TARTU ÜLIKOOL

Majandusteaduskond

Ragner Paevere, Einar Laagriküll

DEVSECOPS TÖÖKORRALDUSE JUURUTAMISE VÕIMALUSED AVALIKUS SEKTORIS SISEMINISTEERIUMI INFOTEHNOLOOGIA- JA ARENDUSKESKUSE NÄITEL

Magistritöö

Juhendaja: Kaasprofessor Eneli Kindsiko, PhD

Kaasjuhendaja: Helen Poltimäe, PhD

Tartu 2021

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

Sisukord

Sissejuhatus....4

1. DevSecOps töökorralduse teoreetilised alused ja kasutamise võimalused....6

1.1. DevSecOps töökorralduse olemus ja roll....6

1.2. DevSecOps töökorralduse ja muudatuse kriitilised edutegurid....12

1.3. DevSecOps töökorralduse juurutamise võimalused avalikus sektoris....19

2. DevSecOps töökorraldus SMIT näitel....26

2.1. Uurimisprotsessi ja SMIT tutvustus....26

2.2. DevSecOps kriitiliste edutegurite kitsaskohad SMIT-s....31

2.3. SMIT-s DevSecOps koostöö mudeli juurutamise võimaluste analüüs....41

Kokkuvõte....45

Viidatud allikad....48

LISA A. Intervjuu küsimused....55

LISA B. Küsitluse ankeet....58

LISA C. Kriitiliste edutegurite koondumine faktoriteks(mina)....60

LISA D. Juhtide intervjuude kodeerimine....61

LISA E. Spearmani korrelatsiooni analüüs....62

Summary....63

Sissejuhatus

2017 augustis tuli ärev teade Tšehhi teadlastelt, kes leidsid Eesti ID-kaardi turvanõrkuse. Teatati, et Infineoni turvakiibis on avastatud haavatavus ja võimalik on varastada iga kodaniku identiteet kui midagi ette kiirelt ei võeta. Üle maailma puudutas see pea miljardit ID kaardi kiipi. Eestis mõjutas see ca 750 000 ID kaarti, elamisloakaarti ja digitaalset isikutunnitust. Seni vankumatuna tundunud Eesti e-riigi alustala ID-kaarti puudutavad arusaamad tuli sellel hetkel ümber vaadata. (Kund, 2017) Tänaseks on aga Eesti e-riik astunud jõudsalt edasi ja lisandunud on palju uusi e-teenuseid, nende hulgas näiteks e-surm ja e-sünd ehk teenused, mis võimaldavad registreerida surma ja sündi läbi e-teeninduse (Delfi, 2020; Postimees, 2019).

Märtsis 2020 kuulutati välja üle maailma Covid-19 pandeemia. Suleti piirid, koolid ja Eesti Vabariigi Valitsus kuulutas välja kriisi. (Valitsuse kommunikatsioonibüroo, 2020) Aprillis 2020 teavitasid videokõnede platvormi pakkuvad ettevõtted plahvatuslikust liiklusmahu kasvust ja kasutajate lisandumisest - mahud kasvasid mitmesaja protsendiliselt võrreldes kriisieelse ajaga (O'Halloran, 2020; Paul, 2020). Covid-19 sundis enamiku inimkonnast otsima uusi viise, kuidas teha tööd kodukontorist, kuidas osaleda loengutel ja kuidas suhelda uues olukorras sõprade ja tuttavatega. See kõik tekitas massiivse kasvu e-teenustes. Samas oli suure eduloo taga näha ka probleemkohti. Novembris raputas Eesti ühiskonda uudis, et kolme ministeeriumi vastu on toimunud sarnase käekirjaga rünnakud, mille käigus lekkisid 9158 isiku andmed. Lisaks varastati ühe ministeeriumi serveritest 350 gigabaiti andmeid. (Tooming et al., 2020) Aastast 2015 on maailmas kasvanud rünnetest tulenev kahju 100% ning 2021 ennustatakse kogu kahju tasemel 6000 miljardit USD (Contact Commitee, 2020). See kõik näitab selgelt, et organisatsioonid peaksid keskenduma lisaks teenuse funktsionaalsuse arendamisele ka e-teenuste turvariskidele ja muudele turvaaspektidele.

Avaliku sektori asutusena pakub Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT) kriitilise tähtsusega IT teenuseid mis on otseselt seotud kodaniku identiteedi ja turvalisusega. Sellest tulenevalt on IT turvalisuse fookus järjest olulisem ka SMIT teenustes. Seda eriti, kuna sisejulgeoleku kontekstis on asutuse poolt pakutavad teenused kõrgendatud huvi all nii avalikkuse kui ka küberkurjategijate vaatest. Oleme kodanikuna usaldanud väga suure osa oma elektroonilisest identiteedist ja andmetest riigile. Ühest vaatest tahame kodanikuna kõike ja kohe, ideaalis igal pool ja ülimugavalt kasutada ning samal ajal on meil

ülikõrged ootused riigile andmete hoidmise ja turvalisuse osas. Tunneme ju Eestit kui ühte turvalist e-riiki ja referentsi terves maailmas.

Selleks, et eelpool toodud riskid ei realiseeruks on SMIT liitnud ca 2 aastat tagasi ärivaldkondades arenduse ja haldusüksused ning moodustas tervikvastutusega tiimid, kes uues töökorralduses vastutavad nii IT arenduse kui ka halduse eest ehk DevOps (*development and operations*) töökorralduse eest. DevOps töökorralduse juurutamise järgselt on esile kerkinud aga uued töökorralduslikud kitsaskohad, mis on eriti tugevalt nähtavad koostöös arendusüksuse ja infoturbeüksuse vahel. Lisaks sellele on probleemiks tänaste DevOps tiimide võime näha tervikut. See tähendab, et arenduse DevOps üksus on eelkõige huvitatud arenduse tähtaegsusest, ehk funktsionaalsuste valmimisest, samas IT turbeüksus üritab maksimeerida arenduste turvalisust ja tehnoloogia keskendub lahenduse kvaliteedile. See kõik sunnib otsima uusi viise ja meetodeid, kuidas koostöömudelit IT asutuses edasi arendada ja millisel viisil on võimalik saavutada järgmine kvaliteedihüpe IT arengus avalikus sektoris. SMIT üksuste vahel on erinevast fookusest tingituna vastutused hägustumas. Üksuste üleselt erinevate fookuste nimel töö tegemine leiab uue tähenduse ka tellijate vaates, kus on näha omavahelise koostöö takerdumisest tingitud tootlikkuse langust. SMIT puhul on tellijateks Siseministeerium, Politsei- ja Piirivalveamet, Sisekaitseakadeemia, Päästeamet ja Häirekeskus. Tellija ootuste ja kvaliteedi vahel tasakaalu leidmise käigus aga kipuvad huvid ning eesmärgid põrkuma. Selle tulemusel venivad projektide tähtajad, mis tekitavad tulemit mitte loovaid vaidluseid ja asutusele tekib täiendav kulu. Välisrahastusega finantseeritavatele projektidele kaasneb sellest olukorrast veel ka risk, et organisatsioonil tuleb leida täiendavad vahendid selleks, et kompenseerida rahastustingimuste mitte täitmisest tulenevaid nõudeid. Samuti mõjutab olukord asutuse töörahulolu.

Turbefookuse kasvuga on IT valdkonnas üle maailma kerkinud esile uus koostöövorm, kus senist DevOps tiimide koostöötamise loogikat on laiendatud ka teistesse distsipliinidesse. Üks selline koostöövorm, kus senistesse halduse ja arenduse tiimidesse on integreeritud lisaks ka küberturbe vastutus on DevSecOps (*development, security and operations*) töökorraldus. (Raynaud, 2017) SMIT vaatest annaks selline lähenemine võimaluse maandada IT arendamise riske, parandada koostööd üksuste vahel ja vähendada arenduste tähtaegade venimisi ning hilises faasis vigade parandamisi. See omakorda looks täiendavat väärtust tellijale ning autorite arvates võiks aidata asutusel võtta kasutusele efektiivsema ja kaasaegsema töökorralduse, et liikuda järgmisele arengutasemele. Avaliku sektori kriitilise tähtsusega IT teenuste osutajale annaks selline lähenemine võimaluse tagada

nii arenduskiirust kui ka turvalisust samaaegselt. Sarnase töökorralduse kasutamist ei ole Eestis siiani avaliku sektori näitel uuritud ja autorite teada ei olda seda seni ka kasutatud.

Magistritöö eesmärk on tuua esile DevSecOps töökorralduse rakendamise võimalused avaliku sektori IT organisatsioonis SMIT näitel.

Uurimiseesmärgi täitmiseks on autorid seadnud järgmised uurimisülesanded:

-Avada DevSecOps olemus ja roll

-Anda ülevaade DevSecOps töökorralduse ja muudatuse kriitilistest eduteguritest

-Kaardistada DevSecOps juurutamise võimalusi avalikus sektoris

-Uurida DevSecOps kriitiliste edutegurite kitsaskohti SMIT-s

-Selgitada DevSecOps koostöömudeli juurutamise võimalusi SMIT-s

Magistritöö koosneb kahest peatükist. Esimeses peatükis uuritakse teaduskirjanduse põhjal DevSecOps olemust ja rolli ning selgitatakse välja töökorralduse kriitilised edutegurid. Samuti uuritakse antud töökorralduse juurutamise võimalusi avalikus sektori IT organisatsioonis.

Teine peatükk on empiiriline, keskendudes SMIT töökorralduse parendamise uurimisele. Esimeses faasis tutvustatakse asutust ja uurimismeetodeid, siis liigutakse edasi kriitiliste edutegurite tänase olukorra analüüsile ja sealt edasi DevSecOps koostöömudeli juurutamise võimaluste analüüsi. Uurimismeetodina kasutatakse kvantitatiivset ja kvalitatiivset uuringut. Küsitlus teostatakse organisatsiooni tiimides selleks, et kontrollida organisatsiooni valmidust töökorralduse muudatuse juurutamiseks ning hinnata muudatuse võimalikku edukust. Lisaks teostatakse arendusüksuse juhtidega kvalitatiivsed intervjuud teooriast leitud kriitiliste edutegurite olemasolu uurimiseks SMIT-s.

Märksõnad: DevSecOps, DevOps, Avalik sektor, Arendus, Organisatsioon, Koostöö

Teaduseriala kood CERCS: S190 Ettevõtte juhtimine

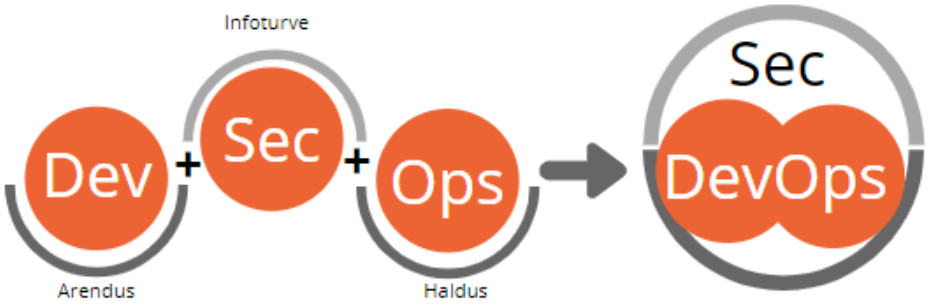
1. DevSecOps töökorralduse teoreetilised alused ja kasutamise võimalused

1.1. DevSecOps töökorralduse olemus ja roll

IT valdkonnas konkurentsis püsimiseks peavad tehnoloogia organisatsioonid suutma kiiresti arengutega kaasa minna. Parimad tarkvara arendavad asutused vajavad oma töö tulemuslikkuse juhtimiseks selgeid ja läbipaistvaid tavasid. Juhtide jaoks on töökorralduse tavade parandamine üheks põhiliseks juhtimisinstrumendiks kiiruse, efektiivsuse ja kvaliteedi eesmärkide saavutamisel (GitKraken, 2020). Tehnoloogiline areng on loonud soodsa pinna uutele asutustele tänu madalamatele sisenemisbarjääridele. See omakorda survestab turul toimetavaid organisatsioone läbi mõtlema oma tööprotsessid ja investeerima digitaalsetesse

tehnoloogiatesse. (Szabo et al., 2020) Infoturve ja küberturvalisus on saamas kriitilisteks aspektideks asutuse eduka toimimise vaatest (von Solms et al., 2018). Digitaalsetesse protsessidesse investeerimise tulemusena kasvab organisatsioonides erinevate digitaalsete tehnoloogiate hulk (Szabo et al., 2020), mis omakorda tingib infoturbega seotud riskide kasvu ja tõstab asutuse juhtide poolset fookuse ning riskidega tegelemise vajadust (von Solms et al., 2018).

DevSecOps on turvalisuse integreerimine kiirelt arenevasse IT- ja DevOps-arenduse kultuuri, tehes seda samas võimalikult sujuvalt ja läbipaistvalt. Ideaalis tuleb seda tagada nii, et arendajate töötamise kiirus ei väheneks ja arenduse töös ei tekitataks ebamõistlikke katkestusi või hilistusi. (Gardner et al., 2019) DevSecOps põhineb DevOps ja CAMS(***C**ulture, **A**utomation, **M**easurement, **S**haring*) põhimõtetel – kultuur, automatiseerimine, mõõtmine ja jagamine, kuid lisab sellele ka turvalisuse arendusprotsessi algusest alates. DevSecOps-i nähakse kui DevOps-i laiendust, mille eesmärk on integreerida turbekontroll ja protsess DevOpsi tarkvara arendusprotsessi tsüklisse. Seda tehakse läbi koostöö edendamise turbetiimi, arendustiimi ja haldustiimi vahel. (Department of Defense, 2020; Koskinen, 2020; Myrbakken et al., 2017) DevSecOpsi töökorraldusliku muutuse peamine omadus on turvalisuse automatiseerimine, monitoorimine ja juurutamine kõigis elutsükli etappides (Lam et al., 2019). Joonis 1 toob esile DevSecOps olemuse.

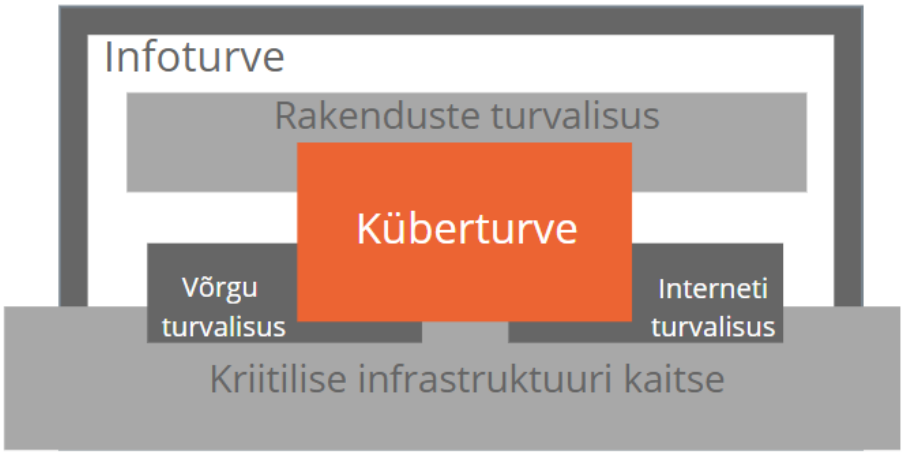


Joonis 1. DevSecOps töökorraldus
Allikas: Autorite loodud

Infoturbe eesmärk on kaitsta andmete terviklikkust, konfidentsiaalsust ning käideldavust (von Solms et al., 2018). Andmete töötlemiseks kasutatavate infosüsteemide terviklikkust, käideldavust ning salastatust ohustavad järjest enam globaalsed ja regionaalsed küberründed, mis omakorda on tõusvas trendis kogu maailmas (RIA, 2020). Terviklikkust tõlgendatakse info täpsuse ja usaldatavuse tagamisena, konfidentsiaalsust info ligipääsu piiramisena ja käideldavust info kättesaadavuse tagamisena (Tchernykh et al., 2015). Nende

kolme aspekti kaitsmise keerukus tuleneb sellest, et nad on omavahel seotud ja vaja on leida tasakaal, mis on raske, kuna liigne fookus käideldavusele kompromiteerib suure tõenäosusega terviklikkust ja konfidentsiaalsust. Samas liigne fookus konfidentsiaalsusele seab ohtu käideldavuse. (Aminzade, 2018)

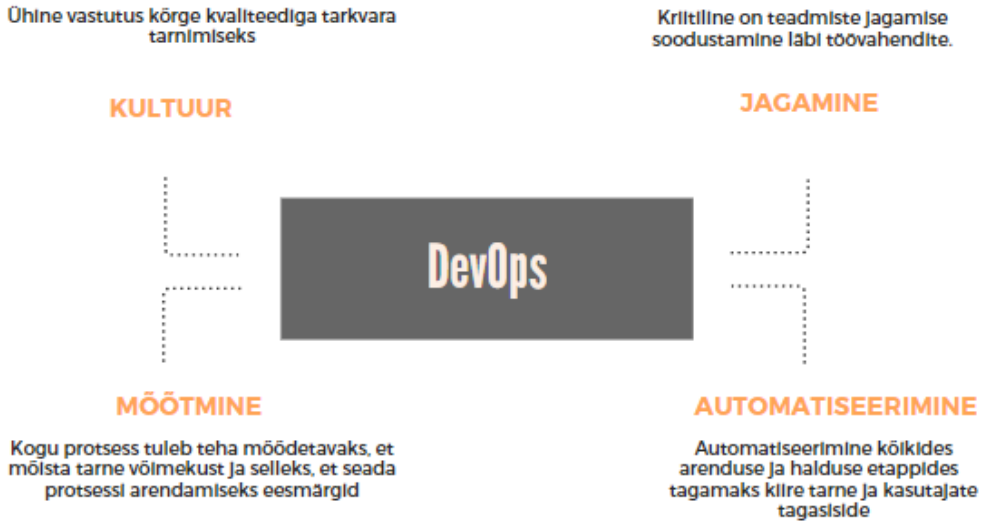
Infoturve tegeleb informatsiooni haldamisega olenemata tema kujust. Infoturve hõlmab nii füüsilisi dokumente, digitaalseid tõendeid kui ka intellektuaalset omandit. Küberturve on osa infoturbest, mis tegeleb organisatsiooni digitaalse informatsiooni kontrollimise ja kaitsega riskide eest, mis tulenevad internetist. (von Solms et al., 2018) DevSecOps on koostöövorm, kus senise halduse ja arenduse tiimidesse on integreeritud lisaks ka küberturbe vastutus (Raynaud, 2017). Infoturbe ja küberturbe seotus on toodud välja joonisel 2.



Joonis 2. Infoturve vs küberturve
Allikas: von Solms et al., 2018

Antud töös on autorite hinnangul oluline keskenduda töökorralduslikule muutusele, mis kaasab halduse ja arendusüksuse juurde ühe täiendava olulise osa, milleks on infoturve. DevSecOps on algselt välja kujunenud DevOps põhimõtete edasiarendamisest (Myrbakken et al., 2017). DevOps on viimase kümnendi jooksul esile kerkinud arenduse ja halduse kontseptuaalne koostöömudel, mis aitab vähendada IT arenduse ja halduse vahelist distantsi ning võimaldab juurutada pidevat arendustsüklit ja publitseerida tarkvara sagedasti. Samuti aitab DevOps arendusel ja haldusel koos efektiivsemalt toimida. (Erich et al., 2014) DevOps on eelkõige IT organisatsiooni kultuuriline töökorraldusliku praktika muutus, ehkki seda võib vaadelda ka protsessi või töövahendit hõlmava muutusena. Seda nähakse kui muudatust kultuuris, mille tulemusena paraneb koostöö arenduse ja halduse vahel, ehk see on tarkvara loomisega seotud eri osapoolte kavatsuste joondamine. Eelkõige nähakse selle töökorralduse

edu läbi kultuuri, automatiseerimise, mõõtmise ja teadmiste jagamise. (Sánchez-Gordón et al., 2018) Joonisel 3 on välja toodud DevOps töökorralduse neli dimensiooni.



Joonis 3. DevOps töökorraldus

Allikas: Autorite loodud

Samas DevOps-i on kritiseeritud selle eest, et ta ei keskendu turvalisusele, sest DevOps juurutamisel jäetakse paljudel juhtudel turbe aspekt katmata. Uuringute kohaselt ainult 20% juhtudest integreeritakse IT turve DevOps initsiatiivi. See viitab sellele, et tiimid näevad IT turvet pidurdava elemendina, mis takistab agiilsust ja arenduskiirust. (Myrbakken et al., 2017) Samas on DevOps töökorraldust rakendanud organisatsioonides läbi viidud uuringutest selgunud, et üle poolte juhtidest usub, et infoturbe inimesed on kaasatud arendusprotsessi, samas tarkvaraarendajatest nõustub sellega natukene üle kolmandiku (Koskinen, 2020).

DevSecOpsi kasutuselevõtt ei tähenda ainult turbevahendite lisamist automatiseeritud arendusprotsessi, vaid see eeldab, et turve on integreeritud DevOps nelja printsiibiga: kultuur, automatiseerimine, mõõtmine ja jagamine. DevSecOps on oma olemuselt transformatsioon, mis integreerib turbekultuuri, praktikad ja vahendid igasse DevOps protsessi faasi. Kaasates turbeeksperdid arendusprotsessi algusest peale on lihtsam planeerida ja juurutada turbe mehhanisme läbi arendusprotsessi ilma, et tekitatakse hilistusi. Juurutades turvet protsessi lõpus on muudatuste mõju suurem ja hilistused võivad olla pikemad. (Department of Defense, 2020; Koskinen, 2020; Myrbakken et al., 2017) Turbe automatiseerimine võimaldab hoida arendusprotsessi kiirena (Nassereddine, 2020) ning kasutades selle juures integreerimist automatiseerimise töövahenditega on võimalik tagada, et ei teki infosulgu ja

organisatsioon saab turbele keskenduda proaktiivselt ja ennetavalt (Raynaud, 2017). See aitab vähendada ja paremini hinnata riske ning võimaldab tekitada reeglistikke ja protseduure nende vältimiseks (Myrbakken et al., 2017). Automatiseerimise eeliseks on see, et protsessid on järjepidevad ja korratavad ning nende tulem on ennustatav sarnaste testide korral. See võimaldab arendusprotsessi vältel logida ja dokumenteerida automatiseeritult. Samuti saavad arendajad automatiseeritud turbe vahendeid ise ilma kõrvalise abita kasutada. (Ahmed et al., 2019) Selle tagajärjel vähenevad adresseerimata turvanõrkuste mahud ja inimvead (Moore et al., 2018). Arendusprotsessi käigus loodud turbenõuetega saab tekitada olukorra, kus turbe tiim ei pea iga projekti eraldi nõustama, see vabastab nende aega ning aitab neil keskenduda tööle, mis loob suuremat väärtust (Koskinen, 2020). Samas ei ole oluline turbe juurutamine ainult arendusprotsessis endas vaid ka infrastruktuuris, et tagada keskkondade turvalisus (Mao et al., 2020). Turbe juurutamine projekti alguses on odavam kui selle tegemine olukorras, kus esimene turbe intsident juhtub. Uuringute kohaselt raiskavad kõrge tulemuslikkusega tiimid vähem aega mitte planeeritud tööde tegemiseks ja lahenduse ümber arendamiseks. Võime monitoorida ja mõõta turvet protsessi nii varajasest algusest kui võimalik tagab, et kasutusele võttu takistavad tarkvaravead avastatakse ja hinnatakse ära. See vähendab vigade tegemise, nende leidmise ja parandamise kulu. (Department of Defense, 2020; Myrbakken et al., 2017)

Suurimaks turbe teemaliseks väljakutseks kujuneb see, kuidas tagatakse soovitud tasemega turve keskkonnas, mis on pidevas muutuses. Teiseks väljakutseks on kuidas balansseerida kiireid arendusi ja turvet, mis on ka autorite kogemusel üks olulisemaid aspekte. Võtmetähtsusega selles protsessis on koostöö arenduse, halduse ja turbetiimidega, kus kõik liikmed töötavad sama eesmärgi nimel ja soovivad ellu viia organisatsiooni visiooni - olgu selleks siis turbele, tarnele või kvaliteedile orienteeritus. Organisatsioon, kes juurutab automatiseeritud turvet peab meeles pidama, et kõike ei saa automatiseerida. Automaatsed töövahendid võivad aidata lihtsalt koodi haavatavust analüüsida, kuid need ei aita hinnata, kas lahenduse disain on turvaline. Selleks on jätkuvalt vaja IT turbe eksperdi poolset manuaalset tööd. Ilma turbe nõueteta on väga raske tagada, et lahendused on turbe vaatest õigel tasemel. (Koskinen, 2020)

Samas on oluline aspekt ka see, et töötajad võtavad vastutuse ja näevad äritulemusteni jõudmist ning ka turvalisust osana enda rollist (Myrbakken et al., 2017). Ilma selleta, et töötajad võtavad turvet enda töö osana ja enda vastutusena jääb infoturve eraldi tiimi vastutuseks, mis tähendab, et turvalisuse lahendusse ehitamine jääb arendusprotsessi vaatest

hilisesse faasi ja see omakorda tähendab terve arenduse vaatest kulukasvu, sest turvet juurutatakse pigem arenduse lõppfaasis (Department of Defense, 2020).

Lisaks on oluline ka töötajate parendustele orienteeritus, kuna kiirelt ja varakult vigadest õppimine toetab organisatsiooni õppimist ja pidevat arengut. See soosib omakorda vigade ja nõrkuste kiiret parendamist ning annab positiivse efekti lahenduste turvalisusele. (Department of Defense, 2020; Morales et al., 2020) Samuti mängib turbe integreerimise juures suurt rolli tiimide vaheline läbipaistvus, kuna see toetab töötajate vahelist koostööd ning soodustab töötajate vahelist teadmiste jagamist, mis omakorda võimaldab organisatsioonil kiiremini edasi areneda (Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017). Samas on vaja DevSecOps tiimides teadmisi turbeprintsiipidest ja meetoditest, mis loovad organisatsioonile võimekuse juurutada turvet arenduse käigus ja aitab neil vältida hilisemat lahenduse parendamist ning ümberehitamist (Morales et al., 2020; Raynaud, 2017). Seda käsitletakse ka kui turbe arendusprotsessis vasakule liigutamist, ehk turbest tulenevaid aspekte käsitletakse arendusprotsessis võimalikult vara (Koskinen, 2020).

Läbipaistvuse ja selguse kasvatamise vaatest aitab organisatsioone see, kui asutuses juurutatakse äriväärtust peegeldavad mõõdikud (Wagner et al., 2020). Läbi selle on töötajatel võimalik mõista kuidas asutusel läheb ja see annab neile võimaluse leida uusi parendusvõimalusi ning peegeldada oma töö mõju tulemustele (Myrbakken et al., 2017). Samas on oluline turbe ohtude ja nõrkuste mõõtmine terves arendusprotsessis, mis toetab organisatsiooni võimekust avastada probleemid varakult ja läbi selle vältida hilisemaid kalleid muudatusi (Department of Defense, 2020).

DevSecOps töökorralduse positiivsete aspektidena nähakse kulu vähendamist, kuna vigade õigeaegne avastamine ja lahendamine aitab täiendavaid kulusid vältida. Samuti aitab see kaasa ka tarne kiirusele, kuna vähem tegeletakse lahendustes tagantjärgi leitud vigade parandamisega. Teise positiivse faktorina nähakse turberiskide paremat maandamist ja teadlikumat juhtimist. See võimaldab probleeme vältida ja olukorras, kus intsident juhtub, on sellest taastumine kiirem ning valutum. Samuti aitab turberiskide proaktiivne käsitlemine organisatsioonil vältida halba mainet ja meediakajastust, mis omakorda mõjutab müügitulemusi, kuna lihtsam on müüa turvalist toodet. Lisaks sellele aitab DevSecOps asutusel võimustada turbe eest vastutamist ja soodustab avatud ja läbipaistva kultuuri juurutamist läbi kõigi arendusprotsessi faaside. (Raynaud, 2017)

Kokkuvõttes on DevSecOps organisatsiooni töökorraldus, mis põhineb agiilsetel põhimõtetel ja olemuslikult on DevOps töökorralduse edasiarendus. Selle töökorralduse eesmärk on kombineerida agiilne DevOps infoturbega ning läbi selle tagada äritulemusi ning

maandada erinevaid turbest tulenevaid riske. Autorid nõustuvad nende uurijatega, kelle arvates ei saa antud töökorraldust vaadata kui tehniliste turbe töövahendite juurutamist, vaid pigem turbe juurutamisena ettevõtte kultuuri. Selleks, et mõista paremini DevSecOps töökorralduse juurutamist on oluline leida muudatuse edukaks elluviimiseks kriitilised edutegurid. Järgmises peatükis vaatleme DevSecOps töökorralduse kriitilisi edutegureid ja muudatuse elluviimise vaatest olulisi aspekte.

1.2. DevSecOps töökorralduse ja muudatuse kriitilised edutegurid

Rockart tutvustas 1979. aastal kriitiliste edutegurite kontseptsiooni, mis oli juhtide aitamiseks mõeldud meetod, võimaldamaks juhtidel leida nende jaoks kõige relevantsem info selleks, et nad saaksid edukalt oma eesmärke saavutada. (Rockart, 1979; Stankovic et al., 2013) Bullen ja Rockart arendasid 1981. aastal meetodit edasi. Nende definitsiooni kohaselt on kriitilised edutegurid piiratud hulk valdkondi, milles rahuldav tulemus tagab indiviidi, osakonna või organisatsiooni konkurentsivõimelise ja eduka tulemuslikkuse. Kriitilised edutegurid on võtmekohad, milles „asjad peavad minema õigesti“ selleks, et äri „õitseks“ ja juhid suudaksid oma eesmärke täita. (Bullen et al., 1981; Chow et al., 2008)

Kriitilised edutegurid ei ole protsessi väljundid, vaid nad on tegevused protsessis, milles tulemuslikkus on oluline (Newton et al., 2019). Konkurentsis edukaks olemiseks peab organisatsioon funktsioneerima kui integreeritud süsteem, kus juhtimine ja juhtimissüsteem on joondatud strateegiliste eesmärkidega (Ferreira et al., 2019) ning joondatud on ka organisatsiooni äri- ja IT-strateegia (Gerow et al., 2014). Kriitilised edutegurid ei ole ühe organisatsiooni spetsiifilised, neid saab üldistada kõikidele organisatsioonidele, mis toimetavad sarnase strateegiaga sarnases tööstusharus. Konkurentsieelis tekib organisatsiooni unikaalsest võimekusest täita neid faktoreid viisil, mis kasutab ära sisemisi tugevusi ja ressursse. (Newton et al., 2019) Millest autorite nägemuses võib järeldada, et antud uurimustöö käigus otsitavad kriitilised edutegurid on üldistatavad ka teistele avaliku sektori IT organisatsioonidele.

Tööstus 4.0 valdkonnas on toimumas radikaalne muutus, milles on edukad ettevõtted, kes juurutavad muudatusi tulemuslikult (Sony et al., 2020) ning kes suudavad adresseerida küberturvalisust (Clim, 2019). Chow ja Cao (2008) liigitasid agiilse tarkvara projektide kriitilised edutegurid nelja kategooriasse: organisatsioon, inimesed, protsessid ja tehnoloogia. Infoturbe juhtimissüsteemi eduka juurutamise vaatest on kriitiliseks eduteguriks eelkõige inimfaktor (Tu et al., 2018). Organisatsiooni tugevaks infoturbekultuuriks loetakse seda, kui teavet kaitstakse kogu selle elutsükli jooksul kõigis arenduse faasides, kus töötajad sellega mingil viisil kokku puutuvad. Oluline on, et töötajate üldised teadmised organisatsiooni

infoturbepoliitikast ja nõuetest oleks tasemel. (da Veiga, 2018) Infoturbel on väga konkreetne ja selge eesmärk - kaitsta andmete terviklikkust, konfidentsiaalsust ning käideldavust (von Solms et al., 2018). Infoturbe organisatsioonis juurutamiseks tuleb läbida 7-astmeline protsess, mis algab infoturbe halduse süsteemi skoopimisest ja turbepoliitika defineerimisest ning lõppeb mõõdikute ning turbe juhtimise valikute tegemisega (vt. Joonis 4) (Nurbojatmiko et al., 2016).

Joonis 4. Infoturbe juurutamise protsess
Allikas: Nurbojatmiko et al., 2016

Infoturbe halduse süsteemi skoopimine on infoturbe juurutamise esimene samm (Nurbojatmiko et al., 2016), mille käigus hinnatakse organisatsiooni, huvigruppe, nende ootusi ning sellest tulenevalt hinnatakse infoturbe juhtimissüsteemi juurutamise võimalusi (Aleksandrova et al., 2020; Carvalho et al., 2019). **Turbepoliitika defineerib** lähtuvalt organisatsiooni strateegilisest arengusuunast infoturbe eesmärgid, kohustused (Aleksandrova et al., 2020) ja protseduurid ning vastutuse (Singh et al., 2014). Poliitika peab olema suunatud infoturbe juhtimissüsteemi järjepidevaks parendamiseks (Carvalho et al., 2019) ja kättesaadav asutuse töötajatele ning huvipooltele (Aleksandrova et al., 2020). Poliitika kehtestamisel on ka autorite kogemusele tuginedes oluline mõista organisatsiooni toimimisloogikat ja valdkonda, kuna infoturve peab toetama asutuse toimimist soovitud riskiisu ja kaitsetaseme juures. Pingutades üle või võttes äriprotsessidest mittetulenevaid eesmärke vähendatakse organisatsiooni kui terviku võimet olla tulemuslik.

Riski hindamise faasis tuleb välja töötada riskide hindamise metoodika, mis võimaldab hinnata ohtude ja nõrkuste ilmnemise tõenäosust (Aleksandrova et al., 2020) ning defineerida riskiisu tasemed, mis võimaldaksid hallata riske tõhusalt (Singh et al., 2014). Antud faas on üks keerulisemaid etappe, kuna sellest sõltub see, kas organisatsioon suudab vältida metoodika uuesti juurutamist. Selle faasi käigus hinnatakse infovarasid, mida tuleb kaitsta nii tehnilise, keskkonna kui ka inimressursside vaatest. (Nurbojatmiko et al., 2016)

Riski halduse faasis toimub riski maandamise meetmete ja kontrollide juurutamine selleks, et vähendada riske, mis ületavad asutuse riskiisu (Aleksandrova et al., 2020) ning jääkriski haldamine ning välistuste ja kontrollide haldamine (Carvalho et al., 2019).

Kontrollmehhanismide valiku käigus valitakse, milliseid meetmeid organisatsioon juurutab selleks, et tagada soovitud turbe tase (Singh et al., 2014). See faas tugineb eelnevate etappide käigus tehtud riski hindamisele, maandamisplaanile ja varade inventuurile (Carvalho et al., 2019). **Rakendatavuse kinnitamine** on etapp, mille käigus kontrollitakse süsteemi toimivust ja vastavust kehtestatud nõuetele (Aleksandrova et al., 2020) ja hinnatakse, kas asutusel on vajadust tõsta turbepoliitika turbeootuste taset (Carvalho et al., 2019). **Mõõdikute ja turbejuhtimise valiku** käigus valitakse asutuse edaspidiseks turbehindamiseks mõõdikute ja juhtimissüsteem, mille abil on võimalik hinnata ning juhtida turbe olukorda (Aleksandrova et al., 2020). Samas jooksev infoturbe haldus on osa üldisest juhtimissüsteemist, mida juhitakse läbi 4 tsüklilise faasi – planeerimine (*Plan*), opereerimine (*Do*), ülevaatus ja monitoorimine (*Check*) ning arendamise ja parendamine (*Act*) (Carvalho et al., 2019).

DevSecOps sõltub tugevalt agiilsetest printsiipidest, milleks on iteratiivne (etapiviisiline) arendamine, pidev tagasisidestamine kliendiga, tihe suhtlus ning koostööhuvi osapoolte vahel. Teadlased ja praktikud näevad agiilseid meetodeid kui filosoofiat, koostöö ja suhtlemise võimendajat või vahendina äritegevuse paremaks muutmiseks. (Department of Defense, 2020; Zaitsev et al., 2018) Paljudel juhtudel aga keskendutakse töökorralduse juurutamisel töövahenditele ja tehnilistele aspektidele, ning organisatsiooni kultuuri muutmine jäetakse tahaplaanile. Tehnoloogiline aspekt on töökorralduse juures oluline, kuid edukaks muudatuse ellu viimiseks tuleb keskenduda eelkõige sellele, kuidas me kaasame partnereid, töötajaid ja juhtkonda, et asutus suudaks tervikuna adapteeruda teist moodi toimetamisega. (Department of Defense, 2020; Morales et al., 2020)

Kuna DevSecOps juurutamine on suuremas plaanis organisatsiooni kultuuri muudatus (Myrbakken et al., 2017), mis eeldab töötajatelt teist moodi käitumist ja ka uut tüüpi kompetentsi (Raynaud, 2017), siis on selle protsessi käigus oluline tähelepanu pöörata võtmetöötajate kompetentside arendamisele ning nende hindamisele (Ahmed et al., 2019).

Ideaalses maailmas eelistatakse muutustega tegeleda teadlikult ja plaanipäraselt selleks, et vältida juhuslikku väljundit. See võimaldab teha sihilikke tegevusi eesmärgiga rakendada organisatsiooni infoturbestrateegia. (da Veiga, 2018) Autorid nõustuvad da Veiga 2018 nägemusega, aga arvavad, et enamus juhtudest muudatused pigem juhtuvad ja tagajärgedega tegeletakse tagantjärgi. Muudatuste juhtimine on struktureeritud protsessi ja tööriistade komplekti rakendamine inimeste juhtimiseks soovitud äritulemuse saavutamisel.

Kõige levinumaks muudatuse juhtimise mudeliks on Kurt Lewini poolt loodud muudatuste mudel, mis on lihtsustatud kolme faasiline protsess, mis hõlmab lahti sulatamist, muutmist ja külmutamist. Muudatuse mudeleid ja nendega kaasnevaid muudatuse faase on erinevates teooriates kirjeldatud erinevalt, kuid enamik neist täpsustavad oma olemuselt Lewini muudatuse mudeli kolme etappi ning on antud teooria edasiarendused. (Zenab et al., 2013)

Kotter-i 8 sammuline muudatuse mudel on samuti Lewini teooria laiendus, mis keskendub muutumise teadlikkuse ja vajaduse juhtimisele. Kotteri kaheksa etappi jagunevad sarnaset Lewinile sulatamise, ülemineku tagamise ja kinnitamise etappidesse. Kotter leiab, et muudatuse edukaks läbi viimiseks peavad inimesed mõistma, et muudatus on vajalik. (Galli, 2018; Zenab et al., 2013)

McKinsey 7-S mudeli töötasid välja Tom Peters, Richard Pascale ja Robert Waterman Jr. Mudel keskendub muudatuse faasile ja käsitleb organisatsiooni muutust tänaselt positsioonilt uuele soovitud tasemele. Mudel pakub kasutajale ettevõtte strateegiliste ressursside põhise vaate ning kirjeldab ära rollid, vastutused ja vastutuse seosed. Mudelit saab edukalt kasutada organisatsiooni positsiooni analüüsimiseks läbi 7 erineva elemendi ning see suudab näidata ära erinevate dimensioonide nõrkused ja tugevused. Antud mudel sobib optimaalse organisatsiooni disainimiseks ja muudatuse juhtimiseks selles suunas ning asutuse hindamiseks. (Cox et al., 2019; Galli, 2018)

Burke-Litwin poolt loodud mudel on põhjus-tagajärg seosele ülesehitatud muudatuse mudel, mis arvestab sise- ja välisekeskkonda. Meetod paneb eelkõige paika muudatuse raamistiku, mis annab vahendid muudatuse määratlemiseks, juhtimiseks ja ka planeerimiseks. Mudel võtab arvesse erinevaid muudatust mõjutavaid tegureid. Alustades välisest keskkonnast ja lõpetades indiviidi ja organisatsiooni mõjutavate teguritega. (Burke et al., 1992; Martins et al., 2009)

Prosci poolt loodud ADKARi mudel põhineb samuti Lewini kolmel faasil ning mudeli eesmärgiks on aidata läbi viia organisatsioonis muudatusi tulemuslikult. (da Veiga, 2018; Hiatt et al., 2012) See tulemustele orienteeritud mudeli lähenemine aitab suunata tähelepanu kõige enam sellele, mis tagab õnnestumise tõenäosuse. (Galli, 2018) Mudelis on muudatuse läbiviimine jaotanud viieks faasiks - *awareness* (teadlikkus), *desire* (tahe), *knowledge* (teadmised), *ability* (võimekus) ja *reinforcement* (kinnistamine). (da Veiga, 2018)

Erinevate muudatusteooriate etapid ja lühikirjeldus on võetud kokku autorite poolt loodud Tabelis 1.

Tabel 1

Muudatuste juhtimise käsitlused teaduskirjanduses

Teooria	Etapid	Kirjeldus
Kurt Lewin	1. Sulata lahti 2. Taga üleminek 3. Käitumise kinnitamine	Muudatuste teooria eelkäija. Võtab kokku muutmise läbi kolme faasi ja üldistab suuremas vaates muutuse olemuse. Mudel keskendub eelkõige muudatusele kui protsessile.
Kotter' s 8-Step	1. Möödapääsmatuse tekkimine 2. Liidu loomine 3. Strateegilise visiooni loomine 4. Visiooni jagamine 5. Volituste jagamine töötajatele 6. Võitude saavutamine 7. Koonda kasum ja jätka muutmist 8. Kinnista saavutatused ja sea uued sihid	Keskendub muudatuse 8 faasile, peamiselt käsitleb organisatsiooni muudatust läbi strateegia ja vajaduse selgitamise läbi kaasatuse. Mudel keskendub eelkõige muudatuse protsessile ja inimeste kaasatust vaadeldakse ülevalt alla. Tähelepanuta jääb inimese isiklike oskuste parandamine.
ADKAR	1. Teadlikkuse ja tahte loomine 2. Tahe muuta 3. Teadmiste teke 4. Võimekused ja oskused 5. Saavutatu kinnistamine	Keskendub muudatuse viiele faasile, mis omakorda aitavad muudatuse läbi viia ja keskenduda inimestele. Mudel sobib töötajate tasandil muudatuse edendamiseks.
McKinsey 7-S	1. Strateegia loomine, mis loob eelduse muutuseks 2. Struktuur, mis määratleb vastutused ja toetab strateegiat 3. Süsteemid, mis toetavad strateegia elluviimist 4. Jagatud oskused, mis aitavad areneda 5. Töötajad kes aitavad arendada oskusi 6. Eestvedav stiil, mis aitab tulemusi saavutada 7. Ühised jagatud eesmärgid	Keskendub muudatuse faasile, mis aitab organisatsioonil liikuda olemasolevast positsioonist uude positsiooni. Mudel võimaldab hinnata organisatsiooni võimekusi ja sobitub organisatsiooni tasandil muudatuse juhtimiseks.
Burke and Litwin	1. Hinda väliskeskkonda, mis mõjutab organisatsiooni 2. Missiooni ja strateegia määratlemine 3. Muudatuse juhtimine 4. Kultuuri kujundamine 5. Tõhusa struktuuri määratlemine 6. Muudatuse kultuuri kujundamine 7. Kaardista oskused ja isiklikud motivaatorid 8. Väärtuste ja vajaduste sõnastamine 9. Töötajate motiveerimine	Keskendub muudatuse 9 tegurile, mis annavad muudatusele kontseptuaalse raamistiku millega hinnata organisatsiooni efektiivsust. Mudeli piiranguks on tema rakendamise keerukus.

Allikas: Almanei et al., 2018; da Veiga, 2018; Galli, 2018; Martins et al., 2009; Rosenbaum et al., 2018; Zenab et al., 2013

Kuna muudatuste juhtimine juhtkonna tasemelt, hierarhiliselt töötaja poole ei kanna endas alati edulugusid ja on ebaefektiivsed, siis soovitatakse muudatuse teooriaid liigitada vastavalt muudatuse vajadusele. Muudatuse võib esile kutsuda erinev vajadus - vajadus muuta organisatsioonikultuuri, juhtimist või tingib selle koguni infotehnoloogia areng. (Hossan, 2015)

Muudatused ebaõnnestuvad aga sageli selle pärast, et töötajad pöörduvad tagasi oma varasemate harjumuste juurde ja soovitud muudatused jäävad rakendamata. Oluline on muudatusi läbi viies jälgida protsessi selleks, et juurutada muudatus töökultuuri. (Galli, 2018) Iga muudatuste juhtimise protsess juhib tähelepanu erinevatele aspektidele ja keskenduvad juhtimisalasele ülesandele ning tahkudele, mis aitavad muudatust ellu viia (Bugubayeva et al., 2017). Igas organsatsioonis, kus muudatust planeeritakse, peavad olema selleks vahendid, mis aitavad tõhusalt läbi viia muutusi ning maandada inimesetest tulenevaid riske, kuna turvalisuse juurutamine ja infoturbe tagamisest sõltub kõige rohkem just inimesest (da Veiga, 2018).

Tuginedes artiklites toodud muudatuste juhtimise erinevatele teooriatele, analüüsisid autorid selleks viite erinevat teooriat fookuse vaatest, et mõista paremini, milline muudatuse teooria toetab kõige enam indiviidi ja keskendub muudatuse edukale elluviimisele. Prosci ADKAR-mudel (***A**warness, **D**esire, **K**nowledge, **A**bility, **R**einforcement*) on parim raamistik üksikisikute oluliste muudatuste ettevalmistamiseks, aktsepteerimiseks ja uue toimemudeli edenemiseks (Boca, 2014). Antud töös keskendume ADKAR muudatuse mudelile, kuna DevSecOps töökorralduslik muudatus puudutab peamiselt just töötaja vajadust muutuda ja teha asju oma töös teisiti ning juurutada need rutiinid oma igapäevatöösse. Lisaks on kriitiline mõista olemasolevat organisatsiooni infoturbekultuuri enne muudatuste sisseviimist. Seetõttu tuleb olemasoleva keskkonna mõistmiseks ja määramiseks läbi viia hindamine, millist käitumist tuleb muuta. Enne muutmist on seega oluline teada, milliseid konkreetseid tegevusi tuleb muudatuste elluviimiseks rakendada, et peale muutust saaks hinnata ka muudatuse edukust. (da Veiga, 2018)

Oluline on ADKAR mudeli juures jälgida seda, et iga samm viiakse lõpule enne järgmise juurde liikumist (Boca, 2014). Samuti pakub mudel võimaluse tuvastada muudatuses erinevaid barjääre, millega meeskonnaliikmed silmitsi seisavad. See aga teeb ADKARist tugeva tööriista, mis aitab organisatsioonil muutumisprotsessi toetada ja töötajatel positiivselt liikuda ühest etapist teise. ADKAR ei paku lahendust ainult organisatsiooni pidevaks täiustamiseks uuenduslike viiside kaudu, vaid pakub lahendusi barjääride

tuvastamiseks muutusprotsessi igas etapis, kui need on tekkinud mõne sobimatu või vigase juhtimisviisi abil. (Zenab et al., 2013)

Selleks, et oleks võimalik hinnata DevSecOps uuringutest kaardistatud kriitilisi edutegureid ja mõista paremini nende mõju muudatuse juurutamise etappidele, kaardistasid autorid kriitilisi edutegureid ADKAR muudatuse etappide lõikes. Selle põhjuseks on soov mõista millised edutegurid mõjutavad milliseid muudatuse etappe. Antud infole tuginedes on empiirilises magistritöö osas võimalik analüüsida muudatuse õnnestumiseks vajalikke samme ja edukaks juurutamiseks olulisemaid kriitilisi edutegureid, millele tuleb esmajärjekorras keskenduda. Kuna kriitiliste edutegurite puhul käsitleti turbe teadmisi eelkõige võimekuse võtmes, siis otsustasid autorid liigitada turbe teadmised võimekuse alla. Kokkuvõttes on võimalik läbi töötatud kirjanduse põhjal välja tuua 12 kriitilist edutegurit (vt. Tabel 2).

Tabel 2

Kriitilised edutegurid DevSecOps juurutamisel

	ADKAR	Edutegur	Kirjeldus
A	Muudatuse vajaduse selgitamine	Suhtlusele orienteeritus	Töötajad on suhtlemisele orienteeritud, mis on eduka koostöö eelduseks ja tagab info liikumise
		Koostööle orienteeritus	Töötajad on koostööle orienteeritud, mis tagab äritulemusele orienteeritus
		Tagasi-sidestamine	Töötajate vahel toimub tagasisidestamine, mis võimaldab organisatsioonil areneda
		Vastutuse võtmine	Töötajad võtavad vastutust ja näevad äritulemusteni jõudmist ning ka turvalisust enda vastutusena
D	Muudatuse soovi tekitamine	Parendustele orienteeritus	Töötajad on parendustele orienteeritud. Toetab organisatsiooni õppimist ja pidevat arengut
K	Toetamine teadmistega	Teadmiste jagamine	Töötajate vaheline teadmiste jagamine võimaldab organisatsioonil kiiremini edasi areneda
A	Oskuste ja teadmiste tugevdamine	Läbipaistvus	Tiimide vaheline läbipaistvus, mis toetab koostööd.
		Turbe teadmised	Turbe teadmiste olemasolu tiimides loob võimaluse juurutada turvet arenduse käigus ja väldib hilisemaid muudatusi
R	Tunnustamine ja töökorralduse kinnistamine	Arendusprotsessi automatiseerimine	Tarkvara ehitamise, juurutamise ja testimise automatiseerimine tagab arendusprotsessi kiiruse
		Ärimõõdikud	Äriväärtust peegeldavate mõõdikute juurutamine tagab läbipaistvuse kuidas asutusel läheb ja aitab leida parenduse kohti
		Turbemõõdikud	Turbe ohtude ja nõrkuste mõõtmine terves arendusprotsessis tagab organisatsioonile võimaluse avastada probleemid varakult
		Turbe automatiseerimine	Turbe teenuste automatiseeritus võimaldab juurutada turbetestimise arendusprotsessi

Allikas: Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; McCartney et al., 2019; Moore et al., 2018; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017; Wagner et al., 2020

Edutegurid on suures plaanis organisatsiooni kultuuri, töötajate teadmisi ja töövahendeid mõjutavad. Vaadeldes neid ADKAR-i muudatuse mudeli põhjal on näha, et

edutegurid on muudatuse juurutamise protsessi vaates jagunenud üle erinevate etappide. Arvestades ADKAR-i mudeli eripära on oluline, et nendele eduteguritele pööratakse tähelepanu DevSecOps töökorralduse juurutamisel organisatsioonis. Selleks, et kaardistada DevSecOps töökorralduse juurutamise eripärasid avalikus sektoris, uurivad autorid järgmises peatükis antud töökorralduse juurutamist avalikus sektoris ja kõrgelt reguleeritud valdkondades ning otsivad täiendavaid nüansse, mida tuleb lisaks juba kaardistatud kriitilistele eduteguritele veel arvesse võtta.

1.3.DevSecOps töökorralduse juurutamise võimalused avalikus sektoris

DevSecOps töökorralduse eripärade uurimiseks töötasid autorid läbi teaduskirjandust, et leida täiendavaid asjaolusid, mis iseloomustavad avalikus sektoris või kõrgelt reguleeritud keskkonnas agiilse arenduse rakendamist. Artiklite otsingute käigus kasutasid autorid märksõnadena erinevaid kombinatsioone järgnevatest sõnadest „*regulated, government, public sector, security, agile, devops, devsecops, system of system, development*“. Otsingute käigus leidus eelkõige artikleid, mis käsitlesid militaar-, lennunduse või meditsiini valdkonnas agiilse töökorralduse juurutamise uurimist. Samas oli uuringuid teostatud ka tööstus-, energeetika- ja finantssektoris (vt. Tabel 3). Enamikku neist artiklitest iseloomustab uuritava valdkonna kõrgelt reguleeritud iseloom, mis seab täiendavaid piiranguid või nõudeid, mida tuleb töökorraldust rakendades täita. Artiklite ühine joon on see, et agiilse töökorralduse juurutamisest nähakse positiivseid aspekte, mis võimaldab üldist organisatsiooni tulemuslikkust parendada. Reguleeritud valdkondi iseloomustab vajadus adresseerida erinevaid kriitilisuse aspekte, vaadates nii turvalisust kui ka infoturbe kriitilisust. Reguleeritud keskkondadel on vajadus vastata formaalsetele standarditele, regulatsioonidele, direktiividele ja juhenditele (Fitzgerald et al., 2013).

Turvalisuse vaatest kriitilised süsteemid on need, mille rike võib põhjustada inimelude kaotust, tõsist varalist kahju või keskkonnakahju. Näideteks sellistest süsteemidest on tuumasüsteemid, meditsiiniseadmed, lennundus, raudtee juhtsüsteemid ja autode kontrollsüsteemid. Tänu füüsilistele riskidele piiratakse üldjuhul turbekriitiliste süsteemide arendamist vastava valdkonna üldise või spetsiifilise standardiga või regulatsioonidega. (Islam et al., 2020) Eestis reguleerib kriitilisi valdkondi Hädaolukorra seadus, mis loetleb 13 elutähtsat teenust (Vabariigi Valitsus, 2017), millele laienevad täiendavad turvalisuse tagamise kohustused tulenevalt Küberturvalisuse seadusest (Vabariigi Valitsus, 2018b). Samas on Euroopa Liit valmistamas ette *Security of Network and Information Systems* (NIS) direktiivi muudatust, millega laiendatakse küberturvalisuse reeglite juurutamise kohustust lisaks tänasetele elutähtsatele teenustele ja digitaalse teenuse osutajatele edaspidi ka teistesse

sektoritesse. Seda eelkõige tuginedes teenuse olulisusele. Läbi selle rakendub meetmete juurutamise kohustus edaspidi sektoritesse, kes täna on jäänud skoobist välja. (European Comission, 2020)

Uuritud artiklites tuuakse regulatoorsete piirangutena välja vastuolulised turbenõuded, intellektuaalse omandi kaitse nõuded, avatud suhtlemist ja koostööd ning kasutajate tagasisidet. Samuti on murekohaks keskkondade nähtavus ja turvalisus. Eriti sisseehitatud süsteemide puhul, kus on keeruline teostada kontrolle keeruliste funktsionaaluste puhul. Lisaks on organisatsioonidel vaja arvestada riistvara sõltuvuse ja piiratud nähtavusega lõppkasutaja süsteemides, kust ei pruugi olla võimalik saada kasutusega seotud informatsiooni. (Lie et al., 2020)

Samuti on olukordi, kus tellija/partner dikteerib arendusmeetodi kasutamise ning piirab agiilse tarkvara arenduse kasutamise võimalusi. Seda eelkõige tulenevalt vajadusest omada selget skoopi ja funktsionaalsuste nimekirja kohe projekti alguses (Islam et al., 2020), mis läheb suuresti vastuollu agiilsete printsiipidega, kus eesmärk on koostöös tellijaga prioriseerida inkrementaalseid arendusülesandeid jooksvalt protsessi käigus (Morales et al., 2020).

Reguleeritud valdkondadele kohalduvad erinevad nõuded, mis sätestavad nii dokumenteerimist, testimist kui ka muid arendusetappe. Meditsiinivaldkonda iseloomustab eelkõige kasutusvaldkonnast tulenev kriitilisus, kus regulatsioonidega üritatakse tagada hilisemas kasutuses tarbijate tervis. DevSecOps töökorralduse vaatest tähendab see eelkõige piiranguid testimises ja dokumenteerimises ning tehnilisele realisatsioonile seatud tingimustes. (Fitzgerald et al., 2013; Heeager et al., 2020; Laukkarinen et al., 2018, 2017)

Lennunduses reguleeritakse toimimist rangete standarditega. Sarnaselt teistele valdkondadele on ka siin asutud reguleerima lisaks muudele aspektidele infoturvet ja selle rakendamist. Samuti on antud valdkonnas selgelt reguleeritud tarkvara elutsükkel ning on kehtestatud erinevad nõuded, alustades testimisest ja lõpetades kohustusliku sertifitseerimisega. Samas on teaduskirjandusest leitav, et agiilset arendust on võimalik ka selles sektoris edukalt juurutada. (Islam et al., 2020; Johnson et al., 2020)

Militaarvaldkonda reguleerivad erinevad piirangud. Tarkvaraarenduse vaatest mõjutavad DevSecOps ja agiilset tarkvaraarendust eelkõige regulatsioonidest tulenevad nõuded ja tehnilised piirangud. Nendeks võivad olla nii dokumenteerimist puudutavad nõuded kui ka tehnilised piirangud, mida tuleb lahendust arendades silmas pidada. Lisaks on militaarvaldkonnas teatud süsteemidel info jagamisele kehtivad piirangud, mis pärsivad agiilse arenduse juurutamise võimalusi. Samas ei piira need täiendavad asjaolud otseselt

kasutatavaid arendusmetoodikaid või tehnikaid. (Department of Defense, 2020; Messina et al., 2016; Wagner et al., 2020)

Finantssektorit ja notari valdkonda puudutavate uuringute puhul oli näha regulatsioonidest tulenevaid piiranguid, kuid muid täiendavaid piiravaid faktoreid artiklitest välja ei tulnud (Caraturan et al., 2019; Sousa et al., 2020). Tööstus- ja haridusvaldkonda puudutavates teadusartiklites valdkonnast tulenevaid piiravaid faktoreid või tehnilisi piiranguid välja ei toodud (Hasselbring et al., 2019; Zaheeruddin et al., 2019). Samas on tööstuse enda tegutsemisvaldkonnast tulenevalt võimalik täiendavate regulatsioonide olemasolu ja antud allikate pealt ei saa väita, et neid sektoreid tervikuna valdkonnapõhised regulatsioonid ei piira.

Avaliku sektori puhul tõi kirjandus välja sõltuvuse erinevatest regulatsioonidest ja tehnilistest piirangutest. Samas ei käsitletud nende juures info jagamisele kehtivaid piiranguid. Eelkõige tulenesid regulatsioonid ja tehnilised piirangud vastava riigi seadusandlusest ning kohustusest olla kooskõlas ISO erinevate nõuetega. Samas ei nähtud otsest piirangut, mis takistaks agiilsete arenduspraktikate juurutamist. (Rindell et al., 2016) Sarnaselt avalikule sektorile on energeetika valdkond ka selline, kus kehtivad erinevad regulatsioonid ja tehnilised piirangud. Seda eelkõige tulenevalt kõrgetest ootustest töökindlusele ja kvaliteedile. (Lewerentz et al., 2019)

Läbi töötatud teadusartiklite põhjal koostasid autorid Tabeli 3, mis võtab kokku erinevates valdkondades tehtud agiilse ja DevSecOps töökorralduse kasutamise uuringud ning nendest tulenevad piiravad faktorid.

Tabel 3

Erinevates valdkondades Agiilse ja DevSecOps töökorralduse kasutamise uuringud

Valdkond	**DevSecOps-i mõjutavad kriitilised piirangud**		
	Täiendavad regulatsioonid	Tehnilised piirangud	Info piirangud
Meditsiin	X	X	
Lennundus	X	X	
Militaar	X	X	X
Finants	X		
Notar	X		
Tööstus			
Haridus			
Avalik sektor	X	X	
Energeetika	X	X	

Allikad: Caraturan et al., 2019; Department of Defense, 2020; Fitzgerald et al., 2013; Hasselbring et al., 2019; Heeager et al., 2020; Islam et al., 2020; Johnson et al., 2020; Laukkarinen et al., 2018, 2017; Lewerentz et al., 2019; Lie et al., 2020; Messina et al., 2016; Rindell et al., 2016; Wagner et al., 2020

Eesti avaliku sektori infosüsteemidele ja nende arendamisele rakenduvad samuti erinevad regulatsioonid. Ühest küljest reguleerib valdkonda Infosüsteemide turvameetmete süsteemi määrus, mis kohustab rakendama kolmeastmelist etalonturbe süsteemi (ISKE) või tagama, et rakendatud meetmed on kooskõlas ISO/IEC 27001 kehtestatud nõuetega. (Vabariigi Valitsus, 2020a) Sõltuvalt valdkonnast võivad kohalduda lisaks nendele nõutele veel ka spetsiifilisemad nõuded. Näiteks audentimislahendustele kohaldub Euroopa Parlamendi ja Nõukogu määrus 910/2014, mis reguleerib e-identimise ja e-tehingute jaoks vajalike usaldusteenuseid Euroopa siseturul (Euroopa parlament ja nõukogu, 2014). Määruse rakendamist Eestis täpsustab Riigi Infosüsteemide Ameti (RIA) poolt loodud Eesti Vabariigi Infosüsteemis Audentimislahendustele kehtivad nõuded, mis sätestab arhitektuursed nõuded, tehnilised piirangud, mittefunktsionaalsed nõuded, soovitused tagatistasemete rakendamiseks ja ISKE kohaldamise piirid (RIA, 2017). Eestis kehtestatud regulatsioonid, juhendid ja standardid otseselt arendusmeetodite valikut ei dikteeri. Pigem sätestavad nad täiendavad nõuded, mida tuleb arvestada aga seda kuidas tulemini jõutakse ei piirata.

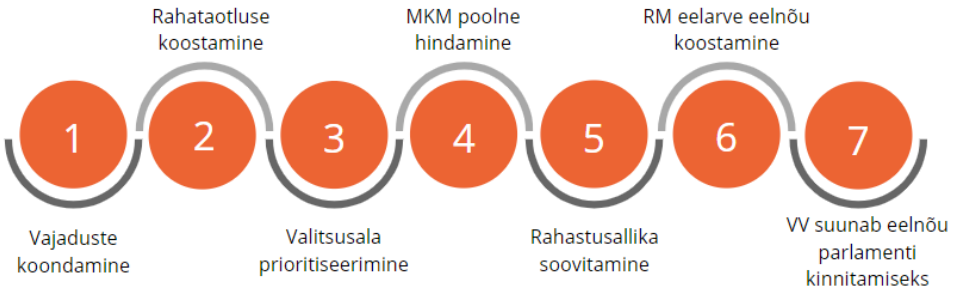
Avalikus sektoris jaguneb infoturbe vaatest informatsioon sensitiivsusest tulenevalt erinevatesse kategooriatesse. Nendeks on tavapärane avalikuks kasutamiseks mõeldud teave ja piiratud juurdepääsuga teave, mis on asutuses kasutamiseks mõeldud informatsioon, mis võib teatud juhtudel olla kogumina ka riigisaladuseks klassifitseeritud informatsioon. (Sorainen, 2016) Kui vaadelda süsteeme ja infot, mida võib avalikult kasutada, siis need süsteemid ei erine tavapärastest erasektoris olevatest süsteemidest, millest johtuvalt ei ole nendel süsteemidel tehnilisest vaatest ühtegi täiendavat piirangut töökorraldusele kuidas neid hallatakse ja arendatakse.

Kui vaadelda asutusesiseseks kasutuseks mõeldud infot ja süsteeme, kus neid töödeldakse, või ka süsteeme, kus käsitletakse salastatud infot, siis nende eripäraks on kõrgendatud turvalisuse nõuded (RIA, 2016; Vabariigi Valitsus, 2020a). Agiilsus piiratud süsteemidega töötamisel eeldab teatud agiilsete põhimõtete kohandamist. Kõige suuremaks väljakutseks on tellija ootuste muutus, kuna turbeaspekt vajab süsteemset läbimõtlemist ja planeerimist. Samuti eeldab kõrgendatud turve põhjalikku testimist, mis hakkab piirama kiiret tarkvara tarnet ja tihedasti toimivat versiooni uuendamist juhul, kui tarkvara turbetestimine ei ole liidetud tarkvaraarendusprotsessi automaatsel kujul. Lisaks sellele ei piisa ainult töötavast tarkvarast kasutaja vaatest, vaid oluline on ka kvaliteet turbe seisukohast. Klassikaliselt defineeritakse agiilse lähenemise puhul kvaliteet lõppkasutaja vaatest, aga see ei ole piirangutega süsteemis piisav. (Department of Defense, 2020; Morales et al., 2020)

Piiratud ligipääsuga süsteeme iseloomustab tavaliselt see, et nad on lisaks eelnevale ka veel “õhu vahega” füüsiliselt isoleeritud ja omavad kõrgendatud turbenõudeid ning nende puhul on kasutusel rollide segregatsioon, mis tagab selle, et töötajad ei saa arutada teatud teemasid väljaspool piiratud alasid ning nad ei saa teatud materjali ja vahendeid viia ruumist välja. (Morales et al., 2020) Eestis reguleerib lisaks eelpool mainitud regulatsioonidele riigisaladust puudutavaid süsteeme Riigisaladuse ja salastatud välisteabe kaitse kord, millega tuleb arvestada süsteemide puhul, mis töötlevad vastavat teavet (Vabariigi Valitsus, 2019).

Piiratud süsteemide iseloom mõjutab DevSecOps põhimõtete juurutamist läbi selle, et töötajate vaheline koostöö on piiratud, kuna isikute turbeload on erinevad, ehk nad saavad „näha“ ainult teatud asju. Lisaks ei pruugi kõik tööriistad olla kasutatavad või lubatud terve süsteemi ulatuses. Samuti ei pruugi olla võimalik kasutada infrastruktuur kui kood lähenemist, kuna süsteemi ligipääs on piiratud. Parimad praktikad koodi turvalisuse tagamiseks arenduse käigus on DevSecOps puhul samad nagu ka DevOps puhul. Turbe taseme määrab see millises ulatuses on tagatud automaattestide ja valideerimisega koodi testimine. (Morales et al., 2020)

Lisaks tehnilistele piirangutele on täiendav mõõde avaliku sektori juures ka finantseerimismudelist tulenevad piirangud. Rahastusprotsess on riigis korraldatud läbi Riigi Eelarve Strateegia (RES) protsessi. Kuna erinevad ministeeriumid kandideerivad suures plaanis sama raha nimel, siis suunatakse võimalusel investeeringu projekte ja rahastustaotlusi välisrahastusele. IT rahastuse puhul koondavad asutused vajadused kokku ja formuleerivad taotluse. Need omakorda suunatakse ministeeriumi prioriseerimiseks ning sealt liiguvad taotlused Majandus- ja Kommunikatsiooni ministeeriumisse (MKM), kus toimub rahastussoovi tehniline valideerimine ja rahastusallika soovitamine. Kui taotlus saab heakskiidu, siis suunatakse see MKM poolt Rahandusministeeriumisse (RM) eelarve eelnõu koostamisele sisendiks ning sealt edasi kinnitamiseks valitsuse kaudu parlamenti. (Riigikontroll, 2019)



Joonis 5. Avaliku sektori IT Rahastusprotsess

Allikas: Autorite loodud

Olukord, kus rahastusallikas dikteerib erinevaid rakenduvaid nõudeid tähendab aga automaatselt seda, et rahastusmudel hakkab mängima asutuse jaoks olulist rolli, kuna riigi eelarve puhul on asutustel paindlikkust rohkem, kui välisrahastuse kaudu finantseeritavate projektide puhul. Seega on rahastusmudel üks faktoritest, mis dikteerib arendusmeetodi valikut. Euroopa Liidu fondidest arenduse rahastamisel eeldatakse üldjuhul fikseeritud lõpptähtaega ja kindlaksmääratud lõpptulemit. (Viira et al., 2019) Riigikontrolli poolt 2019 avaldatud auditis „Avaliku sektori tarkvaraarenduse projektide juhtimine“ esitati soovitus Majandus- ja Kommunikatsiooniministeeriumile (MKM) täpsustada piiranguid, kuna auditeeritud näidete puhul selgus, et agiilne arendus ei sobitunud fondide rahastusmudeliga. Sellegipoolest jäi MKM endale kindlaks ja vastuolu ei tuvastanud. Kui vaadata erinevaid välisabi ja fondide rahastustingimusi, siis otseselt arendusmeetodit nad ette ei dikteeri, aga seal eeldatakse projektilt rahastuse otsuseks selget väljundit ja tulemit (Vabariigi Valitsus, 2018a) ning projekt tuleb ellu viia ettenähtud tingimustel ja ajaks (Vabariigi Valitsus, 2020b). Samas DevSecOps sõltub tugevalt agiilsetest printsiipidest (Department of Defense, 2020), mis tähendab, et fikseeritud skoobi asemel prioriseeritakse muutuvaid vajadusi jooksvalt koos tellijaga (Morales et al., 2020). Sellest võib järeldada, et rahastusmudeli valik võib osutuda piiravaks faktoriks DevSecOps edukal juurutamisel ja seda tuleb eraldi arvestada.

Läbi töötatud materjalide põhjal koostasid autorid Tabeli 4, mis võtab kokku avaliku sektori asutusele kohalduvad DevSecOpsi mõjutavad piirangud.

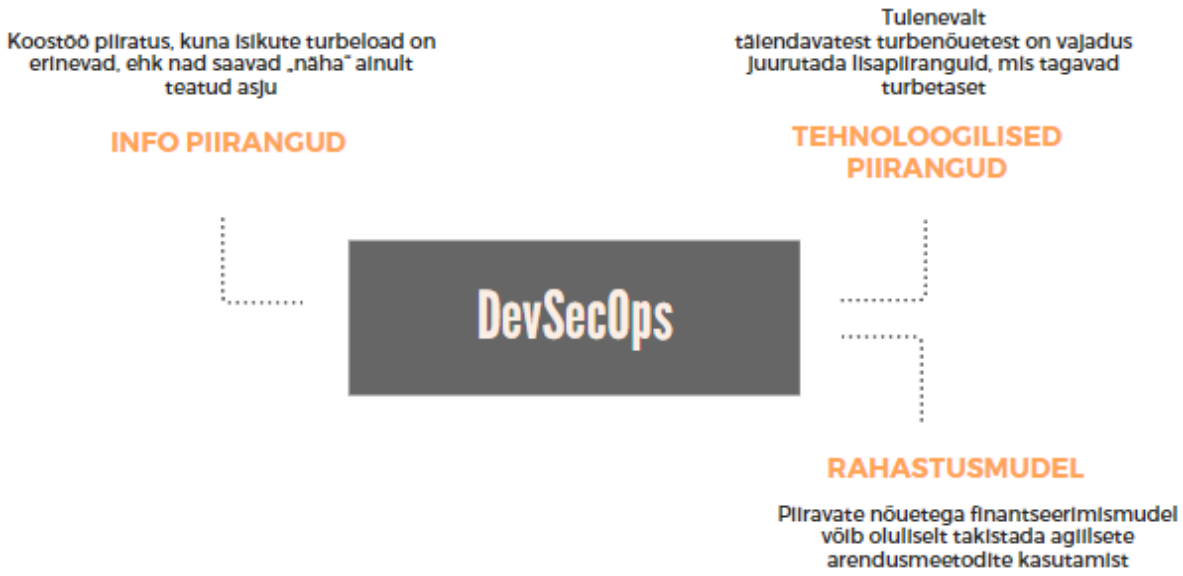
Tabel 4

IT teenuseid osutavale avaliku sektori asutusele Eestis kohalduvad DevSecOps-i mõjutavad piirangud

Täiendavad regulatsioonid	Tehnilised piirangud	Info piirangud	Rahastus
Infosüsteemide turvameetmete süsteem (ISO27001/ISKE)	Riigisaladuse ja salastatud välisteabe kaitse kord	Andmekaitse direktiiv ja Isikuandmete kaitse seadusest	Perioodi 2014-2020 struktuuritoetuse seadus
Küberturvalisuse seadus	Arvutite ja kohtvõrkude kaitse nõuded	Avaliku teabeseadus	Avalike teenuste pakkumise arendamiseks toetuse andmise tingimused ja kord
Eesti Vabariigi infosüsteemis autentimislahendustele kehtivad nõuded	Infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE rakendusjuhend	Riigisaladuse ja salastatud välisteabe seadus	
	Riigi infosüsteemi koosvõime raamistik		
	Riigi IT arhitektuur		

Allikad: MKM, 2007, 2011; RIA, 2016, 2017; Sorainen, 2016; Vabariigi Valitsus, 2018a, 2018b, 2019, 2020a, 2020b

Eelpool toodud teaduskirjanduse ja erinevate uuringute tulemusena kerkisid esile lisaks eelmises peatükis kirjeldatud kriitilistele eduteguritele kolm piiravat faktorit, mis takistavad DevSecOps edukat juurutamist. Täiendavad regulatsioonid otsustasid autorid koondada kolme alles jääva faktori osaks, kuna regulatsioonid sätestavad tehnilised piirangud, info jagamisele kehtivad piirangud ja ka rahastust puudutavad täiendavad piirangud. Ehk eraldi täiendavate regulatsioonide uurimine ei ole otstarbekas. Need leitud kolm täiendavad piiravat faktorit on toodud välja joonisel 6.



Joonis 6. Täiendavad piiravad tegurid DevSecOps juurutamisel
Allikas: Autorite loodud

Avaliku sektori asutustele laienevad mitmed erinevad nõuded ja regulatsioonid ning auditeerimiskohustused. Seda nii mujal maailmas kui ka Eestis. Samas autorite arvates ei piira regulatsioonid uuringutele tuginedes arendusmeetodi valikut. Avalikus sektoris DevSecOps töökorralduse juurutamist mõjutavad lisaks peatükis 1.2 kirjeldatud eduteguritele täiendavad piiravad faktorid (vt. Joonis 6). Nendeks on täiendavad tehnoloogiliste piirangute juurutamise vajadus, info piiratuse tagamise vajadus ja rahastusmudel. See tähendab, et lisaks eduteguritele on oluline arvestada ka nende piiravate faktoritega, kui avalikus sektoris asutakse antud töökorraldust juurutama. Järgmises peatükis uurivad autorid DevSecOpsi töökorralduse juurutamise võimalusi avalikus sektoris SMIT näitel.

2. DevSecOps töökorraldus SMIT näitel

2.1. Uurimisprotsessi ja SMIT tutvustus

SMIT on Siseministeeriumi hallatav IT teenuseid pakkuv riigiasutus. SMIT alustas tegevust 1. märtsil 2008 eesmärgiga osutada Siseministeeriumile ja selle haldusalale info- ja kommunikatsioonitehnoloogia (IKT) teenuseid. 11 töötajaga tööd alustanud asutus on tänaseks kasvanud pea 350 töötajani ja laienenud üle Eesti. (PWC, 2020; SMIT, 2021) Asutuse teenuste portfellis on hetkel 130 aktiivset teenust, millest 28 on haldusala vaatest kriitilised ja 47 olulised. Teenused ja vastutus nende nõuetekohase toimimise ning arendamise eest on jagatud kahe erineva struktuuriüksuse vahel - Äriteenused ja Baasteenused. SMIT-i põhimissioon on pakkuda oma klientidele tarku ja turvalisi tehnoloogilisi lahendusi olles sisejulgeoleku innovatsiooni- ja IKT kompetentsikeskus. (SMIT, 2021; Vabariigi Valitsus, 2020c)

SMIT juhtide ja töötajate taustad on erinevad - osa neist tuleb 10 töötajaga ettevõttest, osa 1500 töötajaga organisatsioonidest. Vajadus on leida võimalusi, et ühtlustada oskusi, teadmisi ja arusaamu tervikuna. SMIT-s on uusi juhte (nii juhtimiskogemuse kui ka organisatsiooni mõttes) viimastel aastatel lisandunud väga palju. Asutuse võimekused ja hoiakud ühiste juhtimispõhimõtete ja arusaamade osas vajavad kindlasti arendamist. Valitsemisala juhtimispõhimõtete uuring 2018. lõpus andis selleks ühe sisendi ning sisemine rahuloluküsitlus 2019. ja 2020. aasta alguses avas teemat juhtkonna jaoks ja olukord ei ole sugugi nii hea, kui esmapilgul paistab. (Siseministeerium, 2018; SMIT, 2020b)

SMIT on võtnud eesmärgiks, et neil oleks ennast tundvad ja arengule suunatud töötajad ja elluviimisele suunatud juhtimine (kirjeldatud SMIT eesmärkidena inimeste fookuses 2020) ning sellest tulenevalt on soov SMIT juhte nimetatud teemades toetada ja arendada. (SMIT, 2020a)

Töökorralduslikult on SMIT alates 2018. aastast asutuses tehtavaid arendus- ja haldustegevusi korraldanud tuginedes DevOps töökorraldusele (PWC, 2018). Selline lähenemine on aidanud oluliselt parendada äriteenuste halduse ja arenduse vahelist koostööd, samas on see töökorraldus koos agiilse arendusega tekitanud uue kitsaskoha, milleks on koostöö Arenduse DevOps tiimide ja Infoturbe tiimi vahel. Seda olukorda ilmestavad töötajate rahulolu-uuringute tagasiside, mille tulemused näitavad selgelt probleemkohti koostöös teiste tiimidega, samas kui koostöö oma tiimi sees on väga hea. (SMIT, 2020b)

Tulenevalt 1. peatükis toodud kirjanduse analüüsist arvavad autorid, et tänase organisatsiooni kitsaskohtade üheks võimalikuks lahenduseks võiks olla DevSecOps töökorralduse juurutamine. Selleks, et veenduda antud töökorralduse sobivuses SMIT-i,

otsustasid autorid uurida teooriast leitud edutegurite esinemist organisatsioonis. Uurimismeetodina otsustasid autorid kasutada kombineeritud lähenemist ühendades kvantitatiivse ja kvalitatiivse lähenemise. Magistritöö peamine uurimismeetod on küsitlus ja intervjuude roll on selgitada, anda küsitluse tulemustele selgitusjõudu ja sügavust. Organisatsiooni küpsustaseme hindamiseks kavandati kasutada kvantitatiivset uurimismeetodit. Selle valiku põhjuseks oli asjaolu, et sooviti saada spetsialistide vaade olukorrale, mis võimaldaks hinnata erinevate edutegurite seisundit spetsialistide tasandilt ning anda hinnang muudatuse võimalikule edukusele. Valimisse planeeriti DevOps tiimide liikmed ja infoturbe osakonna töötajad. Üldkogumi suuruseks oli 179 töötajat kokku kahe valdkonna 8-st osakonnast (vt. Tabel 5). Täiendavalt otsustasid autorid kasutada kvalitatiivset intervjuud, mis valiti selleks, et oleks võimalik võrrelda kvantitatiivsest uuringu tulemusi ja teooriast leitud edutegurite esinemist asutuses juhtide nägemusega. Kvalitatiivse intervjuu kasuks otsustati osakonna juhtide puhul selleks, et anda vestluse käigus intervjueeritavatele ning intervjueerijatele paindlikkus ning võimalus selgitada vastuste tausta või selgitada täiendavalt küsimusi. Intervjueeritavate valimiks plaaniti autorite poolt võtta SMIT DevOps tiimide juhid ja infoturbe tiimi juht. Valimi suuruseks kavandati 8 juhti.

Tabel 5

Küsimustikule vastajad

	Üldkogum	**Vastajaid**	**Vastamise %**
Veebiteenuste osakond	14	10	71,4%
Sisuteenuste osakond	16	15	93,8%
Rahvastikuteenuste osakond	27	8	29,6%
Piiriteenuste osakond	29	13	44,8%
Pääste- ja hädaabiteenuste osakond	22	15	68,2%
Menetlusteenuste osakond	22	13	59,1%
Identiteediteenuste osakond	41	21	51,2%
Infoturbeosakond	8	7	87,5%
Kokku	179	102	56,9%

Allikas: Autorite loodud

Poolstruktureeritud intervjuude (vt. Lisa A) ja kvantitatiivse küsimustiku (vt. Lisa B) koostamisel lähtusid autorid teoreetilise osa käigus leitud eduteguritest ja piiravatest faktoritest ning muudatuse protsessist tulenevatest etappidest (vt. Tabel 2 ja Joonis 5). Lisaks sellele täiendati küsimustikke tausta avavate küsimustega küsimustiku alguses ning jäeti võimalus autoritele küsida vajadusel poolstruktureeritud intervjuude käigus täiendavaid küsimusi. Kokku planeeriti poolstruktureeritud intervjuude läbiviimiseks 30 sisu avavat küsimust, 5 sissejuhatavat tausta avavat küsimust ja 1 kokkuvõttev küsimus (vt. Tabel 6).

Kvantitatiivse uuringu läbiviimiseks koostati 27 edutegurite olemasolu kaardistavat küsimust ja 6 üldisemat küsimust. Üldiste tausta avavate küsimuste eesmärk on analüüsi käigus vaadelda võimalikke seoseid edutegurite ja töötamise aja, ameti, osakonna ning töötaja rahulolu indeksi vahel. Töötaja rahulolu indeks võeti uuringusse sisse, kuna kriitilistest eduteguritest mitmed on seotud töötajate vahelise suhtluse ja koostööga, ning töötajate rahulolu indeks võib näidata täiendavat dimensiooni töökorralduse juurutamise uuringus. Küsimustiku edutegureid uurivate küsimuste koostamisel lähtusid autorid eeldusest, et töötajate enesehinnangu ja kolleegide hinnangu vahel võivad olla suured erinevused ja vältimaks olukorda, kus enesehinnang võib varjutada tegelikku olukorda otsustati tekitada juurde ka kolleegide kohta käivad küsimused, et oleks võimalik võrrelda enesehinnangut ja kolleegide nägemust.

Tabel 6

Küsimustiku ja intervjuu plaan

ADKAR	**Kriitiline Edutegur/Piirav faktor**	**Küsimused**	
-		Küsitlus	Intervjuu
-	Sissejuhatavad küsimused	1.1-1.6	1.1-1.5
A	Suhtlusele orienteeritus	2.1-2.4	2.1-2.2
	Koostööle orienteeritus	3.1-3.2	3.1-3.3
	Tagasisidestamine	4.1-4.2	4.1-4.2
	Vastutuse võtmine	5.1-5.6	5.1-5.3
D	Parendustele orienteeritus	6.1-6.2	6.1-6.3
K	Teadmiste jagamine	7.1-7.2	7.1-7.2
A	Läbipaistvus	8.1-8.2	8.1-8.2
	Turbe teadmised	9.1-9.2	9.1-9.2
R	Arendusprotsessi automatiseerimine	10.1	10.1-10.3
	Ärimõõdikud	11.1	11.1-11.2
	Turbemõõdikud	12.1-12.2	12.1-12.2
	Turbe automatiseerimine	13.1	13.1
-	Täiendavate tehnoloogiliste piirangute juurutamise vajadus	-	14.1
	Info piiratuse tagamise vajadus	-	15.1
	Rahastusmudel	-	16.1
	Intervjuu lõpetamine	-	17.1

Allikas: Autorite loodud

Kvantitatiivse uuringu küsimuste koostamiseks kasutasid autorid kohandatud Likerti 5 palli skaalat vastuste variantidega: „täiesti nõus“ - 4, „pigem nõus“ - 3, „pigem ei ole nõus“ - 2, „ei ole nõus“ - 1, „ei oska hinnata“ - 0. Küsimuste valideerimiseks kasutasid autorid 5

erinevat mitte IT-ga seotud isikut, kellel lasti tutvuda küsimustega ja paluti reflekteerida, kuidas nad küsimusi tõlgendasid. Kasutajate tagasiside põhjal parendati küsimuste sõnastust. Lisaks kasutati samu isikuid ka kaaskirja sõnastuse parendamiseks. Küsimustiku läbiviimiseks valiti SurveyMonkey keskkond, kuhu autorid ehitasid üles küsimustiku. Uuringul osalemise kutse saadeti autorite poolt välja ühise pöördumisega e-kirja teel. Uuring avati kasutajatele 18.02.2021 ja suleti 16.03.2021. Kokku oli küsimustik valimile avatud 27 päeva. Uuringu käigus saadeti täiendavalt 3 meeldetuletust, mille järel kasvas hüppeliselt vastajate aktiivsus. Üldkogumi aktiivsus oli 56,9%, ehk kokku vastas osakondade 179 töötajast 102.

Intervjuude läbiviimiseks planeeriti kohtumised asutuse uuritavate valdkondade osakonna juhtidega. Igaks kohtumiseks broneeriti 1,5h koos võimalusega liituda intervjuuga üle Skype for Business keskkonna. Kuna intervjuude hetkeks oli asutusest lahkunud Infoturbeosakonna juhi ametikohal töötav juht, siis antud juhiga vestlust läbi ei viidud. Samuti otsustati juhi kohusetäitjaga mitte intervjuud teha, kuna selles rollis oli sellel ajahetkel üks töö autoritest.

Tabel 7

Intervjueeritavate valim ja intervjuu toimumise info

Intervjueeritava nimi, ametikoht	**Kuupäev, kanal, kestus**
Juht A, osakonna juhataja	01.03.2021, Skype for Business, 59 min
Juht B, osakonna juhataja	03.03.2021, füüsiline kohtumine, 61 min
Juht C, osakonna juhataja	04.03.2021, Skype for Business, 40 min
Juht D, osakonna juhataja	08.03.2021, Skype for Business, 75 min
Juht E, osakonna juhataja	11.03.2021, Skype for Business, 71 min
Juht F, osakonna juhataja	11.03.2021, Skype for Business, 49 min
Juht G, osakonna juhataja	15.03.2021, Skype for Business, 67 min

Allikas: Autorite loodud

Intervjuude läbiviimise perioodiks oli 01.03.2021 kuni 15.03.2021. Seoses Covidist tingitud olukorraga toimusid 7-st intervjuust 6 üle Skype for Business keskkonna. Ühe juhiga teostati vestlus füüsiliselt. Kõige lühem intervjuu oli 40 minutit ja kõige pikem 75 minutit. Kokku kestsid intervjuud 7 tundi ja 2 minutit. Kõik intervjuud dokumenteeriti märkmete tegemisega intervjuu käigus. Täiendava kokkuleppe alusel intervjueeritavatega intervjuud ka salvestati (vt. Tabel 7).

Analüüsi ettevalmistusfaasis teostasid autorid esimese sammuna vastuskategooria „Ei oska hinnata“ defineerimise puuduvateks väärtusteks, kuna vastasel juhul need tulemused

moonutaksid oluliselt tulemuste analüüsi. Järgmiseks kodeeriti ära ametikohad ja osakonnad tekitamaks valimid, mis võimaldaksid uurida tulemusi osakondade gruppide ja tööpere gruppide lõikes ning tekitaksid andmetesse selgema struktuuri. Osakondade lõikes tekitati 5 gruppi, mis on toodud tabelis 6 ja tööperede lõikes tekitati 3 tööpere gruppi. Gruppide loomisel üritasid autorid koondada sarnaseid osakondi ja rolle. Seda selleks, et oleks võimalik järgmises faasis analüüsida kirjanduse ülevaatest leitud kriitilisi edutegureid ja uurida, kas ja kuidas mõjutab töötajate roll või tiimide erinev vastutusvaldkond vastavaid tegureid.

Osakondade lõikes jätsid autorid Infoturbeosakonna eraldi gruppi, kuna selle osakonna tööiseloom erineb olulisel määral teistes uuringus osalevate osakondade tööiseloomust ning kompetentsidest (vt. Tabel 8). See tähendas küll seda, et antud grupi valimi suurus on oluliselt väiksem, kui teiste gruppide omad.

Tabel 8

Osakondade grupeerimine

Osakond	Grupp 1	Grupp 2	Grupp 3	Grupp 4	Grupp 5
Identiteediteenuste osakond	X				
Menetlusteenuste osakond		X			
Piiriteenuste osakond			X		
Pääste- ja hädaabiteenuste osakond			X		
Rahvastikuteenuste osakond		X			
Sisuteenuste osakond				X	
Veebiteenuste osakond				X	
Infoturbeosakond					X
Valimi suurus	21	21	28	25	7

Allikas: Autorite loodud

Tööpered grupeeriti sarnaste tööülesannete alusel. Esimese grupi alla valiti töötajad, kes uuringus märkisid enda ametiks tooteomanik, scrum master, tiimijuht, PO või analüütik ja andmeanalüütik. Autorid nimetasid grupp 1 koondnimetusega „Tooteomanikud“. Kokku oli grupis 27 töötajat. Teise gruppi koondati töötajad, kes märkisid oma rolliks arendaja või DevOps arendaja. Antud grupp on klassikalise DevSecOps töökorralduse teooria käsitluses toodud kui arenduse rolli täitvad töötajad. Autorid nimetasid grupi koondnimetusega „Arendajad“. Kokku oli selles grupis 25 töötajat. Kolmas grupp on kõik ülejäänud rollid, mis seonduvad infoturbe osakonna erinevate rollidega ning süsteemiadministraator, vanemprogrammeerija, tarkvara vanemarendaja, vanemarendaja, süsteemiarhitekt, arhitekt ja

testija. Antud grupp moodustub DevSecOps teooria käsitluse vaatest halduse ja infoturbe töötajatest, ning sellele on lisatud ka arhitekti rollis töötajad, kelle infoturbe silmaring ja teadmised on eelduste kohaselt laiemad kui tavatöötajal. Autorid nimetasid grupi koondnimetusega „Infoturbe spetsialistid“. Kokku oli selles grupis 21 töötajat. Gruppidest jäeti välja kõik need töötajad, kes enda rolli uuringus välja ei toonud.

Intervjuud kodeeriti selleks, et intervjuu ja uuring oleksid võrreldavad. Intervjuu kodeerimisel markeeriti vastused küsimuste kaupa positiivseks, keskmiseks või negatiivseks vastavalt koodidega kõrge, keskmine, madal (vt. Lisa D). Juhul kui tulemit ei olnud võimalik kodeerida, jäeti vastus kodeerimisel tühjaks. Saadud hinnanguid kasutati selleks, et võrrelda uuringu tulemusi juhtide hinnanguga ja kontrollida juhtide ning töötajate hinnangute vahelisi seoseid. Saadud tulemusi vaadeldi esimeses faasis teoreetilises peatükis leitud edutegurite lõikes uurides eraldi moodustatud osakondade gruppe ja tööperede gruppe. Seda eelkõige eesmärgiga kontrollida ja hinnata, kas töökorralduse juurutamisel on vaja arvestada mõne tööpere või osakonnaga rohkem, kui mõne teisega või kas edutegurite lõikes on asutuses ebaühtlust, mis võib tingida täiendavat keerukust hilisemal töökorralduse juurutamisel. Teises faasis analüüsiti tulemusi ADKAR muudatuse teooria vaatest. Analüüsi käigus kasutati keskmiste võrdlust ja faktoranalüüsi. Uuringu tulemuste analüüsi esimeses faasis teostasid autorid Kruskal-Wallis testi uuringu tulemuste võrdlemiseks tööpere grupi ja osakonna grupi vaatest. Kruskal-Wallis testi kasutati, kuna uuring viidi läbi Likerti skaalal mõõdetud järjestustunnustega. Analüüsivahendina kasutati IBM SPSS Statistics tarkvara. Analüüsid viidi läbi olulisuse nivool 0,05. Analüüsiks vaadeldi uuringu käigus esitatud küsimustiku küsimusi 1.1-13.1 (vt. Lisa B), millest analüüsi fookus oli eelkõige põhiosa küsimustikul ning sissejuhatava osa küsimusi kasutati grupeerimiseks ja erinevate seoste otsimiseks. Üheks täiendavaks aspektiks toodi autorite poolt uuringusse sisse ka töötajate soovitusindeks selleks, et hinnata organisatsiooni valmidust muutuseks.

Järgmises peatükis vaadeldakse uuringute tulemite analüüsi ja tulemusi, mis teostati uuringu ja intervjuude käigus kogutud andmete põhjal.

2.2. DevSecOps kriitiliste edutegurite kitsaskohad SMIT-s

Uuringu tulemusi iseloomustab suures plaanis see, et osakondade gruppide ja tööperede vaatest on enamus küsimuste tulemuste keskmised sarnased. Osakondade gruppide lõikes näitab analüüs, et uuritud kriitilistest eduteguritest erinevad tulemused oluliselt ainult kolme uuritud kriitilise eduteguri küsimuse puhul (vt. Tabel 9). Esiteks teadmiste jagamise osas nähakse erinevalt seda kuidas „Ma jagan teadmisi oma kolleegidega“, kus Sig=0,021. Antud küsimuse osas eristub selgelt Infoturbe osakond, kes näeb teistest osakondadest

olukorda oluliselt paremini. Tulemus tuleb autorite hinnangul Infoturbe osakonna rollist, mis on orienteeritud teiste osakondade toetamisele. Teiseks erineb oluliselt turbe teadmiste osas see, kuidas nähakse küsimust „Mu kolleegide teadmised infoturbest on head“, kus Sig=0,011. Eristuv osakond on antud küsimuse puhul Infoturbeosakond, kes näeb olukorda teistest osakondadest halvemana ja hindas olukorda kriitilisemalt. Selline tulemus on ootuspärane, kuna tänane töökorraldus on tiimipõhine ja infoturbe kompetents on eelkõige Infoturbe osakonnas. See kattub ka teooria käsitlusega, kus DevSecOps juurutamisel viiakse teadmist DevOps tiimi läbi töökorralduse muutuse (Myrbakken et al., 2017). Kolmas eristuv kriitiline edutegur on vastutuse võtmise plokis, kus osakondade lõikes nähakse erinevalt küsimust „Äritulemus on osa minu vastutusest“. Ka selle küsimuse puhul eristub eelkõige Infoturbe osakond, kes hindab seda küsimust madalamalt. Antud tulemit on autorite nägemuses võimalik selgitada Infoturbe osakonna toetava rolliga, mis ei ole otseselt seotud uue funktsionaalsuse loomise või mõne muu tellijapoolse arendussoovi või tellijale osutatava teenuse toimivuse tagamisega. Ülejäänud edutegurite lõikes osakondade gruppide tulemused üksteisest oluliselt ei erinenud, kuna nende puhul on Sig>0,05, mis näitab, et ülejäänud edutegurid on läbivalt sarnase iseloomuga ja organisatsioon näeb neid sarnaselt.

Tabel 9

Osakondade põhiselt grupeeritud Kruskal-Wallis test

	Kruskal-Wallis H	**p-väärtus**
Äritulemus on osa minu vastutusest	10,866	0,028
Ma jagan oma teadmisi oma kolleegidega	11,542	0,021
Mu kolleegide teadmised infoturbest on head	12,968	0,011

Allikas: Autorite loodud

Tööperede gruppide lõikes olulisuse nivool 0,05 eristub kriitilistest eduteguritest koostöö, tagasisidestamine ja vastutuse võtmine (vt. Tabel 10). Igast kategooriast eristub üks küsimus, kus tööpere gruppide lõikes on vastused erinevad. Esiteks koostöö osas nähakse erinevalt „Mu kolleegid on koostööle orienteeritud“, kus Sig=0,04. Teiseks tagasisidestamise osas nähakse erinevalt küsimust „Mu kolleegid annavad tagasisidet teistele, kui see aitab neil edasi areneda“, kus Sig=0,005. Esimese kahe eristuva küsimuse puhul hindavad tulemusi teistest oluliselt madalamalt Infoturbe spetsialistide grupp. Autorite arvates on see seletatav töögrupi eristuva rolliga, mis on rohkem orienteeritud teiste toetamisele ja koostööle. See seletab ka kriitilisust kolleegide koostöö ja tagasisidestamise osas, kuna tööperest tulenevalt on koostööst tingitud murekohad neile rohkem nähtavad. Kolmandaks vastutuse võtmise

puhul nähakse erinevalt küsimust „Mu kolleegid vastutavad oma igapäeva töö eest“, kus Sig=0,043. Antud juhul eristub arendajate tööpere grupp. Ülejäänud kriitilised edutegurid ja nende uurimiseks kasutatud küsimuste vastused tööperede lõikes üksteisest oluliselt ei erinenud. See näitab eelkõige seda, et organisatsioonis ei ole tööpere vaatest suuri erinevusi teiste kriitiliste edutegurite lõikes. Juhul, kui olulisuse nivoona vaadelda 0,1 taset, siis kerkivad esile veel täiendavalt suhtlusele orienteeritus, kus kolleegide info jagamise osas on Sig=0,083 ja turbeteadmiste osas hinnang enda turbe teadmistele, kus Sig=0,089. Samuti täiendavalt tuleb vastutuse võtmise osas juurde ka hinnang kolleegide vastutusest äritulemuste osas. Autorite arvates seletab kolleegide vastutuse võtmise hinnangut ja turbe teadmiste kriitilisemat hinnangut infoturbe spetsialistide tööpere grupi poolt nende enda kõrgem turbeteadlikkus, mis tingib kriitilisema hinnangu nii vastutuse võtmise kui ka turbe teadmiste osas. Mõlemad kattuvad ka teoreetilise käsitlusega, kus ühe kriitilise aspektina nähti turbeteadmiste olemasolu arendustiimides (Koskinen, 2020).

Tabel 10

Tööpere põhiselt grupeeritud Kruskal-Wallis test

	Kruskal-Wallis H	**p-väärtus**
Mu kolleegid on koostööle orienteeritud	6,426	0,04
Mu kolleegid annavad tagasisidet teistele, kui see aitab neil edasi areneda	10,721	0,005
Mu kolleegid vastutavad oma igapäeva töö eest	6,277	0,043
Mu kolleegid jagavad infot oma kolleegide ja teiste tiimidega	4,988	0,083
Äritulemus on osa minu kolleegide vastutusest	4,947	0,084
Mu kolleegide teadmised infoturbest on head	4,84	0,089

Allikas: Autorite loodud

Kogu valimi lõikes iseloomustab uuringut see, et ennast nähakse tugevamana kui oma kolleege. Seda nii käitumuslikest aspektidest, kui ka teadmiste vaatest. Järgmises faasis teostasid autorid korrelatsioonianalüüsi selleks, et kontrollida kas erinevate kriitiliste edutegurite vahel esineb korrelatsiooni ning kas korrelatsiooni esineb töötaja staaži või töötaja soovitusindeksi tulemusega. Analüüs teostati statistilise olulisuse tasemel 0,05. Tugevat korrelatsiooni tasemel üle 0,7 esines ainult seotud küsimuste puhul (vt. Lisa E). Nendeks olid „Turvalisus on osa minu vastutusest“, „Äritulemused on osa minu vastutusest“ ja „Olen piisavalt kursis teistes tiimides toimuvaga, et oma tööd edukalt teha“ mina ja kolleegide küsimuste vahel. Ülejäänud korrelatsioonid esinesid madalamatel tasemetel. Tulemuste analüüsi käigus ilmnes, et korrelatsiooni staažiga ei esine, kuna Spearman-i

korrelatsioonikordaja tugevat seost ei näidanud ja küsimuste vastuste analüüsi tulemused jäid kõik alla 0,2. Samas näitas teistest tugevamat korrelatsiooni töötaja soovitusindeks 12 küsimuse puhul 27-st, ehk korrelatsiooni indeks oli nende puhul üle 0,3. Kokku 23 küsimuse puhul oli korrelatsioon üle 0,2 taseme. Autorite arvates on see tingitud töötaja soovitusindeksi ja positiivse suhtumise tugevast seosest, mis tingib töötaja poolse positiivse hoiaku nii enda toimetamise kui ka kolleegide suhtes. Ainukesed erinevused esinesid küsimustes „Mu kolleegid jagavat infot oma kolleegide ja teiste tiimidega“, „Ma leian igapäevaselt võimalusi, et muuta oma tööd paremaks“, „Ma jagan oma teadmisi oma kolleegidega“ ja „Mu kolleegide teadmised infoturbest on head“, kus korrelatsiooni kordaja oli kõigil juhtudel alla 0,2. Seda võib autorite arvates seletada sellega, et nende küsimuste iseloom on selline, kus organisatsiooni suhtes positiivne hoiak ei mõjuta niivõrd tugevalt hinnangut. Kui vaadelda korrelatsiooni erinevate kriitiliste edutegurite lõikes, siis on näha, et 77% edutegureid uurivatest küsimustest korreleerub.

Kuna lisaks korrelatsioonile erinevate küsimuste vahel olid tööpere ja osakonnapõhiste gruppide lõikes enamik küsimuste vastused sarnased ja erisused tulid välja ainult paari küsimuse ja kriitilise eduteguri lõikes, otsustasid autorid teostada faktoranalüüsi kontrollimaks, kas teooriast leitud edutegurid koonduvad faktoriteks. Selle kaudu on autorite hinnangul võimalik kontrollida, kas osad teooriast leitud eduteguritest on erinevad ainult sõnastuse vaatest ja tegelikult kirjeldavad sama faktorit. Selleks teostati eksploratiivne faktoranalüüs, kus kasutati andmete struktureerimiseks Verimatrix roteerimismeetodit. Elementide ja faktorite korrelatsiooni seose lävendiks kasutati 0,3, kuna väärtused alla selle ei oma tugevat seost. Tugevaks seoseks lugesid autorid väärtusi >0,6. Juhul, kui elemendid koondusid erinevate faktorite alla, siis liigitasid autorid elemendid faktoritesse kõige tugevama seose alusel. Juhul, kui erinevus oli minimaalne, siis kasutasid autorid enda kogemusele tuginedes kõige sobivamat liigitust. Andmeid vaadeldi kahes erinevas lõikes. Esiteks läbi enesehinnangu vastuste ja teiseks läbi kolleegidele antud hinnangute, et valideerida leitud faktoreid.

Faktoranalüüsi tulemusena leidsid autorid, et tuginedes enesehinnangule koonduvad 12 kriitilist edutegurit ja 16 küsimust kokku kolleegide küsimuste analüüsi alusel 4 erinevaks faktoriks (vt. Tabel 11). Sama tulemust kinnitab autorite hinnangul ka enesereflektsiooni vastustest tehtud faktoranalüüs (vt. Lisa C). Samas on autorite hinnangul viiendaks oluliseks kriitiliseks eduteguriks lisaks neljale faktorile turbeteadmised. Seda põhjusel, et hinnang kolleegide turbeteadmistele iseloomustab eelkõige infoliikumist, sest kolleegide turbeteadmistes teadlikkus eeldab organisatsiooni sisest läbipaistvust. Samas turbe teadmiste

enesehinnang on pigem hinnang kompetentsile. Sellest tulenevalt on autorite arvates õigem kasutada viienda kriitilise edutegurina faktorite kõrval Teadmiseid. Teadmiste olulisuse leidu kinnitab ka teooria käsitlusest leitud turbe teadmiste ära märkimine kriitilise edutegurina (Ahmed et al., 2019). Kriitiliste edutegurite koondumine neljaks faktoriks näitab autorite hinnangul seda, et erinevates teaduskirjandustest leitud kriitilised edutegurid on osaliselt kattuvad ja nende põhjal koostatud küsimused uurivad sama tegurit. Edaspidi sarnase uuringu korral ei ole vaja keskenduda kaheteistkümnele edutegurile ja piisab nelja erineva faktori uurimisest. Teooria käsitluses on toodud DevOps põhimõtetele sarnaseid nelja kategooria jaotust, mis on kultuur, automatiseerimine, mõõtmine ja jagamine (Koskinen, 2020), kui ka kolme kategooriasse jaotamist – inimesed, protsessid ja tehnoloogia (Raynaud, 2017). Eespool teostatud analüüsile sarnaste faktoritega lähenemist autorid teaduskirjandusest ei leidnud.

Tabel 11

Kriitiliste edutegurite koondumine faktoriteks kolleegide küsimuste kaudu

Kriitiline edutegur	**Küsimus**	**Koostöö**	**Protsess**	**Info liikumine**	**Parendustele orienteeritus**
		1	2	3	4
Suhtlusele orienteeritus	2.2	**0,791**	0,385		
	2.4	**0,789**			0,416
Koostööle orienteeritus	3.2	**0,649**		0,418	
Tagasisidestamine	4.2	**0,781**			
Vastutuse võtmine	5.2			0,362	0,360
	5.4				0,424
	5.6		0,372	**0,633**	
Parendustele orienteeritus	6.2				**0,809**
Teadmiste jagamine	7.2	0,324			**0,791**
Läbipaistvus	8.2	0,514		**0,593**	
Turbe teadmised	9.2			**0,832**	
Arendusprotsessi automatiseerimine	10.1		**0,666**	0,360	
Ärimõõdikud	11.1	0,434	**0,666**		
Turbe mõõdikud	12.1		0,460	0,747	
	12.2		**0,778**		
Turbe automatiseerimine	13.1		**0,807**		

Allikas: Autorite loodud

Uute moodustunud faktorite tulemusena on näha, et kokku koonduvad kriitilistest eduteguritest suhtlusele orienteeritus, koostööle orienteeritus ja tagasisidestamine. Autorid otsustasid koondunud faktorit nimetada koondnimetusega „Koostöö“. Kokku koonduvad ka arendusprotsessi automatiseerimine, ärimõõdikud, turbe mõõdikud ja turbe automatiseerimine. Turbe mõõdikud on võimelised koonduma ka kolmanda faktori alla, aga

autorid lähtusid sellest, et mõõdikud aitavad eelkõige hinnata ja juhtida protsessi, ning sellest tulenevalt koondasid autorid turbe mõõdikud teise faktori alla. Uue tekkinud faktori koondnimetuseks panid autorid „Protsess“. Kolmanda faktori alla koondub vastutuse võtmine, läbipaistvus ja kolleegide turbe teadmised, mida autorid nimetavad koondnimetusega „Info liikumine“. Läbipaistvus näitas samas võimekust koonduda ka „Koostöö“ alla, aga kuna autorite hinnangul on see olulisem just info liikumise juurutamise vaatest, siis otsustati järgida laadungi poolt osutatud „Info liikumise“ faktorit. Samuti koonduvad kokku parendustele orienteeritus ja teadmiste jagamine. Autorid otsustasid uut tekkinud faktorit nimetada koondnimetusega „Parendustele orienteeritus“. Viiendaks faktoriks kujuneb autorite hinnangul mina küsimuste põhisel faktoranalüüsi tulemusel (vt. Lisa C) turbe teadmine, mida autorid nimetavad koondnimetusega „Teadmised“. Moodustunud faktorite usaldusväärsust kontrolliti Cronbachi alfa kaudu (vt. Tabel 12). Tulemused näitavad seda, et kolm faktorit on usaldusväärsed, kus alfa on suurem kui 0,7. Samas „Info liikumine“ faktori puhul on alfa alla usaldusväärse nivoo. Seda võib autorite hinnangul seletada sellega, et faktor moodustus väga erinevate kriitiliste edutegurite pealt ja vähemalt üks neist iseloomustab lisaks infoliikumisele ka turbeteadmiste vaadet. See toetab autorite hinnangul „Teadmiste“ eraldiseisvat vaatlemist.

Tabel 12

Kriitiliste edutegurite koondumine faktoriteks kolleegide küsimuste kaudu

	Cronbachi Alfa
Koostöö	0,806
Protsess	0,838
Info liikumine	0,659
Parendustele orienteeritus	0,731

Allikas: Autorite loodud

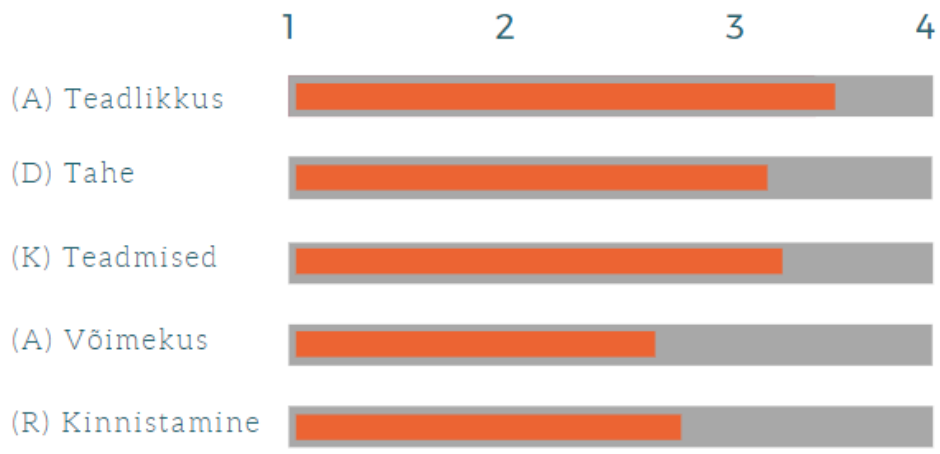
Selleks, et oleks võimalik hinnata organisatsiooni valmidust DevSecOps töökorralduse muudatuse juurutamiseks, kasutasid autorid töö analüüsi järgmises faasis teooria uurimise käigus koostatud ADKAR muudatuse etappide analüüsi, tuginedes teooria uurimise käigus leitud kriitilistele eduteguritele (vt. Tabel 2), mille baasil teostati uuringu tulemuste keskmiste tulemuste analüüs ADKAR etappide lõikes. Selleks moodustati kriitiliste edutegurite tulemuste põhjal iga ADKAR muudatuse teooria etapi osas kriitiliste edutegurite uuringu tulemuste koond, mis on toodud joonisel 7. Antud analüüs on oluline, kuna teooriast tulenevalt on DevSecOps töökorralduse juurutamine eelkõige kultuuriline muudatus fookusega töötajale (Myrbakken et al., 2017), mille juures on autorite hinnangul vaja

veenduda, et iga töötaja mõistaks muudatuse vajadust ja juhi roll on aidata töötajatel mõista protsesse ning enda rolli töökorralduse muutudes. Juhid aga peavad selleks olema teadlikud kriitilistest eduteguritest ja oskama seada fookust õigetele küsimustele muudatuse protsessis. Tulemuste põhjal võib järeldada, et organisatsioonis on tugevamal tasemel muudatuse etappidest (A) Teadlikkus, (D) Tahe ja (K) Teadmiste faas, kus tulemused jäävad keskmisest kõrgemaks. Sellest võib järeldada, et oma teadmiste ja oskustega ollakse valmis kolleegi toetama ja aitama, kui selleks on loodud vajalikud tingimused läbi kommunikatsiooni ja tagasisidestamise ning vastutuse andmise/võtmise tiimides tervikuna. Ehk muudatuse protsessi vaatest on töötajate valmisolek töökorralduslikuks muudatuseks keskmisest kõrgem. Seda kinnitab ka juhtide arvamus intervjuus.

„Tiimi sees on teadmiste jagamine väga hea. Kui üks suund ja eesmärk on ühine, siis panustatakse maksimaalselt ja see soodustab ka teadmiste jagamist.“ (Juht E, 11.03.2021)

Samas (A) Võimekuse ja (R) Kinnistamise faasides jäävad tulemused pigem keskpäraseks ja hinnangud on keskmiselt alla kolme (vt. Joonis 7). See tähendab seda, et eduka muudatuse vaatest on oluline tagada turbe teadmiste tõus töötajate seas, mis toetaks inimeste oskuste kasvu ja suurendaks töötajate võimekust täiendavate teadmiste ja oskuste kinnistumiseks, mis omakorda annab kindlust töötajatele oma töös õnnestumiseks. Probleemkohaks kriitilise edutegurina on võimekus infoturbe tööprotsesse automatiseerida ja tagada info liikumine ning läbipaistvus. Selleks, et saavutada hea ülevaade ja läbipaistvus vajab organisatsioon häid äri- ja turbemõõdikuid tulemuslikkuse mõõtmiseks. See aitab omakorda tagada eduka infoturbe juurutamist juba arenduse algfaasidest alates. Info liikumine ja puudulikud või ebavõrdsed infoturbe alased oskused/teadmised hakkavad autorite hinnangul pärssima koostööd. Sama nägemus leidis kinnitust ka juhtide intervjuudes, kus toodi välja, et koostöö arendamine on organisatsioonis tiimide vahel üks olulisemaid teemasid, mis vajab ka juhtide tähelepanu.

„5 skaalal annaks kõva 3+. Äriteenuste valdkonna juhid pingutavad, saavad kokku, mõtlevad koos. Asju arutatakse ka ilma juhtide abita.“ (Juht C, 04.03.2021)



Joonis 7. Organisatsiooni küpsus ADKAR muudatus teooria kohaselt
Allikas: Autorite loodud

Kui võrrelda faktoranalüüsis koondunud kriitilisi edutegureid ja ADKAR muudatuse teooria etappe, siis (A) Teadlikkuse etappi koonduvad faktoritest Koostöö ja osaliselt Info liikumine. (D) Tahe ja (K) Teadmised etappi koondub Parendustele orienteeritus. (A) Võimekuse etappi paiknevad Info liikumine ja Teadmised ning (R) Kinnistamise alla Protsess. ADKAR mudeli ja leitud faktorite jaotuse vahel on jagunemine erinev (A) Teadlikkus ja (A) Võimekus etappide puhul, kus Info liikumise faktor jaguneb kahe etapi vahel. See võib autorite hinnangul viidata ebakõlale, millele viitas ka Cronbachi alfa. Lisaks sellele koonduvad faktorite vaatest kokku ADKAR-i etapid (D) Tahe ja (K) Teadmised. Samal ajal ühtivad need etapid üks ühele algsete teaduskirjandusest leitud Teadmiste jagamise ja Parendustele orienteerituse edutegurite ga (Department of Defense, 2020; Myrbakken et al., 2017). Samas faktoranalüüs näitab nende vahelist tugevat seost. Autorite hinnangul võib selle taga olla faktoranalüüsis kasutatud uuringu küsimuste sõnastus või ka uuritud asutuse eripära, mis võib tingida kõrgema teadmiste vajaduse selleks, et oleks võimalik parendusi teostada.

Järgmises sammus uurisid autorid uute tekkinud faktorite keskmiste tulemuste lõikes organisatsiooni küpsust. Selleks moodustati faktorite põhjal küsimuste keskmised tulemused ja võrreldi neid organisatsiooni ja tööperede lõikes ning juhtide intervjuudest saadud hinnangutega.

Koostöö on uuringu tulemuste järgi keskmise tulemusena 3,507 (vt. Tabel 11), mis on kõrge tulemus. Osakondade ja tööpere gruppide lõikes eristuvust faktori keskmiste lõikes ei ole. Juhtide intervjuudest tulenev hinnang on keskmine, mis erineb oluliselt töötajate

hinnangust. Juhtide madalam hinnang on autorite arvates tingitud sellest, et juhid näevad koostöö keerukust selgemalt, kuna nende peale jääb sagedasti organisatsioonis koostöö edendamine ja probleemsete olukordade lahendamine.

Tabel 11

Faktorite võrdlus uuringute ja intervjuude lõikes

	Töötajad	Juhid
Koostöö	3,507	Keskmine
Parendustele orienteeritus	3,287	Keskmine
Info liikumine	2,622	Keskmine/kõrge
Teadmised	3,061	Keskmine
Protsess	2,871	Keskmine

Allikas: Autorite loodud

„Hästi palju on meie tegime ja meie oleme kõik teinud, et see info liiguks, aga teised ei ole aru saanud. Teise poole infost arusaamist peetakse teise poole vastutuseks, mitte enda vastutuseks. Selle mentaliteedi muutmine on suurim probleem.“ (Juht E, 11.03.2021)

Parendustele orienteeritus on uuringu tulemuste järgi keskmise tulemusena 3,287, mis on kõrge tulemus ja erineb juhtide poolt intervjuu käigus antud keskmisest hinnangust. Osakondade gruppide lõikes paistab välja Infoturbe osakond, kus keskmine on teistest osakondadest kõrgem. Samas tööperede gruppide vaatest on tulemused sarnased. Autorite hinnangul on tulemus tingitud sellest, et juhtide ootus arengule ja tulemuslikkusele on kõrgem, kui töötajatel keskmiselt.

„Üldiselt on see päris hea. On väga palju inimesi, kes mõtlevad sellele, et asjad muutuksid paremaks. Et kood muutuks paremaks, et ta õpiks juurde. Väga paljud inimesed tegutsevad väga tublisti. Keskmiselt on mõtteviis päris paljudel.“ (Juht A, 01.03.2021)

„Kõik pudelikaelad kaoksid ära kui see oleks paigas. Hetkel on palju olukordi, kus üks inimene teab.“ (Juht F, 11.03.2021)

Info liikumine on töötajate poolt antud uuringu tulemuste järgi kõige madalama hinnanguga tasemel 2,622. Osakondade lõikes on tulemused läbivalt madalad. Tööpere gruppide osas eristub keskmisest madalamate vastustega Infoturbe spetsialisti tööpere grupp. Kui võrrelda töötajate hinnanguid juhtide nägemusega, siis juhid hindavad info liikumist keskmiselt/kõrgelt. See on ootuspärane, kuna juhtide infoväli on üldjuhul suurem ja teadlikkus organisatsioonis toimuvast kõrgem. Samas töötajate madalam tulemus näitab pigem info liikumise probleemi juhtide ja töötajate tööperede vahel. Juhtide intervjuude info liikumise faktori vastused on vastajate lõikes varieeruva hinnanguga, on juhte, kes hindavad

turvalisuse ja äritulemuste eest vastutuse võtmist kõrgelt ja on juhte, kes hindavad keskmiselt. Intervjuudest mitmel juhul markeeriti ka eraldi ära see, et turvalisust nähakse pigem Infoturbe tiimi vastutusena.

„Peaks olema suurem kui see on. Väga sellele ei mõelda. See on lükatud SEC osakonna õlule. Küsivad üle SECist, aga kui SEC on kooskõlastanud, siis nad ise ei kahtle ja ei mõtle üle.“ (Juht E, 11.03.2021)

„*Ma olen päris hästi kursis. Juhi tase teab projekti pealkirja tasemel. Oma ajaloost tean ka tehnoloogilisi asju. Kui kerkib mingi teema ülesse, siis oskan kogemuse pealt soovitada kust uurida.“ (Juht B, 03.03.2021)*

Teadmiste osas on uuringu tulemused tasemel 3,061, mis on keskmisel tasemel ja ühtib juhtide poolt antud hinnanguga. Osakondade vaatest eristub teistest madalamate vastustega Infoturbe osakond ja infoturbe spetsialisti tööpere. Tulemused on autorite vaatest üllatavad, kuna võiks eeldada inimeste kriitilisemat enesehinnangut. Samas peegeldab selline hinnang olukorda, kus inimeste teadlikkus infoturbest tervikuna on madal.

„Mudel puudub teadmiste valideerimiseks. Aga hinnangu alusel pigem keskmisel tasemel. Inimesed on läbinud erinevaid koolitusi, osadel on kogemusi. Selle põhjal on tekkinud teadmised kuidas vältida ja mida tasub teha. Aga see ei ole süsteemne, et oskaksid kõigele olulisele tähelepanu pöörata.“ (Juht D, 08.03.2021)

Protsessi tulemused on uuringu järgi keskmisest madalamal tasemel 2,871, mis erineb juhtide poolt antud keskmisest hinnangust. Juhtide nägemuses on tulemus pigem keskmine, samas kui töötajate hinnang on alla keskmise. Osakondade gruppide lõikes on teistest madalama keskmise hinnanguga Menetlusteenuste ja Rahvastikuteenuste osakondade grupp. Tööperede vaatest on eristuvaks Infoturbe spetsialisti tööpere grupp, kelle hinnangud protsessi osas on teistest kõrgemad. Autorite hinnangul tulenevad tööpere erinevad tulemused tööpere suuremast teadlikkusest ja ligipääsust rolli spetsiifilistele töövahenditele.

„Uuemate rakenduste puhul kirjutame juurde automaatteste. Uute puhul 80% aga vanade puhul väga väike. Turbetestimisi tehakse alles lõpus. Pidevalt ei tehta. Automaatne turbetestimine pigem puudub. Osaliselt tehakse, aga arendusprotsessi alguse poole peal. Turbeasju vahendid alati ei näita. Suuremaid asju avastatakse pentestidega.“ (Juht C, 04.03.2021)

Juhtide intervjuude käigus hinnati ka täiendavate piirangute olukorda. Juhtide hinnangul nende tänast toimetamist täiendavad tehnoloogilised piirangud ja ka infoliikumise piirangud ei piira. Samuti ei suutnud nad leida ajaloost olukordi, kus need asjaolud oleksid nende tiimide tegevust piiranud. Enamus juhtidest suutsid tuua näiteid rahastusmudelist

tulenevate piiravate olukordade osas ning olid selle küsimuse juures emotsionaalsed. See tähendab autorite hinnangul seda, et protsesside faktori juures on oluline hinnata ka rahastuse toetuse aspekti ning see kinnitab Riigikontrolli poolt välja toodud rahastuse probleemi olemasolu (Viira et al., 2019).

„1000% piirab. Põhimõtteliselt on meil kliendi strateegiline prioriteet. Meil on olemas enda arusaam mida tuleb muuta, aga me ei suuda teenuste tagamiseks kuidagi raha välja võluda. Palutakse kirjutada taotlusi, siis kuna see läheb protsessi, siis teed seda 10 korda ümber, siis otsustatakse kuskil, et minge SF-i ja RES-st rahastust ei saa. Ja siis tekib probleem, et me ei saa oma inimestega lahendada. Rahastust ei saa ja ainus variant on prioritiseerida. Selle tulemusena tekib väga palju legacyt. On vaja keskenduda sellele, mille jaoks on raha.“ (Juht D, 08.03.2021)

Kokkuvõttes teostasid autorid uuringu andmete põhjal Kruskal-Wallis testi, millega uuriti tööpere gruppide ja osakonna gruppide erisusi. Tulemustest oli näha osakondade ja tööpere gruppide lõikes vastuste erinevust 3 küsimuse osas, kus Sig<0,05. Kui tööperede osas laiendada usaldusnivood 0,1 peale, siis oli näha eristuvust veel kolme täiendava küsimuse lõikes. Lisaks teostati korrelatsioonianalüüs, kust selgus, et küsimuste vahel on tugev korrelatsioon ning lisaks esineb korrelatsioon töötaja soovitusindeksi ja vastuste positiivsuse vahel. Järgmises faasis teostati faktoranalüüs selleks, et uurida teooriast leitud kriitiliste edutegurite koondumist ning vaadeldi küsimuste vahelise korrelatsiooni põhjuseid. Tulemustena leiti neli faktorit, mis on DevSecOps juurutamise vaatest kriitilised – Koostöö, Protsess, Info liikumine ja Parendustele orienteeritus. Peale seda vaadeldi tulemusi ADKAR muudatuse mudeli lõikes selleks, et tuvastada muudatuse protsessi vaatest keskmisest madalamaid kategooriaid, mis vajavad täiendavat tähelepanu. Tulemused osutasid, et suuremat pingutust vajavad (A) Võimekuse ja (R) Kinnistamise faasid. Viimase etapina võrreldi leitud faktorite keskmisi ning juhtide intervjuudest antud hinnangute erinevust ning osakondade ning tööpere gruppide erisusi.

Järgmises peatükis keskendume DevSecOps koostöö mudeli juurutamise võimaluste analüüsile ja soovitustele, kuidas SMIT-s tänases seisus oleks võimalik töökorralduslik muudatus edukalt ellu viia.

2.3.SMIT-s DevSecOps koostöö mudeli juurutamise võimaluste analüüs

Uurimustöö näitab, et SMIT on küll juurutanud DevOps töökorralduse, kuid täna on kriitilised edutegurid seisus, kus DevSecOps töökorraldust juurutades on vaja tähelepanu pöörata erinevatele töökorralduslikele aspektidele. Autorid lähenesid analüüsile kasutades teoreetilises osas leitud edutegureid ja ADKARi muudatusteooriat ning kombineerisid neid

Tabel 2 toodud ülesehituse alusel. Uuringust tulenevalt täiendati kriitiliste edutegurite vaadet koondunud faktoritega, sest mitmed kriitilistest eduteguritest erinesid ainult sõnastuse vaatest ja sisuliselt peegeldasid samu faktoreid erinevatest külgedest.

Selleks, et SMIT suudaks olla edukas DevSecOps töökorralduse juurutamisel on oluline pöörata tähelepanu muudatuse elluviimisele vastavalt ADKAR etappidele (vt. Tabel 13). Esimeses (A) Teadlikkus etapis on kõige olulisemateks faktoriteks Koostöö ja Infoliikumine. Uuringust selgub, et antud faas on suures pildis heas seisus, kuid tähelepanu vajavad eelkõige töötajate vaheline koostöö, tagasisidestamine ja turbe vastutuse aspekt. Uue töökorralduse juurutamisel tuleb organisatsioonis tegeleda usaldusliku õhkkonna loomisega, kus inimesed julgevad anda üksteisele tagasisidet. Samuti tuleb jätkata töötajate vahelise koostöö süvendamisega seda nii spetsialistide kui ka juhtide tasemel. Samuti vajab tähelepanu ja pingutust turbe vastutuse teadlikkuse tõstmine. Selle juures on oluline roll nii juhtidel, kui ka üldisel teadlikkuse tõstmisel. Lisaks sellele on oluline mõelda ka töötajate ja juhtide vahelisele infoliikumise parendamisele, et hoida ühist infovälja ja läbipaistvust.

Muudatuse faasides (D) Tahe ja (K) Teadmised on kitsaskohtade vaatest olukord pigem hea ja otseseid kitsaskohti autorite vaatest uuringu tulemustest välja ei tulnud. Samas on selles etapis kriitiline Parendustele orienteerituse faktor, mille juures on oluline organisatsioonis tagada senise parendustele orienteeritud kultuuri edendamine ja soodustada töötajate vahelist teadmiste jagamist. Oluline on, et tänane positiivne seis oleks jätkusuutlik ja muudatuse käigus ei tuleks tagasilööke, ehk see on miski, mida juhid peavad teadlikult jälgima.

Järgmine muudatuse faas on (A) Võimekus, mille kriitilisteks eduteguriteks on Info liikumine ja teadmised. Info liikumine toetab lisaks Võimekuse faasile ka esimest Teadlikkuse faasi. See näitab seda, et antud faktor on oluline mitmes muudatuse faasis. Võimekuse faasi vaatest tuli uuringust välja üksuste vaheline info liikumise pärsitus ja töötajate turbe teadmiste tase, mis on osakondade ja rollide vaatest erineval tasemel. DevSecOps töökorralduse juurutamisel on oluline panustada erinevate rollide vahelisse infoliikumisse ning mõelda läbi kus millist infot jagatakse ning kust millist infot on võimalik saada. Lisaks sellele on oluline panustada töötajate turbe teadmistesse. Selleks on oluline läheneda süstemaatiliselt ja planeerida pikaajalisem programm, mis aitaks tõsta inimeste oskusi ja teadlikkust. Juhtide intervjuust ja uuringust tulenevalt on näha, et inimeste enesehinnang ja tegelik seis ei pruugi olla kooskõlas reaalsusega. Ehk isegi, kui inimesed ise arvavad, et nende teadmised infoturbest on head, siis tegelik seis võib olla oluliselt halvem. Selleks, et olukorda muuta on oluline mõelda läbi inimeste teadmiste hindamise süsteem,

ning see kuidas neid turbe teadmiste omandamisel süsteemselt toetada, kas läbi koolituste või mentorluse.

Tabel 13

Uurimustöö leiud ja soovitused

ADKAR	Faktor/ kriitiline edutegur	Uuringust tulnud kitsaskohad	Fookus DevSecOps juurutamisel
A	Koostöö Info liikumine	• Töötajate koostööle orienteeritus • Tagasiside kultuuri juurdumine • Turbe vastutust nähakse Infoturbe tiimi rollina • Info liikumine juhtide ja töötajate vahel	• Tagasisidestamine kolleegide vahel • Juhtide ja töötajate vaheline koostöö süvendamine ja info liikumine • Turvalisuse eest vastutuse süvendamine ja teadlikkuse tõstmine
D K	Parendustele orienteeritus		• Parendustele orienteeritud kultuuri toetamine juhtide poolt • Teadmiste jagamise toetamine juhtide poolt
A	Info liikumine Teadmised	• Üksuste vaheline info liikumine on pärsitud • Töötajate turbe teadmised on piiratud	• Parandada info liikumist juhtide ja töötajatele vahel • Infokanalite kokkulepped - kus ja mida jagatakse • Turbe teadmiste tõstmine töötajate ja juhtide seas • Süstemaatiline töötajate koolitamine turbe teemades
R	Protsess	• Teadlikkus turbe automatiseerimise vahenditest ja turbe mõõdikutest madal • Turbe automatiseerimise vahendite seis kesine • Ärimõõdikute teadlikkus madal • Rahastusmudeli piirangud	• Ühtlustada juhtide ja töötajate arusaama protsessidest ja nende sisust • Tõsta teenuste automatiseeritust • Automatiseerida turbe teenuseid • Suurendada turbe mõõdikute teadlikkust • Juurutada läbivad turbemõõdikud • Selgete ärimõõdikute juurutamine • Töötajate teadlikkuse tõstmine mõõdikutest • Arvestada rahastusmudeli piirangutega töökorralduse juurutamisel

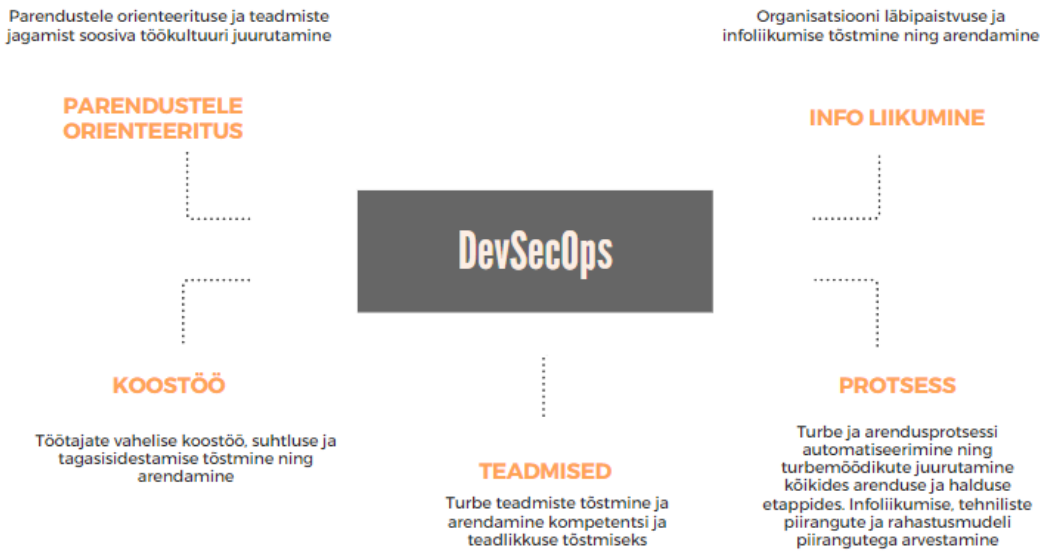
Allikas: Autorite loodud

Viimane etapp on (R) Kinnistamine, mille juures on kriitilise edutegurina oluline tagada Protsessi faktor. Uuringu tulemustest ilmnes, et tänasteks kitsaskohtadeks on teadlikkus turbe automatiseerimise vahenditest. Ehk töötajad kas ei tea või ei oska kasutada

olemasolevaid vahendeid. Üheks oluliseks arengukohaks on turbeteenuste arendamine selliselt, et nad võimaldaksid arendajatel iseseisvalt ilma Infoturbe osakonna abita toimetada. Selle juures on oluline mõelda terve elukaare ulatuses toe tekitamisele, et oleks katvus ja võimekus mõista ning tegeleda turbega igal sammul. Lisaks sellele on oluline puudus see, et töötajad ei ole kursis turbe mõõdikutega, mis on täna juurutatud. See näitab olulist puudujääki just läbipaistvuse tekitamise vaatest, kus on eesmärk saavutada inimeste teadlikkus turbe seisust läbi mõõdikute süsteemi, mis katab teenuste elukaare kõik etapid. Hetkel kasutusel olevad turbevahendid ja turbemõõdikud ei ole ideaalsed. Nende murekohaks on keskendumine teatud faasile, mis tähendab, et nad ei ole läbivad. Sarnane seis on ka ärimõõdikutega. Töötajate teadlikkus mõõdikutest tiimides on erinev, mis ei ole ideaalne ja vajab adresseerimist. Seda on võimalik lahendada läbi juhtide süsteemse töö info jagamise ja teadlikkuse tõstmisega või ka läbi info kajastamise erinevates raportites või tulemuste tutvustamisel. Edukaks muudatuse juurutamiseks on oluline ühtlustada juhtide ja töötajate arusaama protsessidest ja nende sisust. Täiendavalt on oluline edasi panustada teenuste automatiseerimisele, et tagada arendusprotsessi sujuvus. Oluline on keskenduda turbe teenuste teenusepõhisele arendamisele, mis võimaldaks pakkuda teenuseid ilma inimmahuka sekkumiseta ja annaks arendajatele võimekuse ise turbe teemalisi murekohti uurida. Samas on vaja mõelda sellele, kuidas inimesed teaksid turbe seisu, mille juures on oluline turbe mõõdikute teadlikkus ja nende võime visualiseerida turbe tegelikku seisu läbivalt kogu arendusprotsessi vältel ning teenuse elutsükli jooksul. Lisaks turbe mõõdikutele on oluline tõsta töötajate teadlikkust erinevatest ärimõõdikutest ja tagada selgete ärimõõdikute juurutamine. Üheks täiendavaks tänaseks murekohaks on rahastusmudel, mis pärsib tiimide võimet toimida agiilses töömudelis. Intervjuudele tuginedes on näha ka seda, et asutuse vaatest on vaja toetada juhte ja organisatsiooni rahastusmudeli valiku ja protsessiga. Kui rahastusprotsess piirab agiilse töökorralduse edukat juurutamist ja tingib erinevaid murekohti, siis on vaja enne agiilsele töökorraldusele ja sealt ka edasi DevSecOps töökorraldusele liikumist mõelda läbi kuidas rahastus tagatakse pikema ajaliselt ja nii, et see tiimi toetaks.

Lisaks sellele tuli analüüsi faasis välja, et uuringu tulemustes esineb korrelatsioon töötajate soovitusindeksi ja DevSecOps kriitiliste edutegurite positiivse hinnangu vahel. Sellest johtuvalt võib autorite hinnangul organisatsiooni esmaseks olukorra hindamiseks kasutada töötajate soovitusindeksi küsitluse tulemusi. Selle mõõdiku kaudu on võimalik saada hinnang organisatsiooni üldisele seisukorrale. Seda eelkõige tulenevalt sellest, et kui töötajate soovitusindeks on madal, siis suure tõenäosusega ka suhtumine eduteguritesse ja faktorite seisu on pigem kriitiline. See tähendab, et muudatuse läbiviimisel peavad juhid

pingutama rohkem ja panustama enam muudatuse esimestesse faasidesse ning ettevalmistusse. See annab autorite hinnangul hea ja lihtsa töövahendi muudatusvalmiduse ja olukorra hindamiseks.



Joonis 8. DevSecOps juurutamisel kriitilised faktorid ja tegurid
Allikas: Autorite loodud

DevSecOps töökorralduse juurutamisel soovitavad autorid kasutada lisaks esmasele töötajate soovitusindeksi uurimisele magistritöö käigus leitud nelja faktorit - Koostöö, Infoliikumine, Parendustele orienteeritus, Teadmised ja Protsess (vt. Joonis 8). Samas eraldi on oluline uurida ka töötajate turbe teadmisi, kuna antud tegur ei koondunud teiste faktorite alla ja samuti ei korreleerunud ka teiste küsimustega. Samas oli nii teooria kui ka uuringu tulemuste järgi antud aspekt kriitiline ja seda on oluline eraldi DevSecOps töökorraldust juurutades vaadelda, et mõista organisatsiooni seisu. Faktorite uuringu läbiviimise järgselt tasub organisatsioonidel kindlasti juurutamisel jälgida ADKAR muudatuse teooria etappe ja tegeleda etappidega süsteemselt, et kindlustada juurutuse edukus.

Kokkuvõte

Küberohtude ja turbefookuse kasvuga on IT valdkonnas üle maailma kerkinud esile uus koostöövorm, kus senist DevOps tiimide koostöötamise loogikat on laiendatud ka teistesse distsipliinidesse. Üks selline koostöövorm, kus senistesse halduse ja arenduse tiimidesse on integreeritud lisaks ka küberturbe vastutus, on DevSecOps (*development, security and operations*) töökorraldus (Raynaud, 2017). Antud magistritöö eesmärk oli tuua esile DevSecOps töökorralduse rakendamise võimalused avaliku sektori IT organisatsioonis

SMIT näitel. Töö eesmärgi täitmiseks püstitasid autorid viis uurimisülesannet, alustades DevSecOps töökorralduse olemuse ja rolli avamisest ning töökorralduse kriitiliste edutegurite ja võimalike kitsaskohtade kaardistamisega avalikus sektoris ning lõpetades koostöömudeli edutegurite uurimisega SMIT-s ning töökorralduse juurutamise võimaluste selgitamisega.

Magistritöö koosneb kahest peatükist. Magistritöö teoreetilises osas töötati läbi teaduskirjandust ja toodi selle põhjal välja 12 kriitilist edutegurit (vt. Tabel 2). Lisaks kaardistati avalikku sektorit mõjutavad piiravad tegurid (vt. Joonis 6) ja uuriti muudatuse elluviimise samme muudatusteooria vaatest. Leitud edutegurid on suures plaanis organisatsiooni kultuuri, töötajate teadmisi ja töövahendeid mõjutavad. Samas teooriast kaardistatud piiravad tegurid on seotud info liikumise, tehnoloogia kasutamise ja rahastusmudeliga. Täiendavalt uurisid autorid erinevaid muudatuse teooriaid ja kombineerisid ADKAR muudatuse teooria DevSecOps kriitiliste edutegurite ga. Vaadeldes edutegureid ADKAR-i muudatuse mudeli põhjal oli näha, et edutegurid olid muudatuse juurutamise protsessi vaates jagunenud üle erinevate etappide.

Magistritöö empiirilises osas viidi läbi uuring SMIT kahe valdkonna töötajate seas. Magistritöö peamine uurimismeetod oli küsitlus ja intervjuude roll oli selgitada, anda küsitluse tulemustele selgitusjõudu ja sügavust - kasutati kvantitatiivset ja kvalitatiivset uuringut. Küsitlus teostati organisatsiooni tiimides selleks, et kontrollida organisatsiooni valmidust muudatuse juurutamiseks ning selleks, et hinnata muudatuse võimalikku edukust. Lisaks teostati arendusüksuse juhtidega kvalitatiivsed intervjuud teooriast leitud kriitiliste edutegurite olemasolu uurimiseks. Uuringu üldkogumi suuruseks oli 179 töötajat 8-st osakonnast (vt. Tabel 5). Üldkogumi aktiivsus oli 56,9%, ehk kokku vastas 102 töötajat. Uuring viidi läbi veebruar-märts 2021 ja intervjuud teostati märts 2021. Kokku kestsid intervjuud 7 tundi ja 2 minutit. Uuringu tulemuste analüüsi esimeses faasis teostasid autorid Kruskal-Wallis testi uuringu tulemuste võrdlemiseks. Lisaks teostati korrelatsioonianalüüs selleks, et kontrollida, kas erinevate kriitiliste edutegurite vahel esineb korrelatsioon. Järgmises faasis viidi läbi faktoranalüüs selleks, et uurida teooriast leitud kriitiliste edutegurite koondumist ning vaadeldi küsimuste vahelise korrelatsiooni põhjuseid. Tulemustena leiti neli faktorit, mis on DevSecOps juurutamise vaatest kriitilised – koostöö, protsess, info liikumine ja parendustele orienteeritus. Lisaks leiti täiendav tegur - teadmised, mis on kriitiline turbe teadmiste vaatest. Peale seda vaadeldi tulemusi ADKAR muudatuse mudeli lõikes selleks, et tuvastada muudatuse protsessi vaatest tähelepanu vajavaid aspekte. Viimase etapina võrreldi leitud faktorite keskmisi ning intervjuude ja uuringu tulemuste erisusi.

Analüüsi tulemustena võib väita, et DevSecOps töökorralduse edukaks juurutamiseks on oluline pöörata tähelepanu kriitilistele eduteguritele muudatuse elluviimisel vastavalt ADKAR muudatuse mudeli etappidele. Töökorralduse juurutamisel SMIT-s on oluline keskenduda Tabel 13 välja toodud leidudele ja soovitustele - fookust on vaja pöörata faktoritest info liikumisele ja protsessile ning eraldi leitud tegurile teadmised. Info liikumise osas vajab tähelepanu eelkõige töötajate ja juhtide vaheline info liikumine. Protsessi faktori osas vajab tähelepanu turbe automatiseerimine, turbe ja äri mõõdikute selgus ning töötajate teadlikkus neist. Teadmiste poolel on vaja tegeleda süstemaatiliselt töötajate ja juhtide turbe teadmiste kasvatamisega. Samas on oluline tagada ka koostöö ja parendustele orienteerituse hea seisu kindlustamine. Muudatuse elluviimisel tuleb SMIT-s olla tähelepanelik eelkõige võimekuse ja kinnistamise faasidega.

Antud töö oli keskendunud DevSecOps töökorralduse juurutamise võimaluste uurimisele SMIT-s, kuid DevSecOps töökorralduse vaatest on töö tulemused kasutatavad ka teistes avaliku sektori IT organisatsioonides. DevSecOps töökorralduse juurutamisel avalikus asutuses on autorite hinnangul oluline järgida antud uuringust leitud nelja faktorit (parendustele orienteeritus, info liikumine, protsess, koostöö) ja eraldi vaadelda turbe teadmisi, kuna esialgu teaduskirjandusest leitud kriitilised edutegurid olid osaliselt kattuvad ja nende põhjal koostatud küsimused uurisid osaliselt samu tegureid. Lisaks on autorite hinnangul võimalik kasutada organisatsiooni DevSecOps muudatuse valmiduse hindamiseks töötajate soovitusindeksit, kuna uuringu tulemustes oli näha korrelatsiooni enamuse küsimustega, mida kasutati kriitiliste edutegurite hindamiseks. Autorite hinnangul võiksid tulevased uuringud täiendavalt uurida info liikumise faktorit, kuna faktoranalüüsi tulemuse usaldusväärsus oli selle faktori lõikes madal.

Viidatud allikad

1. Ahmed, A. M., Moonsamy, V., Overbeek, S., & Manadis, C. (2019). *DevSecOps: Enabling Security by Design in Rapid Software Development*.
2. Aleksandrova, S. v., Vasiliev, V. A., & Aleksandrov, M. N. (2020). Problems of implementing information security management systems. *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020*, 78–81. doi: 10.1109/ITQMIS51053.2020.9322896
3. Almanei, M., Salonitis, K., & Tsinopoulos, C. (2018). A conceptual lean implementation framework based on change management theory. *Procedia CIRP*, *72*, 1160–1165. doi: 10.1016/j.procir.2018.03.141
4. Aminzade, M. (2018). *Confidentiality, integrity and availability – finding a balanced IT framework.*
5. Boca, D. G. (2014). *ADKAR Model vs Quality Management Change*. Retrieved from https://www.researchgate.net/publication/266310181
6. Bugubayeva, R. O., Sansyzbayevna, R. B., & Teczke, M. (2017). Approaches and models for change management. *Jagiellonian Journal of Management*, *3*, 195–208. doi: 10.4467/2450114XJJM.17.014.9785
7. Bullen, C. v., & Rockart, J. F. (1981). *A primer on critical success factors*.
8. Burke, W. W., & Litwin, G. H. (1992). A Causal Model of Organizational Performance and Change. *Journal of Management*, *18*(3). doi: 10.1177/014920639201800306
9. Caraturan, S. B. O. G., & Goya, D. H. (2019). Major Challenges of Systems-of-Systems with Cloud and DevOps - A Financial Experience Report. *Proceedings - 2019 IEEE/ACM 7th International Workshop on Software Engineering for Systems-of-Systems and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems, SESoS-WDES 2019*, 10–17. doi: 10.1109/SESoS/WDES.2019.00010
10. Carvalho, C., & Marques, E. (2019). *Adapting ISO 27001 to a Public Institution*.
11. Chow, T., & Cao, D. B. (2008). A survey study of critical success factors in agile software projects. *Journal of Systems and Software*, *81*(6), 961–971. doi: 10.1016/j.jss.2007.08.020
12. Clim, A. (2019). Cyber Security Beyond the Industry 4.0 Era. A Short Review on a Few Technological Promises. *Informatica Economica*, *23*(2/2019), 34–44. doi: 10.12948/issn14531305/23.2.2019.04

13. Contact Commitee. (2020). *Cybersecurity in the EU and its Member States*. Retrieved from www.contactcommittee.eu
14. Cox, A. M., Pinfield, S., & Rutter, S. (2019). Extending McKinsey's 7S model to understand strategic alignment in academic libraries. *Library Management*, *40*(5), 313–326. doi: 10.1108/LM-06-2018-0052
15. da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information and Computer Security*, *26*(5), 584–612. doi: 10.1108/ICS-08-2017-0056
16. Delfi. (2020). *Lapse sünni saab homsest registreerida e-rahvastikuregistris - DELFI*. Delfi. Retrieved from https://www.delfi.ee/archive/print.php?id=89273343
17. Department of Defense. (2020). *OSD DevSecOps Best Practice Guide*.
18. Erich, F., Amrit, C., & Daneva, M. (2014). *Report: DevOps Literature Review*. doi: 10.13140/2.1.5125.1201
19. Euroopa parlament ja nõukogu. (2014). Euroopa Parlamendi ja Nõukogu määrus (EL) nr 910/2014. *Euroopa Liidu Teataja*.
20. European Comission. (2020). *Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*.
21. Ferreira, S. A., Neto, J. V., & Batista, H. M. C. da S. (2019). Critical success factors on project and process management in competitive strategy implementation. *Brazilian Journal of Operations & Production Management*, *16*(4), 605–616. doi: 10.14488/bjopm.2019.v16.n4.a6
22. Fitzgerald, B., Stol, K. J., O'Sullivan, R., & O'Brien, D. (2013). Scaling agile methods to regulated environments: An industry case study. *Proceedings - International Conference on Software Engineering*, 863–872. doi: 10.1109/ICSE.2013.6606635
23. Galli, B. J. (2018). Change Management Models: A Comparative Analysis and Concerns. *IEEE Engineering Management Review*, *46*(3), 124–132. doi: 10.1109/EMR.2018.2866860
24. Gardner, D., & MacDonald, N. (2019). *12 Things to Get Right for Successful DevSecOps*.
25. Gerow, J. E., Grover, V., Thatcher, J., & Roth, P. L. (2014). Looking Toward the Future of IT-Business Strategic Alignment through the Past. *Source: MIS Quarterly*, *38*(4), 1159–1186. doi: 10.2307/26627966
26. GitKraken. (2020). *DevOps Tools Report 2020*.

27. Hasselbring, W., Henning, S., Latte, B., Mobius, A., Richter, T., Schalk, S., & Wojcieszak, M. (2019). Industrial DevOps. *Proceedings - 2019 IEEE International Conference on Software Architecture - Companion, ICSA-C 2019*, 123–126. doi: 10.1109/ICSA-C.2019.00029
28. Heeager, L. T., & Nielsen, P. A. (2020). Meshing agile and plan-driven development in safety-critical software: a case study. *Empirical Software Engineering*, *25*(2), 1035–1062. doi: 10.1007/s10664-020-09804-z
29. Hiatt, J. M., & Creasey, T. J. (2012). *Change Management*. Retrieved from www.change-management.com
30. Hossan, C. (2015). Applicability of Lewin's Change Management Theory in Australian Local Government. *International Journal of Business and Management*, *10*(6). doi: 10.5539/ijbm.v10n6p53
31. Islam, G., & Storer, T. (2020). A case study of agile software development for safety-Critical systems projects. *Reliability Engineering and System Safety*, *200*. doi: 10.1016/j.ress.2020.106954
32. Johnson, M., Cummings, D., Leinwand, B., & Elsberry, C. (2020). Continuous testing and deployment for urban air mobility. *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, *2020-October*. doi: 10.1109/DASC50938.2020.9256435
33. Koskinen, A. (2020). *DevSecOps: Building security into the core of DevOps*.
34. Kund, O. (2017, September 7). Vihje ID-kaardi kohta andsid Tšehhi teadlased. *Postimees*. Retrieved from https://www.postimees.ee/4235419/vihje-id-kaardi-kohta-andsid-tsehhi-teadlased
35. Lam, T., & Chaillan, N. (2019). *DoD Enterprise DevSecOps Reference Design*.
36. Laukkarinen, T., Kuusinen, K., & Mikkonen, T. (2018). Regulated software meets DevOps. *Information and Software Technology*, *97*, 176–178. doi: 10.1016/j.infsof.2018.01.011
37. Laukkarinen, T., Kuusinen, K., & Mikkonen, T. (2017). DevOps in regulated software development: Case medical devices. *Proceedings - 2017 IEEE/ACM 39th International Conference on Software Engineering: New Ideas and Emerging Results Track, ICSE-NIER 2017*, 15–18. doi: 10.1109/ICSE-NIER.2017.20
38. Lewerentz, M., Bluhm, T., Daher, R., Dumke, S., Grahl, M., Grün, M., Holtz, A., Krom, J., Kühner, G., Laqua, H., Riemann, H., Spring, A., & Werner, A. (2019). Implementing DevOps practices at the control and data acquisition system of an experimental fusion

device. *Fusion Engineering and Design*, *146*, 40–45. doi: 10.1016/j.fusengdes.2018.11.022

39. Lie, M. F., Gordón, M. S., & Colomo-Palacios, R. (2020). DevOps in an ISO 13485 Regulated Environment: A Multivocal Literature Review. In ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (Vol. 2657). CEUR-WS. doi: 10.1145/nnnnnnn.nnnnnnn
40. Mao, R., Zhang, H., Dai, Q., Huang, H., Rong, G., Shen, H., Chen, L., & Lu, K. (2020). Preliminary Findings about DevSecOps from Grey Literature. *Proceedings - 2020 IEEE 20th International Conference on Software Quality, Reliability, and Security, QRS 2020*, 450–457. doi: 10.1109/QRS51102.2020.00064
41. Martins, N., & Coetzee, M. (2009). Applying the Burke–Litwin model as a diagnostic framework for assessing organisational effectiveness. *SA Journal of Human Resource Management*, *7*(1). doi: 10.4102/sajhrm.v7i1.177
42. McCartney, D., & Semple, W. (2019). *Understanding cultural differences*.
43. Messina, A., & Fiore, F. (2016, June 20). The Italian Army C2 evolution: From the current SIACCON2 land command & control system to the LC2EVO using agile software development methodology. *2016 International Conference on Military Communications and Information Systems, ICMCIS 2016*. doi: 10.1109/ICMCIS.2016.7496585
44. MKM. (2007). *Riigi IT arhitektuur*. Retrieved from http://www.riso.ee/et/koosvoime/
45. MKM. (2011). *Riigi infosüsteemi koosvõime Raamistik*. Retrieved from http://www.creativecommons.ee
46. Moore, M. G., Bovoso, A. L., & Llp, T. (2018). *DevSecOps Embedded Security Within the Hyper Agile Speed of DevOps*.
47. Morales, J., Turner, R., Miller, S., Capell, P., Place, P., & Shepard, D. J. (2020). *Guide to Implementing DevSecOps for a Systems of Systems in Highly Regulated Environments*. Retrieved from http://www.sei.cmu.edu
48. Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: A multivocal literature review. *Communications in Computer and Information Science*, *770*, 17–29. doi: 10.1007/978-3-319-67383-7_2
49. Nassereddine, M. (2020). DevSecOps practices for an agile and secure it service management. In Journal of Management Information and Decision Sciences (Vol. 23, Issue 2).

50. Newton, N. ;, Anslow, C. ;, & Drechsler, A. (2019). *Information security in agile software development projects: a critical success factor perspective*. Retrieved from https://aisel.aisnet.org/ecis2019_rp/92
51. Nurbojatmiko, Susanto, A., & Shobariah, E. (2016, September 26). Assessment of ISMS based on standard ISO/IEC 27001:2013 at DISKOMINFO Depok City. *Proceedings of 2016 4th International Conference on Cyber and IT Service Management, CITSM 2016*. doi: 10.1109/CITSM.2016.7577471
52. O'Halloran, J. (2020). Microsoft Teams usage growth surpasses Zoom. *Computer Weekly*. Retrieved from https://www.computerweekly.com/news/252485100/Microsoft-Teams-usage-growth-surpasses-Zoom
53. Paul, K. (2020, April 2). "Zoom is malware" why experts worry about the video conferencing platform Technology. *The Guardian*.
54. Postimees. (2019). *Digipööre 1. juulist saab surma e-registreerida*. Postimees. Retrieved from https://tarbija24.postimees.ee/6703781/digipoore-1-juulist-saab-surma-e-registreerida
55. PWC. (2018). *Siseministeeriumi haldusala IKT teenuste arendamise ja haldamise finantseerimise jätkusuutlikkus ning mõju siseturvalisuse tagamisele*.
56. PWC. (2020). *IKT baasteenuste korrastamise analüüs*.
57. Raynaud, F. (2017). *DevSecOps Whitepaper The business benefits and best practices of DevSecOps implementation*.
58. RIA. (2016). *Infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE rakendusjuhend*.
59. RIA. (2017). *Eesti Vabariigi infosüsteemis autentimislahendustele kehtivad nõuded*.
60. RIA. (2020). *Cyber security in Estonia 2020*.
61. Riigikontroll. (2019). *Ülevaade infotehnoloogia kuludest ja investeeringutest ministeeriumides ja nende asutustes*.
62. Rindell, K., Hyrynsalmi, S., & Leppänen, V. (2016). Case Study of security development in an agile environment: Building identity management for a government agency. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 556–563. doi: 10.1109/ARES.2016.45
63. Rockart, J. F. (1979). Chief Executives Define Their Own Data Needs. *Harvard Business Review*, *57*(2), 81–93.
64. Rosenbaum, D., More, E., & Steane, P. (2018). Planned organisational change management: Forward to the past? An exploratory literature review. In Journal of

Organizational Change Management (Vol. 31, Issue 2, pp. 286–303). Emerald Group Publishing Ltd. doi: 10.1108/JOCM-06-2015-0089

65. Sánchez-Gordón, M., & Colomo-Palacios, R. (2018). *Characterizing DevOps Culture: A Systematic Literature Review*.
66. Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management." *Journal of Enterprise Information Management*, *27*(5), 644–667. doi: 10.1108/JEIM-07-2013-0052
67. Siseministeerium. (2018). *Siseministeeriumi Valitsemisala juhtimispõhimõtete uuring 2018*.
68. SMIT. (2020a). *SMIT eesmärgid 2020*.
69. SMIT. (2020b). *Töötaja rahulolu uuring 2020*.
70. SMIT. (2021). *SMIT*. Retrieved from www.smit.ee
71. Sony, M., & Naik, S. (2020). Critical factors for the successful implementation of Industry 4.0: a review and future research direction. *Production Planning and Control*, *31*(10), 799–815. doi: 10.1080/09537287.2019.1691278
72. Sorainen. (2016). *Riigipilve kontseptsiooni rakendamise õigusanalüüs*.
73. Sousa, P. S. de, Nogueira, N. P., Santos, R. C. dos, Maia, P. H. M., & Souza, J. T. de. (2020). Building a prototype based on Microservices and Blockchain technologies for notary's office: An academic experience report. *Proceedings - 2020 IEEE International Conference on Software Architecture Companion, ICSA-C 2020*, 122–129. doi: 10.1109/ICSA-C50368.2020.00031
74. Stankovic, D., Nikolic, V., Djordjevic, M., & Cao, D. B. (2013). A survey study of critical success factors in agile software projects in former Yugoslavia IT companies. *Journal of Systems and Software*, *86*(6), 1663–1678. doi: 10.1016/j.jss.2013.02.027
75. Szabo, R. Z., Herceg, I. V., Hanák, R., Hortovanyi, L., Romanová, A., Mocan, M., & Djuričin, D. (2020). Industry 4.0 implementation in b2b companies: Cross-country empirical evidence on digital transformation in the cee region. *Sustainability (Switzerland)*, *12*(22), 1–20. doi: 10.3390/su12229538
76. Tchernykh, A., Schwiegelsohn, U., Alexandrov, V., & Talbi, E. G. (2015). Towards understanding uncertainty in cloud computing resource provisioning. *Procedia Computer Science*, *51*(1), 1772–1781. doi: 10.1016/j.procs.2015.05.387
77. Tooming, M., & Pärli, M. (2020). Riigi vastu toimusid küberründed, kätte saadi 9158 koroonapatsiendi andmed. *ERR*. Retrieved from https://www.err.ee/1192309/riigi-vastu-toimusid-kuberrunded-katte-saadi-9158-koroonapatsiendi-andmed

78. Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: a critical success factor analysis. *Information and Computer Security*, *26*(2), 150–170. doi: 10.1108/ICS-06-2017-0042
79. Vabariigi Valitsus. (2017). *Hädaolukorra seadus*.
80. Vabariigi Valitsus. (2018a). *Avalike teenuste pakkumise arendamiseks toetuse andmise tingimused ja kord*.
81. Vabariigi Valitsus. (2018b). *Küberturvalisuse seadus*.
82. Vabariigi Valitsus. (2019). *Riigisaladuse ja salastatud välisteabe kaitse kord*.
83. Vabariigi Valitsus. (2020a). *Infosüsteemide turvameetmete süsteem*.
84. Vabariigi Valitsus. (2020b). *Perioodi 2014-2020 struktuuritoetuse seadus*.
85. Vabariigi Valitsus. (2020c). *Siseministeeriumi infotehnoloogiaja arenduskeskuse põhimäärus*.
86. Valitsuse kommunikatsioonibüroo. (2020). *Valitsus kuulutas Eestis välja eriolukorra 1. maini*. Vabariigi Valitsus. Retrieved from https://www.valitsus.ee/et/uudised/valitsus-kuulutas-eestis-valja-eriolukorra-1-maini
87. Viira, T., Lääne, A., Saksing, M., Lazartšuk, J., & Nõuakas, A. (2019). *Avaliku sektori tarkvaraarenduse projektide juhtimine Miks tarkvaraarendused ebaõnnestuvad?*
88. von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, *26*(1), 2–9. doi: 10.1108/ICS-04-2017-0025
89. Wagner, T. J., & Ford, T. C. (2020). Metrics to Meet Security & Privacy Requirements with Agile Software Development Methods in a Regulated Environment. In 2020 International Conference on Computing, Networking and Communications (ICNC).
90. Zaheeruddin, A., & Shoba, C. F. (2019). *Integrating Security with DevSecOps: Techniques and Challenges*.
91. Zaitsev, A., Gal, U., & Barney, T. (2018). *Reviewing the Role of the Agile Manifesto and Agile Methods in Literature*. Retrieved from https://www.researchgate.net/publication/334899651
92. Zenab, K. S. A., & Naarananoja, M. (2013). Comparative approaches of key change management models - a fine assortment to pick from as per situational needs! *Annual International Conference on Business Strategy & Organizational Behaviour (BizStrategy)*, 217–224. doi: 10.5176/2251-1970_BizStrategy13.41

LISA A

Intervjuu küsimused

Teema-plokk	Küsimus	Seos kirjandusega
Sissejuhatavad küsimused ja taustainfo	1.1. Mis üksuses töötate? 1.2. Kui vana olete? 1.3. Kui pikalt olete SMIT-s töötanud? 1.4. Kui suures organisatsioonis te enne töötasite? 1.5. Kas te soovitaksite SMIT-i tööandjana (10 palli skaalal, eNPS mudel)?	-
Suhtlusele orienteeritus	2.1. Millisel viisil toimib täna töötajate vaheline suhtlus? 2.2 Kuidas hindate tänast töötajate vahelist info liikumist?	Töötajad on suhtlemisele orienteeritud, mis on eduka koostöö eelduseks ja tagab info liikumise. (Department of Defense, 2020; Koskinen, 2020; Morales et al., 2020)
Koostööle orienteeritus	3.1. Millisel viisil toimib koostöö töötajate vahel? 3.2. Kuidas toimib koostöö osakondade vahel? 3.3. Kuivõrd piirab koostöö täna tulemuslikkust?	Töötajad on koostööle orienteeritud, mis tagab äritulemusele orienteritus. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; McCartney et al., 2019; Moore et al., 2018; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017; Wagner et al., 2020)
Tagasi-sidestamine	4.1. Kuidas toimib SMIT-s töötajate vaheline tagasisidestamine? 4.2 Kuivõrd toetab tagasisidestamine organisatsiooni, üksuse ja sinu kui töötaja arengut?	Töötajate vahel toimub tagasisidestamine, mis võimaldab organisatsioonil areneda. (Department of Defense, 2020; Koskinen, 2020; Morales et al., 2020)
Vastutuse võtmine	5.1. Kuidas toimib täna töötajate poolne vastutuse võtmine? 5.2. Kuivõrd näevad teie tiimi töötajad täna enda rolli äritulemuste saavutamisel? 5.3. Milline on teie tiimi töötajate vastutus turvalisuse tagamisel?	Töötajad võtavad vastutust ja näevad äritulemusteni jõudmist ning ka turvalisust enda vastutusena. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; McCartney et al., 2019; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017)
Parendustele orienteeritus	6.1. Kuidas hindate tänast töötajate parendustele orienteeritust? 6.2. Kuivõrd töötajad julgevad ja tahavad uuendusettepanekuid pakkuda? 6.3. Kust tulevad tavaliselt ettepanekud(juhilt/kõigilt)?	Töötajad on parendustele orienteeritud. Toetab organisatsiooni õppimist ja pidevat arengut. (Department of Defense, 2020; Morales et al., 2020)
Teadmiste jagamine	7.1. Kuidas toimib täna töötajate vaheline teadmiste jagamine? 7.2. Millisel määral toetab teadmiste jagamine organisatsiooni arengut?	Töötajate vaheline teadmiste jagamine võimaldab organisatsioonil kiiremini edasi areneda. (Department of Defense, 2020; Koskinen, 2020; Myrbakken et al., 2017)

Läbipaistvus	8.1. Kuidas olete kursis teistes tiimides toimuvaga? 8.2. Millisel määral toetab tänane info liikumine tiimide vahelist koostööd?	Tiimide vaheline läbipaistvus, mis toetab koostööd. (Department of Defense, 2020; Morales et al., 2020)
Turbe teadmised	9.1. Milline on teie tiimi töötajate turbe alaste teadmiste seis? 9.2. Kuidas toetab turbe teadmiste olemasolu teie tiimi võimekust juurutada turvet õigeaegselt?	Turbeprintsipide ja meetodite ning teadmiste olemasolu DevSecOps tiimides loob võimaluse juurutada turvet arenduse käigus ja väldib hilisemat lahenduse parendamist ning ümber ehitamist. (Ahmed et al., 2019; Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017)
Arendusprotsessi automatiseerimine	10.1. Kuidas toetavad tänased arendusprotsessi automatiseerimise vahendid teie tiimi töö efektiivsust? 10.2 Milline on asutuse automatiseerimisvahendite seis võrreldes teiste organisatsioonidega? 10.3. Kui palju on teie arvates arenguruumi tuleviku mõttes?	Arendusprotsessis tarkvara ehitamise, juurutamise ja testimise automatiseerimine, mis tagab arendusprotsessi kiirus. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017)
Ärimõõdikud	11.1. Millisel määral peegeldavad tänased ärimõõdikud asutuse tulemuslikkust? 11.2. Kuivõrd aitavad tänased ärimõõdikud leida uusi parendus võimalusi?	Äriväärtust peegeldavate mõõdikute juurutamine selleks, et tagada läbipaistvus ja selgus, kuidas asutusel läheb ja et oleks võimalik leida uusi parendus võimalusi. (Ahmed et al., 2019; Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017; Wagner et al., 2020)
Turbe mõõdikud	12.1. Kuidas on täna tagatud terve arendusprotsessi kaetus turbemõõdikutega? 12.2. Kuivõrd aitavad tänased turbemõõdikud avastada probleeme varakult?	Turbe ohtude ja nõrkuste mõõtmine terves arendusprotsessis tagab organisatsioonile võimaluse avastada probleemid varakult. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017; Wagner et al., 2020)
Turbe automatiseerimine	13.1. Millisel määral on tänasesse arendusprotsessi juurutatud automaatne turbetestimine?	Turbe teenuste automatiseeritus võimaldab juurutada turbetestimise arendusprotsessi. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; Moore et al., 2018; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017)
Täiendavate tehnoloogiliste piirangute	14.1. Kuivõrd on teie tiim seotud süsteemidega, mis eeldavad täiendavaid turbemeetmeid (n. õhuvahe)?	Tulenevalt täiendavatest turbenõuetest on vajadus juurutada lisapiiranguid, mis tagavad turbetaset. (Morales et al., 2020; Wagner et al., 2020)

Info piiratuse tagamise	15.1 Millisel määral on tänaste süsteemide turbepiirangutest tulenevalt teie tiimis täiendavaid infovahetuse piiranguid töötajate vahel?	Koostöö piiratus, kuna isikute turbeload on erinevad, ehk nad saavad „näha“ ainult teatud asju. (Morales et al., 2020)
Rahastus-mudel	16.1. Kas ja millisel määral piirab teie tiimi toimetamist rahastusmudel (Struktuurfond jne.)?	Piiravate nõuetega finantseerimismudel võib oluliselt takistada agiilsete arendusmeetodite kasutamist asju. (Vabariigi Valitsus, 2018a, 2020b; Viira et al., 2019)
Intervjuu lõpetamine	17.1. Kui see teema kokku võtta, siis mis on teie jaoks need kõige olulisemad asjad SMIT-i toimimise puhul, mida me võiks siit intervjuust kaasa võtta?	-

LISA B

Küsitluse ankeet

ADKAR	Teemaplokk	Küsimus	Seos kirjandusega
-	Sissejuhatavad küsimused ja taustainfo	1.1. Millises üksuses töötate? 1.2. Mis on teie ametikoht? 1.3. Kui vana olete? 1.4. Kas te olete mees/naine? 1.5. Kui pikalt olete SMIT-s töötanud? 1.6. Kuivõrd te soovitate SMIT-i tööandjana?	-
(A) - Teadlikkus	Suhtlusele orienteeritus	2.1. Mulle meeldib suhelda oma kolleegidega 2.2. Mu kolleegid on suhtlusele orienteeritud 2.3. Ma jagan infot oma kolleegide ja teiste tiimidega 2.4. Mu kolleegid jagavad infot oma kolleegide ja teiste tiimidega	Töötajad on suhtlemisele orienteeritud, mis on eduka koostöö eelduseks ja tagab info liikumise. (Department of Defense, 2020; Koskinen, 2020; Morales et al., 2020)
	Koostööle orienteeritus	3.1. Ma olen koostööle orienteeritud 3.2. Mu kolleegid on koostööle orienteeritud	Töötajad on koostööle orienteeritud, mis tagab äritulemusele orienteeritus. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; McCartney et al., 2019; Moore et al., 2018; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017; Wagner et al., 2020)
	Tagasi-sidestamine	4.1. Ma annan oma kolleegidele tagasisidet kui näen, et see aitab neil edasi areneda 4.2. Mu kolleegid annavad tagasisidet teistele, kui see aitab neil edasi areneda	Töötajate vahel toimub tagasisidestamine, mis võimaldab organisatsioonil areneda. (Department of Defense, 2020; Koskinen, 2020; Morales et al., 2020)
	Vastutuse võtmine	5.1. Ma vastutan oma igapäeva töö eest 5.2. Mu kolleegid vastutavad oma igapäeva töö eest 5.3. Äritulemus on osa minu vastutusest 5.4. Äritulemus on osa minu kolleegide vastutusest 5.5. Turvalisus on osa minu vastutusest 5.6. Turvalisus on osa minu kolleegide vastutusest	Töötajad võtavad vastutust ja näevad äritulemusteni jõudmist ning ka turvalisust enda vastutusena. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; McCartney et al., 2019; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017)
(D)- Tahe	Parendustele orienteeritus	6.1. Ma leian igapäevaselt võimalusi, et muuta oma tööd paremaks 6.2. Mu kolleegid leiavad igapäevaselt võimalusi, et muuta oma tööd paremaks	Töötajad on parendustele orienteeritud. Toetab organisatsiooni õppimist ja pidevat arengut. (Department of Defense, 2020; Morales et al., 2020)

(K)- Teadmised	Teadmiste jagamine	7.1. Ma jagan oma teadmisi oma kolleegidega 7.2. Mu kolleegid jagavad oma teadmisi teistega	Töötajate vaheline teadmiste jagamine võimaldab organisatsioonil kiiremini edasi areneda. (Department of Defense, 2020; Koskinen, 2020; Myrbakken et al., 2017)
(A)- Võimekus	Läbipaistvus	8.1. Olen piisavalt kursis teistes tiimides toimuvaga, et olla edukas oma töös 8.2. Mu kolleegid on piisavalt kursis teistes tiimides toimuvaga, et olla edukad oma töös	Tiimide vaheline läbipaistvus, mis toetab koostööd. (Department of Defense, 2020; Morales et al., 2020)
	Turbe teadmised	9.1. Minu teadmised infoturbest on head 9.2. Mu kolleegide teadmised infoturbest on head	Turbeprintsipide ja meetodite ning teadmiste olemasolu DevSecOps tiimides loob võimaluse juurutada turvet arenduse käigus ja väldib hilisemat lahenduse parendamist ning ümber ehitamist. (Ahmed et al., 2019; Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017)
(R)- Kinnistamine	Arendusprotsessi automatiseerimine	10.1. Arendusprotsessi automatiseeritud töövahendid toetavad minu igapäevast tööd	Arendusprotsessis tarkvara ehitamise, juurutamise ja testimise automatiseerimine, mis tagab arendusprotsessi kiirus. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017)
	Ärimõõdikud	11.1. Ärimõõdikud aitavad mul mõista, kuidas minu töö mõjutab asutuse tulemuslikkust	Äriväärtust peegeldavate mõõdikute juurutamine selleks, et tagada läbipaistvus ja selgus, kuidas asutusel läheb ja et oleks võimalik leida uusi parendus võimalusi. (Ahmed et al., 2019; Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017; Wagner et al., 2020)
	Turbe mõõdikud	12.1. Ma tean kogu arendusprotsessi vältel turvalisust peegeldavate mõõdikute seisu 12.2. Turvalisust peegeldavad mõõdikud aitavad mul avastada probleeme varakult	Turbe ohtude ja nõrkuste mõõtmine terves arendusprotsessis tagab organisatsioonile võimaluse avastada probleemid varakult. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; Morales et al., 2020; Myrbakken et al., 2017; Wagner et al., 2020)
	Turbe automatiseerimine	13.1. Automaatne turbetestimine toetab mu igapäevatööd	Turbe teenuste automatiseeritus võimaldab juurutada turbetestimise arendusprotsessi. (Ahmed et al., 2019; Department of Defense, 2020; Koskinen, 2020; Moore et al., 2018; Morales et al., 2020; Myrbakken et al., 2017; Raynaud, 2017)

Skaala: 4- täiesti nõus, 3- pigem nõus, 2- pigem ei ole nõus, 1-ei ole nõus, 0- Ei oska hinnata

LISA C

Kriitiliste edutegurite koondumine faktoriteks(mina)

		Protsess	Koostöö	Info liikumine	Parendustele orienteeritus	Teadmised
		1	2	3	4	5
Suhtlusele orienteeritus	Mulle meeldib suhelda oma kolleegidega		**0,792**			
	Ma jagan infot oma kolleegide ja teiste tiimidega		**0,662**			
Koostööle orienteeritus	Ma olen koostööle orienteeritud		0,533	0,535		
Tagasisidestamine	Ma annan oma kolleegidele tagasisidet kui näen, et see aitab neil edasi areneda		0,503	0,307	0,459	
Vastutuse võtmine	Ma vastutan oma igapäeva töö eest	0,477	0,493		0,369	
	Äritulemus on osa minu vastutusest		0,394	**0,604**	0,343	
	Turvalisus on osa minu vastutusest	0,376	0,456	0,403		
Parendustele orienteeritus	Ma leian igapäevaselt võimalusi, et muuta oma tööd paremaks				**0,821**	
Teadmiste jagamine	Ma jagan oma teadmisi oma kolleegidega				**0,808**	
Läbipaistvus	Olen piisavalt kursis teistes tiimides toimuvaga, et edukalt oma tööd teha			**0,800**		
Turbe teadmised	Minu teadmised infoturbest on head					**0,872**
Arendusprotsessi automatiseerimine	Arendusprotsessi automatiseeritud töövahendid toetavad minu igapäevast tööd	**0,667**				
Ärimõõdikud	Ärimõõdikud aitavad mul mõista, kuidas minu töö mõjutab asutuse tulemuslikkust	0,588		**0,619**		
Turbe mõõdikud	Turvalisust peegeldavad mõõdikud aitavad mul avastada probleeme varakult	**0,835**				
	Ma tean kogu arendusprotsessi vältel turvalisust peegeldavate mõõdikute seisu	0,515	0,467			0,498
Turbe automatiseerimine	Automaatne turbetestimine toetab mu igapäevatööd	**0,780**				

LISA D

Juhtide intervjuude kodeerimine

Kriitiline edutegur/ piirav faktor	**Küsimus**	**Juht A**	**Juht B**	**Juht C**	**Juht D**	**Juht E**	**Juht F**	**Juht G**
Suhtlusele orienteeritus	2.1							
	2.2	keskmine	keskmine	keskmine	keskmine	keskmine	madal	keskmine
Koostööle orienteeritus	3.1	keskmine	keskmine	kõrge	keskmine	keskmine	keskmine	keskmine
	3.2	keskmine	keskmine	keskmine	madal	madal	keskmine	keskmine
	3.3	keskmine	keskmine	keskmine	keskmine	keskmine	keskmine	keskmine
Tagasisidestamine	4.1	keskmine	keskmine	keskmine	keskmine	madal	keskmine	keskmine
	4.2	keskmine	keskmine			keskmine		keskmine
Vastutuse võtmine	5.1	madal	keskmine	keskmine	keskmine	keskmine	keskmine	keskmine
	5.2	keskmine	keskmine	kõrge	kõrge	keskmine	kõrge	kõrge
	5.3	keskmine	kõrge	kõrge	kõrge	keskmine	keskmine	keskmine
Parendustele orienteeritus	6.1	kõrge	kõrge	kõrge	keskmine	kõrge	kõrge	keskmine
	6.2	keskmine	keskmine	keskmine	kõrge	keskmine	keskmine	keskmine
	6.3	kõrge	kõrge	kõrge	kõrge	kõrge	kõrge	keskmine
Teadmiste jagamine	7.1	keskmine	keskmine	kõrge	kõrge	keskmine	kõrge	keskmine
	7.2	keskmine	keskmine		keskmine	keskmine	madal	keskmine
Läbipaistvus	8.1	keskmine	kõrge	kõrge	keskmine	madal	madal	keskmine
	8.2	madal	madal	kõrge	keskmine	madal	madal	kõrge
Turbe teadmised	9.1	keskmine	kõrge	keskmine	keskmine	madal	keskmine	keskmine
	9.2	kõrge	keskmine	madal	keskmine	keskmine	keskmine	keskmine
Arendusprotsessi automatiseerimine	10.1	keskmine	keskmine	kõrge	keskmine		keskmine	keskmine
	10.2	keskmine	madal	kõrge	keskmine		kõrge	madal
	10.3	madal	madal	keskmine	keskmine	keskmine	madal	keskmine
Ärimõõdikud	11.1	kõrge	keskmine	kõrge	keskmine	keskmine	kõrge	keskmine
	11.2	kõrge	kõrge	kõrge	kõrge	kõrge	kõrge	kõrge
Turbe mõõdikud	12.1	keskmine	keskmine	madal	keskmine	keskmine	madal	madal
	12.2	kõrge	kõrge	madal	madal	keskmine	madal	keskmine
Turbe automatiseerimine	13.1	madal	keskmine	keskmine	keskmine	keskmine	keskmine	keskmine
Täiendavate tehnoloogiliste piirangute juurutamise vajadus	14.1							
Info piiratuse tagamise vajadus	15.1							
Rahastusmudel	16.1	madal	madal	kõrge	madal	kõrge	madal	madal

LISA E

Spearmani korrelatsiooni analüüs

		Küsimus																												
		1.3	1.5	1.6	2.1	2.2	2.3	2.4	3.1	3.2	4.1	4.2	5.1	5.2	5.3	5.4	5.5	5.6	6.1	6.2	7.1	7.2	8.1	8.2	9.1	9.2	10.1	11.1	12.1	12.2	13.1
Spearman's rho	1.3	1,000	,319**	0,075	-0,036	0,000	-0,008	-0,025	0,077	-0,019	0,144	-0,074	-0,027	-0,098	0,060	-0,055	-0,028	-0,048	-0,001	0,073	-0,089	-0,116	-0,070	-0,089	-,210*	-0,053	-0,064	0,183	-0,046	-0,058	0,228
	1.5	,319**	1,000	0,071	-0,103	-0,013	-0,003	-0,114	-0,011	-0,132	0,119	0,032	0,051	0,004	0,061	0,025	0,038	0,050	-,243*	-,268*	0,016	-,208*	-0,021	-0,152	-0,028	-0,050	0,074	0,065	-0,011	0,004	0,202
	1.6	0,075	0,071	1,000	,460**	,248*	0,187	,367**	,455**	,298**	,290**	,303**	,256**	,202*	,391**	,318**	,293**	,225*	0,132	,249*	0,152	,250*	,334**	,351**	,217*	0,104	,239*	,409**	,466**	,380**	,492**
	2.1	-0,036	-0,103	,460**	1,000	,371**	,393**	,380**	,446**	,365**	,333**	,230*	,224*	,312**	,254*	,220*	,247*	,236*	,265**	,233*	,259**	,301**	,270**	,285**	0,149	0,212	0,178	0,139	,470**	,259*	0,145
	2.2	0,000	-0,013	,248*	,371**	1,000	,430**	,536**	,406**	,567**	,213*	,442**	,293**	,381**	,424**	,264**	,291**	,300**	0,098	,243*	,281**	,346**	0,191	,244*	0,010	0,092	0,098	,216*	,220*	0,058	,248*
	2.3	-0,008	-0,003	0,187	,393**	,430**	1,000	,542**	,418**	,382**	,362**	,281**	,240*	,297**	,339**	0,192	,377**	,341**	,356**	,254*	,469**	,322**	0,155	,224*	,228*	0,085	-0,013	0,074	,326**	0,038	0,104
	2.4	-0,025	-0,114	,367**	,380**	,536**	,542**	1,000	,409**	,549**	,301**	,490**	,300**	,328**	,387**	,294**	,389**	,344**	,201*	,392**	,362**	,430**	,284**	,398**	,231*	0,164	0,116	,234*	,287**	0,167	0,191
	3.1	0,077	-0,011	,455**	,446**	,406**	,418**	,409**	1,000	,532**	,508**	,388**	,378**	,272**	,424**	,404**	,543**	,551**	,280**	,402**	,408**	,230*	,361**	,396**	0,178	0,172	0,116	,295**	,431**	,269*	,245*
	3.2	-0,019	-0,132	,298**	,365**	,567**	,382**	,549**	,532**	1,000	,311**	,454**	,310**	,451**	,387**	,374**	,354**	,333**	0,046	,406**	,302**	,408**	,238*	,423**	,255*	,284**	0,106	0,205	,327**	0,162	0,154
	4.1	0,144	0,119	,290**	,333**	,213*	,362**	,301**	,508**	,311**	1,000	,540**	,286**	,272**	,323**	,297**	,341**	,416**	,240*	0,121	,458**	0,178	0,169	,312**	,263**	,258*	0,087	0,198	,365**	0,117	0,097
	4.2	-0,074	0,032	,303**	,230*	,442**	,281**	,490**	,388**	,454**	,540**	1,000	0,117	,388**	,306**	,332**	,218*	,286**	-0,032	0,154	0,184	,370**	,322**	,460**	0,126	,230*	0,094	,274*	,245*	0,016	0,066
	5.1	-0,027	0,051	,256**	,224*	,293**	,240*	,300**	,378**	,310**	,286**	0,117	1,000	,408**	,396**	,374**	,338**	,322**	0,137	0,186	,357**	,205*	0,061	0,133	0,008	0,023	,226*	0,048	,224*	0,174	0,178
	5.2	-0,098	0,004	,202*	,312**	,381**	,297**	,328**	,272**	,451**	,272**	,388**	,408**	1,000	0,141	,236*	0,169	,202*	0,067	,324**	,246*	,379**	0,181	,269*	,223*	,261*	0,132	0,187	,282*	0,186	0,228
	5.3	0,060	0,061	,391**	,254*	,424**	,339**	,387**	,424**	,387**	,323**	,306**	,396**	0,141	1,000	,758**	,384**	,393**	0,152	,234*	,256*	0,151	,311**	,403**	0,137	,223*	,235*	,268*	,294**	,226*	,279*
	5.4	-0,055	0,025	,318**	,220*	,264**	0,192	,294**	,404**	,374**	,297**	,332**	,374**	,236*	,758**	1,000	,383**	,417**	0,124	,239*	,243*	0,200	,284**	,374**	0,185	0,212	0,155	,255*	,244*	0,189	0,227
	5.5	-0,028	0,038	,293**	,247*	,291**	,377**	,389**	,543**	,354**	,341**	,218*	,338**	0,169	,384**	,383**	1,000	,903**	0,140	0,143	,285**	0,112	0,177	,226*	,335**	,213*	,223*	,258*	,338**	0,165	,262*
	5.6	-0,048	0,050	,225*	,236*	,300**	,341**	,344**	,551**	,333**	,416**	,286**	,322**	,202*	,393**	,417**	,903**	1,000	0,137	0,148	,242*	0,106	0,165	,232*	,337**	,309**	0,179	0,187	,296**	0,043	0,182
	6.1	-0,001	-,243*	0,132	,265**	0,098	,356**	,201*	,280**	0,046	,240*	-0,032	0,137	0,067	0,152	0,124	0,140	0,137	1,000	,611**	,537**	,315**	0,153	0,059	0,199	0,004	0,030	0,138	,255*	0,168	0,117
	6.2	0,073	-,268*	,249*	,233*	,243*	,254*	,392**	,402**	,406**	0,121	0,154	0,186	,324**	,234*	,239*	0,143	0,148	,611**	1,000	,314**	,569**	0,193	,260*	0,164	,239*	0,201	,266*	,325**	0,213	,298*
	7.1	-0,089	0,016	0,152	,259**	,281**	,469**	,362**	,408**	,302**	,458**	0,184	,357**	,246*	,256*	,243*	,285**	,242*	,537**	,314**	1,000	,555**	,256*	,226*	,311**	0,085	0,069	0,164	,325**	,273*	0,136
	7.2	-0,116	-,208*	,250*	,301**	,346**	,322**	,430**	,230*	,408**	0,178	,370**	,205*	,379**	0,151	0,200	0,112	0,106	,315**	,569**	,555**	1,000	,250*	,259*	,287**	0,133	0,186	0,106	,241*	0,214	0,188
	8.1	-0,070	-0,021	,334**	,270**	0,191	0,155	,284**	,361**	,238*	0,169	,322**	0,061	0,181	,311**	,284**	0,177	0,165	0,153	0,193	,256*	,250*	1,000	,781**	,283**	,223*	,232*	,426**	,317**	,288**	,274*
	8.2	-0,089	-0,152	,351**	,285**	,244*	,224*	,398**	,396**	,423**	,312**	,460**	0,133	,269*	,403**	,374**	,226*	,232*	0,059	,260*	,226*	,259*	,781**	1,000	,334**	,357**	,361**	,381**	,498**	0,181	0,214
	9.1	-,210*	-0,028	,217*	0,149	0,010	,228*	,231*	0,178	,255*	,263**	0,126	0,008	,223*	0,137	0,185	,335**	,337**	0,199	0,164	,311**	,287**	,283**	,334**	1,000	,619**	0,114	0,150	,407**	0,167	0,044
	9.2	-0,053	-0,050	0,104	0,212	0,092	0,085	0,164	0,172	,284**	,258*	,230*	0,023	,261*	,223*	0,212	,213*	,309**	0,004	,239*	0,085	0,133	,223*	,357**	,619**	1,000	0,150	0,053	,431**	0,090	-0,016
	10.1	-0,064	0,074	,239*	0,178	0,098	-0,013	0,116	0,116	0,106	0,087	0,094	,226*	0,132	,235*	0,155	,223*	0,179	0,030	0,201	0,069	0,186	,232*	,361**	0,114	0,150	1,000	,414**	,366**	,435**	,344**
	11.1	0,183	0,065	,409**	0,139	,216*	0,074	,234*	,295**	0,205	0,198	,274*	0,048	0,187	,268*	,255*	,258*	0,187	0,138	,266*	0,164	0,106	,426**	,381**	0,150	0,053	,414**	1,000	,463**	,415**	,579**
	12.1	-0,046	-0,011	,466**	,470**	,220*	,326**	,287**	,431**	,327**	,365**	,245*	,224*	,282*	,294**	,244*	,338**	,296**	,255*	,325**	,325**	,241*	,317**	,498**	,407**	,431**	,366**	,463**	1,000	,450**	,515**
	12.2	-0,058	0,004	,380**	,259*	0,058	0,038	0,167	,269*	0,162	0,117	0,016	0,174	0,186	,226*	0,189	0,165	0,043	0,168	0,213	,273*	0,214	,288**	0,181	0,167	0,090	,435**	,415**	,450**	1,000	,575**
	13.1	0,228	0,202	,492**	0,145	,248*	0,104	0,191	,245*	0,154	0,097	0,066	0,178	0,228	,279*	0,227	,262*	0,182	0,117	,298*	0,136	0,188	,274*	0,214	0,044	-0,016	,344**	,579**	,515**	,575**	1,000

Summary

DEVSECOPS IMPLEMENTATION OPPORTUNITIES IN PUBLIC SECTOR ON THE EXAMPLE OF IT AND DEVELOPMENT CENTRE AT THE ESTONIAN MINISTRY OF INTERIOR

Einar Laagriküll, Ragner Paevere

With the raise of cyber threat and security focus in IT all over the world new cooperation method has emerged that helps to expand DevOps collaboration model to other disciplines. One such model, where security responsibility has been integrated into current development and operations teams is DevSecOps. (Raynaud, 2017) The main aim of this thesis was to explore DevSecOps implementation opportunities in public sector IT organization on the example of SMIT. Five subgoals were established to reach the goal.

Work consists of two parts. First theoretical part investigated DevSecOps nature and role, clarified CSF of the model and researched opportunities of the cooperation model in public sector. Based on theory in total 12 CSF were presented. Mainly they were related to culture, knowledge, and tools. Additionally, authors found that information flow, use of technology and funding are limiting factors that impact public sector when implementing DevSecOps. Furthermore, authors researched different change models and combined ADKAR model with DevSecOps CSF-s. When looking from the ADKAR change model perspective authors found that CFS are spread over different change phases.

Second chapter was empirical and clarified opportunities of improving SMIT operating model, both qualitative and quantitative methods were used. Survey was conducted among staff from two divisions in SMIT. Total population was 179 persons from 8 departments. Survey activity was 56,9%. In total 7 interviews were conducted. In the first phase of analysis authors conducted Kruskal-Wallis test to compare survey results. Additionally, correlation analysis was done to verify correlations among CSF. Also factor analysis was conducted to validate if CSF found would concentrate into factors. As a results four factors formed that are critical when implementing DevSecOps – cooperation, process, information movement and improvement orientation. Additionally, authors found that security knowledge plays important role and needs focus. Discovered results were analyzed based on ADKAR change process point of view. In the last phase means of found factors were compared with interview results and deviations were analyzed.

To successfully implement DevSecOps model it is important to pay attention to CSF in the change implementation process according to ADKAR phases. While implementing

new cooperation model in SMIT it is important to focus on information movement and process factors and on security knowledge. From information movement factor aspect information flow between staff and management needs to improve. In process side security automation, security and business metrics clarity and staff awareness needs attention. Security knowledge must be delt with systematic approach both on staff and management level. In change implementation at SMIT focus should be on ability and reinforcement phases. When implementing DevSecOps in public organization it is crucial to focus on found four factors and additionally pay attention to security knowledge. Furthermore, it is possible to use employee net promoter score to evaluate organizations readiness to change as it showed correlation with most of the questions formed to study CSF. From authors view further study is needed in the future to explore information movement factor as reliability of the factor across the result of analysis was low.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Meie, Einar Laagriküll ja Ragner Paevere,

anname Tartu Ülikoolile tasuta loa (lihtlitsentsi) meie loodud teose

DEVSECOPS TÖÖKORRALDUSE JUURUTAMISE VÕIMALUSED AVALIKUS SEKTORIS SISEMINISTEERIUMI INFOTEHNOLOOGIA- JA ARENDUSKESKUSE NÄITEL,

mille juhendajateks on

Eneli Kindsiko ja Helen Poltimäe,

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

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 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

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

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

Einar Laagriküll, Ragner Paevere
25.05.2021