rolli näed sina ministeeriumil selles protsessis? Kuidas koostöö sinu hinnangul täna toimib? Mis on hästi ja millest tunned puudust?
7. Räägime kommunikatsioonist nii ministeeriumi poolt METKi kui ka METKi sees.
   - Kuidas on korraldatud infoturbealane kommunikatsioon METKis ja kes selle eest vastutab?
   - Milline on sinu hinnangul olnud kogemus info jagamisega ministeeriumi poolelt ISKE standardilt E-ITSile üleminekul? Kas oled saanud ministeeriumilt piisavat ja õigeagset infot või on esinenud murekohti?

8. Kui oluliseks ja suureks murekohaks pead täna infoturbealaseid riske METKi jaoks?
9. Milliseid infoturbealaseid riske näed organisatsiooni ohustamas?

Lisa 5. Poolstruktureeritud intervjuukava strateegiajuhile

Teema plokk	Küsimus	Teoreetiline raamistik
Organisatsiooni strateegiliste eesmärkide defineerimine	Kirjelda palun lühidalt Maaelu Teadmuskeskuse visiooni ja missiooni.	Organisatsioon on sotsiotehniline süsteem, mis on loodud selleks, et teatud eesmärke saavutada või ülesandeid ellu viia. Organisatsiooni eesmärgid on aluseks protsessipõhisele juhtimisele. Defineeritud funktsionaalsed eesmärgid viitavad organisatsiooni prioriteetsetele protsessidele, kvaliteedieesmärgid kirjeldavad süsteemi olemust. Vajadus infoturbe järele lähtub eesmärkidest. (Muehlen & Ho, 2005, lk 457; Sommerville, 2015; Sterling & Taveter, 2009; Sulis & Taveter, 2022)
	Milleks on organisatsioon loodud ja mis on selle peamine eesmärk? Mida peab organisatsioon saavutama/tegema/millist rolli täidab?	
	Kas selle põhieesmärgi saab omakorda jaotada erinevateks aspektideks? Jagada alameesmärkideks, mis panustavad põhilise eesmärgi saavutamisse?	
	Kas ja kuidas mõõdetakse eesmärgi kvaliteeti? Mida sellelt sotsiotehniliselt süsteemilt oodatakse?	
Vastutuse määratlemine	Kes vastutab antud eesmärgi täitmise eest?	Protsessi edu tagamiseks on oluline, et sellel oleks vastutaja. See on üks viiest kriitilisest edutegurist. Iga eesmärgi täitmise eest peab keegi vastutama. (APQC, 2024; Hammer, 2007; Sulis & Taveter, 2022)

Lisa 6. Poolstruktureeritud intervjuukava protsesside modelleerimiseks

Teema plokk	Küsimus	Teoreetiline raamistik
Üldine plokk	Kirjelda palun oma sõnadega, mida mõistad protsessi all? Too mõni näide protsessist.	Protsessipõhise juhtimise järjepidev elutsükkel. Teadlikkus protsessipõhisest juhtimisest. (Dumas et al, 2018; Sulis & Taveter, 2022, lk 21)
	Kirjelda, mida näed sina protsessi eest vastutava inimese tööülesannetena.	
Protsessi skoop ja sisu	Pidades silmas kirja pandud funktsionaalset eesmärki, mille eest vastutad, kuidas sõnastaksid selle protsessina? Mida on vaja teha, et see eesmärk saavutada?	Protsessi tasand, seotus eesmärkidega, protsessi olemus (Dumas & et al, 2018; APQC, 2023)
	Mis on protsessi käivitav sündmus? Kes on selle protsessi algataja?	
	Millega protsess lõppeb? Mis on protsessi väljund?	
	Kirjelda üldises pildis, millised on selle protsessi vajalikud ja olulisemad etapid?	
	Millist sisendit on vaja protsessi õnnestumiseks?	
Rollid ja vastutused	Kes on protsessi osapooled?	Seotud osapooled ja nende mõju protsessi küberturvalisusele. Selgelt defineeritud rollide määratlemise olulisus. Rollid peegeldavad ülesandeid ja vastutust, mis protsessis osalevatele inimestele on antud, et eesmärk saavutada. Rollide vastutuse määratlemine annab omakorda sisendi protsesside modelleerimisse, kus vastutust on võimalik ümber sõnastada sooritatud ülesannetena. (Sommerville, 2015; Sterling & Taveter, 2009; Sulis & Taveter, 2022; Laybats & Tredinnick, 2016; Soomro *et al*., 2015)
	Milline on nende osapoolte roll ja vastutus?	
	Lähtudes vastutusest, mida nimetasid, siis kuidas sõnastaksid need vastutused ümber ülesanneteks, mida rollid tegema peavad?	
	Kas selle protsessiga on seotud organisatsioonivälised osapooli?	Informatsiooni liikumine protsessis ja võimalikud haavatavused. (Sommerville, 2015)
Gruppeerimine ja üldistamine	Vaadates määratletud rolle, kas on võimalik leida ka ühisosasid, mis neid rolle seob? On meil võimalik üldistada ning gruppeerida? Näide: laborianalüütik või meditsiiniõde on üks roll, ei pea minema spetsiifilisemaks.	Rollide määratlemisel on mõistlik otsida ühisosasid ja võimalusi üldistamiseks ning gruppeerimiseks, kus see on võimalik. Tervikpildi säilitamise huvides ei ole mõistlik laskuda liigsesse detailsusesse. (Sommerville, 2015, lk 152)

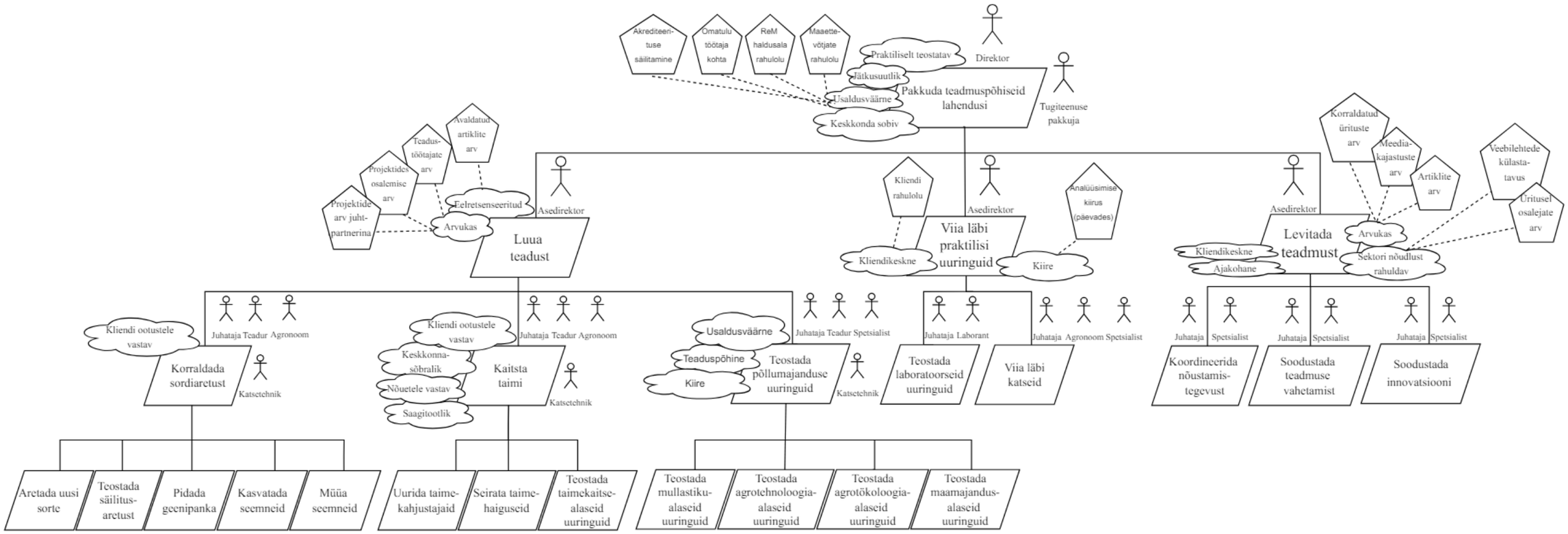
Lisa 6 järg

Info vajaduse tuvastamine	Vaadates protsessi etappe, loetle palun, millised infosüsteemid, andmebaasid jne on nende etappidega seotud? Millist infot on protsessi läbi viimiseks vaja ja mida luuakse?	Protsessiga seotud infrastruktuuri tuvastamine, mis on infoturbealase olukorra kaardistamisel ning riskide määratlemisel oluline. (Hammer, 2007, Sommerville, 2015)
	Kas sa oskad öelda, kuhu ja kuidas talletatakse protsessiga seotud andmeid? Milliseid keskkondi selleks kasutatakse? Kuidas on andmete talletamine reguleeritud?	
Tulemusnäitajate tuvastamine.	Millised on protsessi olulisimad kvaliteedimõõdikud?	Protsessi edu peab olema mõõdetav. Paigas peavad olema kvaliteedieesmärgid ja tulemusnäitajad. Tulemusnäitajad näitavad seda, kuidas kvaliteeti teatud eesmärgi puhul mõõdetakse. (Hammer, 2007; Sulis & Taveter, 2022, lk 85)
Infoturbealane teadlikkus ja protsessi ohustavad riskid	Kas oled teadlik organisatsioonis kehtivatest infoturbepoliitika põhimõtetest ning kuidas järgid seda oma igapäevase töö tegemisel?	ReM ITO infoturbepoliitika ja üldine teadlikkus infoturbe ning riskijuhtimise kohta. Protsessi omanik peab oskama märgata ja adresseerida ka infoturbealaseid riske, mis tema poolt juhitud muutustega kaasa võisid tulla. (Eesti infoturbestandard, 2024)
	Kirjelda, mida tähendab sinu jaoks infoturve, kui oluliseks seda pead ja millised on infoturbega seotud olulisemad probleemid, mis sulle meenuvad?	
	Milliseid infoturbealaseid koolitusi oled läbinud?	
	Mida teed igapäevaselt infoturbealaste riskide maandamiseks?	
	Vastutades antud protsessi eest, kas oled mõelnud ka infoturbealastele riskidele, mis sinu protsessi ohustavad? Kui suureks neid riske pead?	
	Kas teadvustad infoturbe riske ka siis, kui protsessis muudatusi teed?	

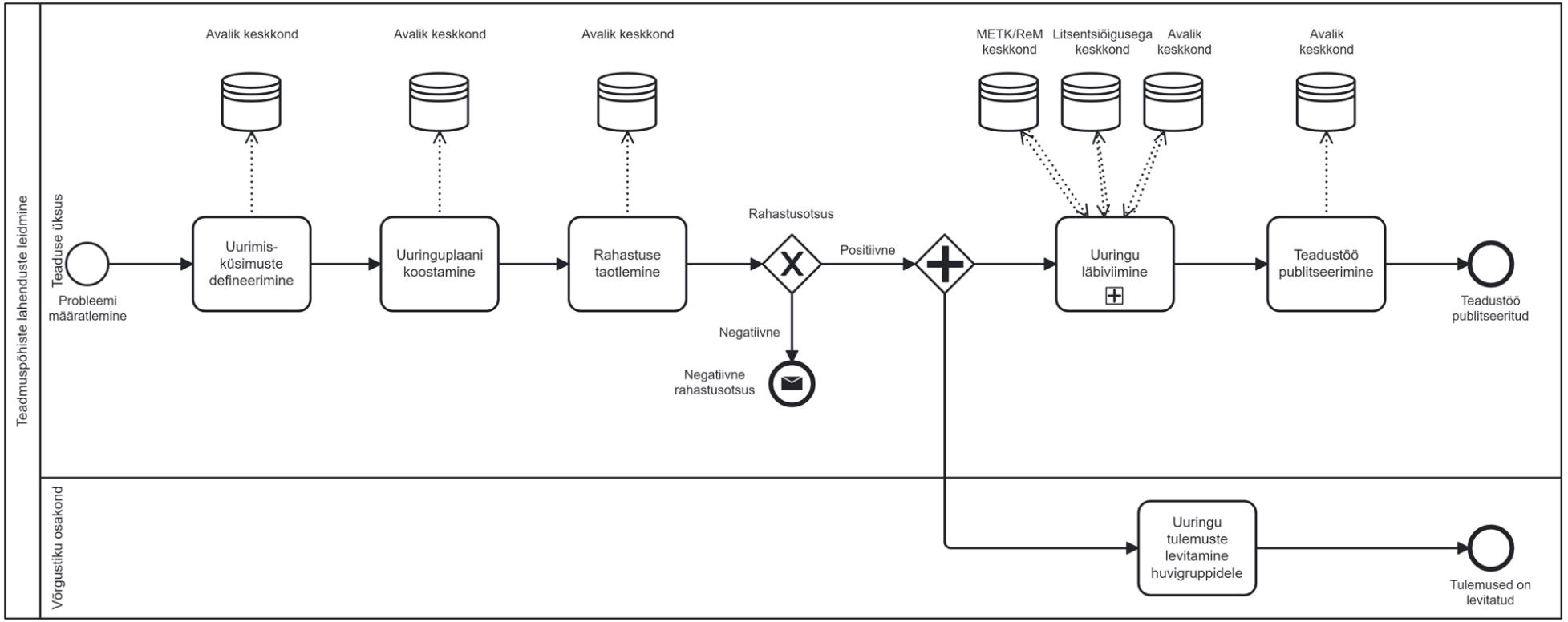
Lisa 7. Magistritöö empiirilise uuringu metoodika

Andmete kogumise väljund	**Andmete kogumis-meetod**	**Andmete analüüsi-meetod**	**Aeg**	**Valim/ allikad**
Sisend asutuse infoturbe hetkeolukorra kaardistamiseks	Dokumendi-analüüs	Kvalitatiivne sisuanalüüs	Veebruar 2024	METK põhimäärus, ReM IT-osakonna põhimäärus, info-turbepoliitika määrus, kvartaalsete IT-kohtumiste memod 2023-2024
Sisend asutuse infoturbe hetkeolukorra kaardistamiseks	Poolstrukturee-ritud intervjuu (vt lisa 3 ja lisa 4)	Kvalitatiivne sisuanalüüs	11.03.24 15.03.24	ReM infoturbejuht, METK direktor
I etapp: hetkeolukorra kaardistus asutuse infoturbealasest hetkeolukorrast				
Sisend asutuse missioonikriitiliste äriprotsesside tuvastamiseks	Dokumendi-analüüs	Kvalitatiivne sisuanalüüs	Veeburar-märts 2024	METK põhimäärus, otseste avalike teenuste loetelu, asutuse struktuurimudel, arengukava, HUKO
II etapp: asutuse eesmärgimudeli konstrueerimine (esmane versioon)				
Sisend asutuse missioonikriitiliste äriprotsesside tuvastamiseks	Poolstruktu-reeritud intervjuu (vt lisa 5)	Kvalitatiivne sisuanalüüs	12.03.24 19.03.24	METK strateegiajuht
II etapp: vastavuskontrolli läbinud eesmärgimudel				
Sisend E-ITS protsesside modelleerimisse, sidumine rollide ja ressurssidega	Poolstruktu-reeritud intervjuu (vt lisa 6)	Kvalitatiivne sisuanalüüs	26.03.24	Põllumajandusuuringute osakonna juhataja
Valmib III etapp: modelleeritud missioonikiitilised protsessid (E-ITS)				
Modelleeritud ja tegeliku protsessi vastavus	Vastavuskontroll	-	09.04.24 09.04.24	METK asedirektor teadustegevuse alal, METK asedirektor laborite ja katsetegevuse alal.
Ettepanekud standardi rakendamist takistavate asjaolude ületamiseks				

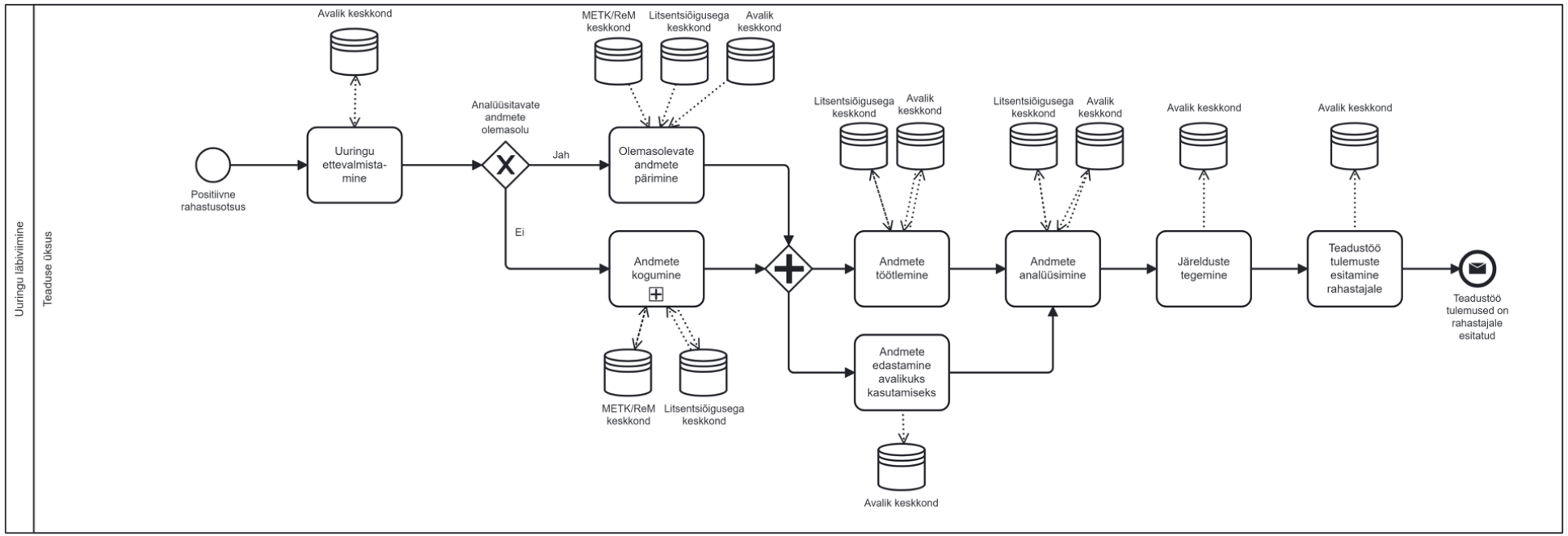
Lisa 8. Maaelu Teadmuskeskuse (*as-is*) eesmärgimudel



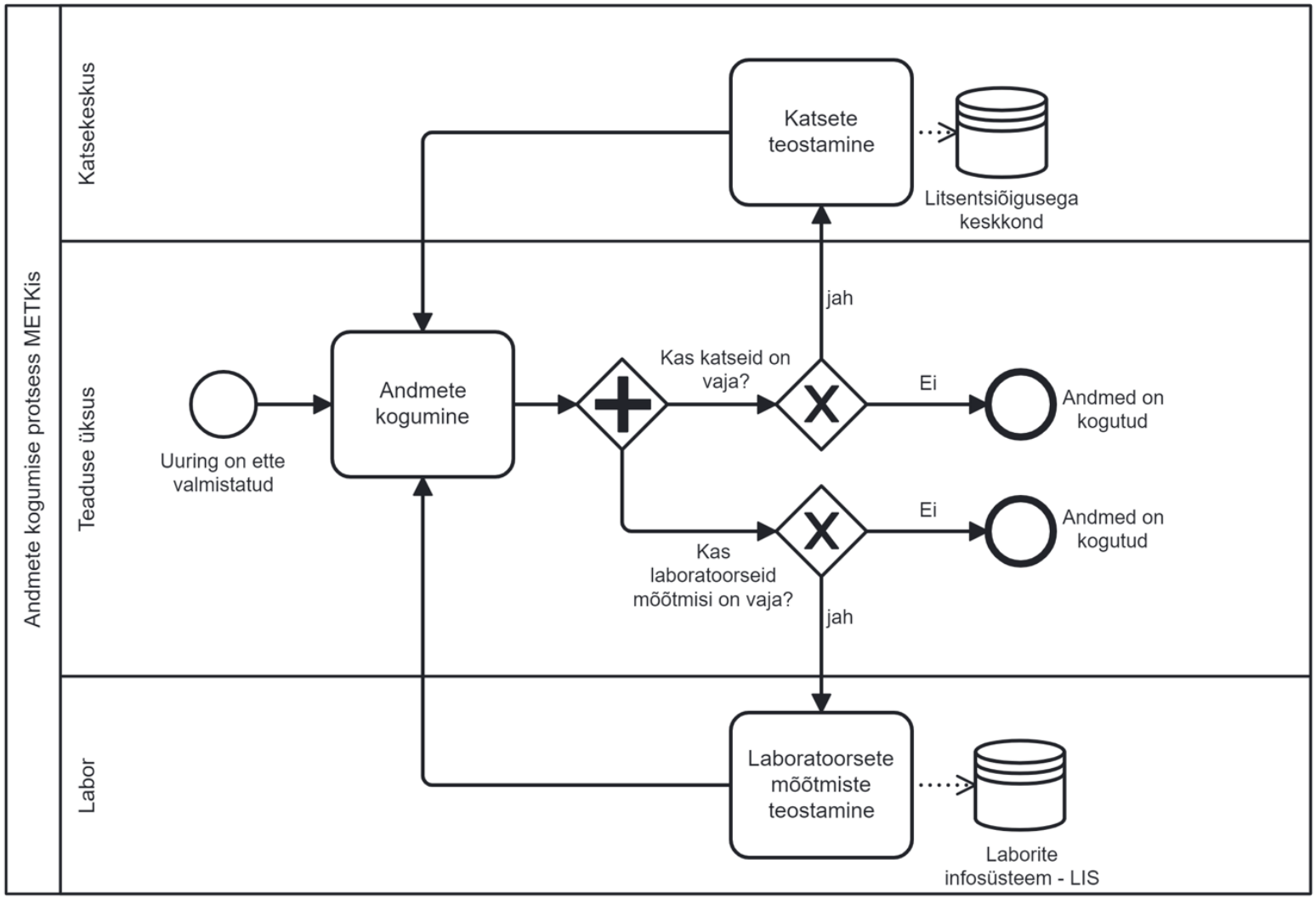
Lisa 9. Teadmuspõhiste lahenduste leidmise (*as-is*) protsess METKis



Lisa 10. Uuringu läbiviimise (*as-is*) protsess METKis



Lisa 11. Andmete kogumise (*as-is*) protsess METKis



SUMMARY

IMPLEMENTING THE ESTONIAN INFORMATION SECURITY STANDARD IN THE CENTRE OF ESTONIAN RURAL RESEARCH AND KNOWLEDGE

Triin Vasli

Cybercrime is a growing risk for organizations in today's digital era and one of the main risks for public sector organizations due to the large volumes of sensitive and personal data they handle. Cybercrime can endanger national security and lead to citizens distrusting their government. Therefore, it is important to mitigate cyber risks and ensure information security, especially in public sector organizations. In order to better address cyber security risks, a new Estonian Information Security Standard (E-ITS) was introduced in 2022. It replaces the previous three-tier system of baseline security of information systems (ISKE), which applied from 2003 to 2022. Implementation of E-ITS is important and mandatory for those subject to the Estonian Cybersecurity Act, ensuring the security of the country and its citizens.

E-ITS requires a novel, process-based approach to information security. Piloting the standard revealed several problems: it is difficult for liable parties to identify processes that need protection, the declarative language of the standard remains distant, and it is difficult to place the standard into the context of a particular organization. At the same time, the standard is obligatory since 2024, which shows the urgency of the problem. To the author's knowledge, several public institutions in Estonia have not yet implemented E-ITS. One of them is the Centre of Estonian Rural Research and Knowledge (METK), an institution under the Ministry of Regional Affairs and Agriculture (ReM).

In view of the aforesaid, the research problem is that E-ITS is not implemented by the liable parties, who thus fail to fulfil their legal obligations and thereby endanger the national security of Estonia and its citizens.

This master's thesis was conducted as a case study of METK. The objective of this thesis is to identify the reasons why METK has not yet implemented E-ITS and to propose ways for overcoming these obstacles.

To fulfil this objective, the following research questions were asked:
1. What obstacles does METK face in implementing E-ITS?
2. What are the possible ways to overcome these obstacles and implement the standard?

The conceptual part deals with information security management in the public sector, focusing on process-based management. Information security must be aligned with the organization's strategic goals (Estonian Information Security Standard, 2024). It involves business risks, therefore, it is increasingly seen as a business issue rather than a technical one (Kayworth and Whitten, 2010, p. 164).

It is important to protect the organization's mission-critical processes to ensure the functioning of public services. This knowledge has led to a process-based approach to ensuring cyber security, with the top management of the organization seen as playing a decisive role (Soomro *et al*., 2015, p. 223). In addition, it is important to define also other roles responsibilities in order to avoid the dispersion of responsibility and ambiguity of the tasks to be performed (Höne & Eloff, 2002, p. 404). Given that both social and technical aspects are involved in the processes, information security is addressed as a socio-technical issue in this thesis. As the weakest link in ensuring information security are people and their unpredictable nature (Laybats and Tredinnick, 2016, p. 79), it is essential to educate employees.

The second chapter addresses the situation of information security in Estonia, focusing on the new information security standard E-ITS. An overview of the researched organization and the research methodology is also given. The empirical study was conducted in three stages. The current information security situation of METK was mapped, the obstacles to implementing E-ITS were identified, METK's mission-critical processes were identified using a goal-oriented approach, and the most important process of the organization – providing knowledge-based solutions – was modelled using BPMN notation. The main databases and information systems used in the process were also mapped and the sub-processes – the process of conducting the study and the

process of data collection – were analysed. Since the identification of business processes has been a difficult point for those subject to E-ITS, the author proposed a practical example for process identification as an additional result of the thesis.

The study was conducted using qualitative methods, document analysis and semi-structured interviews, and a compliance check was performed to compare the actual business process with the created model. The thesis focused on the as-is view of the processes and did not address the to-be view, as it is not needed to implement E-ITS.

The conducted analysis revealed twelve obstacles to implementing E-ITS in METK. A key finding is that the current situation of information security in METK does not support E-ITS implementation. Among other obstacles, there is a lack of resources, the need for information security is undervalued, the specific roles and responsibilites are not in place and serious communication problems exist between ReM and METK.

Eleven suggestions on how to overcome the identified obstacles were made to the persons responsible for METK's information security management and E-ITS implementation. The results and suggestions of this study may also be of interest to other organizations subject to the standard, who are facing similar obstacles and have not yet implemented E-ITS.

As the most important suggestions, the author would like to emphasize the importance of assigning specific roles, responsibilities and tasks related to information security management in the organization and ensuring systematic cooperation between IT and the business side. It is also important to update the information security documentation, map the organization’s actual information security needs, find the necessary financial resources to cover those needs, and systematically educate the employees. Since business processes have not been mapped in METK before, the organization could benefit from process mapping and implementing a process-based management system.

In this thesis, the circumstances preventing the implementation of E-ITS were investigated from the information security point of view, which can be considered as a limitation of the work and as a possible topic for further research, because obstacles may also occur outside the field of information security.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Triin Vasli,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Eesti infoturbestandardi rakendamine Maaelu Teadmuskeskuse näitel“, mille juhendajad on Linda Rosenkron ja Arvi Kuura, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Triin Vasli

17.05.2024