

TARTU ÜLIKOOL

Majandusteaduskond

Merilyn Haugas

ÄRIKIRJAPETTUSTE TÕKESTAMINE TÖÖKORRALDUSLIKE MEETMETE
ABIL EESTI AVALIKU SEKTORI NÄITEL

Magistritöö

Juhendajad: Kristjan Pulk PhD, Heidi Reinson MSc

Tartu 2026

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

Kasutasin generatiivse tehisintellekti tööriistu ChatGPT (OpenAI), Claude (Anthropic) ja Microsoft Copilot abistava vahendina magistritöö struktuuri täpsustamisel ning kirjanduse ülevaate koostamise algfaasis materjali süstematiseerimisel. Töö sisuline osa, empiiriliste andmete kogumine, tulemuste tõlgendamine ja järeldused on minu koostatud.

Sisukord

Sissejuhatus.....	4
1. Teoreetiline raamistik	8
1.1. Ärikirjapettuse olemus ja areng küberkuritegevuses	8
1.2. Arvete menetlemise protsessi töökorralduslik käsitus ja haavatavused	13
1.3. Töökorralduslikud turvameetmed haavatavuste leevendamiseks	17
2. Empiiriline uuring.....	22
2.1. Ärikirjapettuste avaldumine ja käsitus Eestis	22
2.2. Uuringu metoodika ja andmekogumine.....	28
2.3. Uurimistulemused ja järeldused.....	31
Kokkuvõte.....	46
Viidatud allikad.....	49
Lisad.....	60
LISA A Kasutatud lühendid.....	60
LISA B Intervjuuküsimused	61
LISA C Intervjuuandmete kategoriseerimine ja kodeerimine	62
Summary	71

Sissejuhatus

Tehnoloogia kiire areng on viimastel aastakümnetel oluliselt muutnud nii ühiskonna toimimist kui majandustegevust. Digitaalne infrastruktuur on võimaldanud organisatsioonidel tegutseda senisest efektiivsemalt, toetades automatiseeritud töövooge, rahvusvahelist äritegevust ja reaalaajas toimuvat infovahetust ja tehinguid. Samal ajal on digitaliseerimine loonud uusi võimalusi ka kuritegevuseks, mis on üha enam küberruumi liikudes muutunud ulatuslikumaks ja raskemini tuvastatavaks. Küberkuritegevus on kujunenud üheks kiiremini kasvavamaks ja majanduslikult ulatuslike tagajärgedega kuritegevuse vormiks, mõjutades nii üksikisikuid, organisatsioone kui ka riike. INTERPOLi (2026) ülemaailmse kuritegevuse trendi raporti kohaselt on erinevad kuritegevuse vormid omavahel tihedalt seotud, kus tehnoloogia areng soodustab küberkuritegevust, küberkuritegevus võimaldab finantspettuste toimepanemist ja rahapesu võimaldab organiseeritud kuritegevusel oma tegevust rahastada.

Küberruumi areng on tihedalt seotud geopoliitiliste ja ühiskondlike protsessidega. Euroopa Liidu Nõukogu on nimetanud küberruumi viiendaks sõjapidamise valdkonnaks, mille roll on võrreldav traditsiooniliste tegevusruumidega, nagu maismaa, meri, õhuruum ja kosmos (Council of the European Union, n.d.). Riikidevahelises mõjutustegevuses kasutatakse üha enam digitaalset vahendeid strateegiliste eesmärkide saavutamiseks. Rahvusvahelist ohupilti seiravate ametiasutuste hinnangul on avalik sektor oma suure andmemahu ja strateegilise väärtuse tõttu küberkuritegevuse, eelkõige andmevarguse ja finantspettuste suhtes eriti haavatav. ENISA (2025b) andmetel oli avalik haldus 2024. aastal Euroopa Liidus kõige sagedamini rünnatav sektor, moodustades 38,2% kõigist tuvastatud intsidentidest. Küberintsidentide arvukuse, keerukuse ja tekitatud kahju kasv on tõstnud küberohud keskeks murekohaks kogu ühiskonnale.

Organisatsioonid jagavad avalikkusega teadlikult üha rohkem informatsiooni oma töötajate, struktuuri ja tegevuste kohta, eesmärgiga luua usaldusväarsust ning tugevdada sidet sihtrühmadega. Kaasaegne turundus ja kommunikatsioon, sealhulgas tööandja maine kujundamine, tuginevad sihtrühma mõistmisele ning teadlikult kujundatud sõnumitele, mille eesmärk on mõjutada hoiakuid ja käitumist. Paradoksaalsel kombel tuginevad samadel põhimõtetel ka sotsiaalse manipuleerimise (*social engineering*) rünnakud. Ründajad kohandavad oma sõnumeid vastavalt sihtmärgi rollile või organisatsioonilisele kontekstile, et psühholoogiliste mõjutusvõtete abil luua usaldust ning suunata ohvri otsuseid (Ferreira et al., 2020; Halevi et al., 2015; Khursheed et al., 2020). Paratamatult võib organisatsiooni enda kommunikatsioon tahtmatult kujuneda sisendiks sihitud rünnete ettevalmistamiseks. Seetõttu

on oluline käsitleda teabe avalikustamist riskijuhtimise osana ning hinnata teadlikult, millist teavet ja millises ulatuses on otstarbekas avalikult jagada.

Küberruumi olukorda kirjeldavate raportite järgi moodustavad organisatsioonide vastu suunatud õngitsusründed olulise osa küberkuritegevuse kogukahjust (Europol, 2023; 2025b; ENISA, 2025a). Kuritegevuse arengut iseloomustab viimastel aastatel liikumine massõngitsustelt üha enam sihitud ja personaliseeritud lähenemiste suunas. Sellised ründed ei tugine mitte tehnilistele haavatavustele, vaid töökorralduslikele ja käitumuslikele nõrkustele. Lähenemine võimaldab rünnetel sulanduda organisatsiooni tavapärasesse tegevusse ja igapäevasesse suhtlusesse, mistõttu on ründeid keeruline avastada. Nendele tunnustele vastab ka ärikirjapettus (*Business Email Compromise*), mis on kujunenud organisatsioonide jaoks üheks suurimat finantskahju põhjustavaks küberpettuse vormiks (Europol, 2023a; 2023b; FBI, 2026).

Käesolev magistritöö keskendub ärikirjapettuse alaliigile, arvepettusele, kus pettus realiseerub ostuarvete menetlemise protsessis makseandmete muutmise kaudu. Tegemist on organisatsioonide finantsprotsessi kuritarvitava pettuskeemiga, mille eripäraks on märkimisväärne finantskahju ning keerukas taastatavus, kuna pärast pettusliku makse teostamist liigub raha kiiresti edasi läbi mitme kanali. Uurimisfookuse kujunemist mõjutas ka autori professionaalne taust infoturbe valdkonnas, mis on andnud praktilise kogemuse sellest, kuidas tehnilised turvameetmed üksi ei suuda ennetada sotsiaalsel manipulatsioonil põhinevaid küberründeid, kui samal ajal võivad tööprotsessides esinevad nõrkused jääda märkamata.

Olemasolev teaduskirjandus on arvepettuste uurimisel valdavalt keskendunud tehnoloogilistele turvameetmetele, mille eesmärk on tuvastada pettuslik tegevus digitaalsete turbesüsteemide ja tarkvaralahenduste abil, ning psühholoogilistele aspektidele, mis selgitavad, kuidas kurjategijad mõjutavad inimeste otsustusprotsessi ja kasutavad ära käitumuslikke haavatavusi. Vähem tähelepanu on pööratud sellele, kuidas ostuarvete menetlemise ehk ostutehingute läbiviimiseks kujundatud protsessi ülesehitus ja töökorralduslikud kontrollimehhanismid aitavad pettuseid ennetada. Käesolevas töös käsitletakse töökorralduslike meetmetena organisatsiooni protsessides rakendatavaid juhtimise-, vastutuse jaotuse- ja rollipõhiseid tegevusi, mille eesmärk on tagada toimingute eesmärgipärane kulg ja kontrollitavus ning vähendada riskide realiseerumise tõenäosust. Vajalik on luua terviklik käsitus töökorralduslike meetmete olemusest ja ulatusest, mida organisatsioonid saavad arvepettuste tõkestamiseks praktikas rakendada. Piiratud on ka

varasemad empiirilised uuringud selle kohta, kuidas need kontrollimehhanismid reaalses tööprotsessis toimivad.

Magistritöös käsitletakse tehnoloogia arenguga seotud muutusi ja rahvusvahelisi ohutrende peamiselt konteksti loomiseks ning neid ei analüüsita detailselt töö põhisisu käsitlevates peatükkides. Magistritöö eesmärk on uurida, kuidas tööprotsessidega seotud haavatavused ja nende leevendamiseks rakendatud meetmed mõjutavad Eesti avaliku sektori organisatsioonide suutlikkust ennetada ja tuvastada ärikirjapettuseid. Uuringu põhjal selgitatakse välja, millised meetmed on selliste rünnete vastu kõige tõhusamad.

Tulemuse saavutamiseks püstitab autor järgmised uurimisülesanded:

- Käsitleda ärikirjapettust sotsiaalmanipulatsioonil põhineva küberpettusena, selgitades tehniliste, psühholoogiliste ja töökorralduslike tegurite rolli ründe toimimisel.
- Kaardistada arvete menetlemise protsessi ülesehitusest ja töökorralduslikest praktikatest tulenevad protsessilised haavatavused.
- Analüüsida töökorralduslike turvameetmete rolli ärikirjapettuste ennetamisel, varajasel tuvastamisel ja võimaliku kahju vähendamisel.
- Koguda ja süstematiseerida andmeid protsessiliste haavatavuste ning töökorralduslike turvameetmete kohta Eesti avaliku sektori organisatsioonide arvete menetlemise protsessis ning võrrelda neid käesolevas töös esitatud teoreetilise raamistikuga.
- Selgitada, kuidas uuritavates organisatsioonides rakendatud töökorralduslikud meetmed toetavad ärikirjapettuste ennetamist, tuvastamist ja võimaliku kahju vähendamist.
- Sõnastada soovitusel tööprotsessides rakendavate meetmete kohta, mis suurendavad organisatsioonide vastupidavust ärikirjapettustele.

Magistritöö algab laiemast probleemikäsitlest ja teoreetilise raamistiku avamisest ning liigub edasi empiirilise uuringu ja praktiliste järeldusteni. Töö esimene peatükk keskendub teemakohase kirjanduse süstemaatilisele ülevaatele. Allikate analüüsimisel kasutatakse nii teaduspublikatsioone kui ka teadusväliseid allikaid, sealhulgas valitsusasutuste ja rahvusvaheliste organisatsioonide aruandeid, poliitikadokumente ning konverentsi-ettekandeid. Täiendavate allikate kaasamine võimaldab käsitleda uurimisvaldkonda laiemalt ning tuua esile nii teoreetilised käsitlused kui praktilised kogemused valdkondades, kus teaduslikke väljaandeid on vähe.

Teoreetilise ülevaate koostamisel lähtub autor töö alguses püstitatud kolmest esimesest uurimisülesandest. Peatüki alguses avatakse ärikirjapettuse teoreetilisi lähtekohti, käsitledes tehniliste, psühholoogiliste ja töökorralduslike tegurite rolli ründe toimimisel. Seejärel analüüsitakse varasemate uurimuste põhjal tuvastatud arvete menetlemise protsessi haavatavusi ning nendega seotud töökorralduslikke eripärasid, mis loovad eeldused ärikirjapettuste realiseerumiseks. Viimases alapeatükis käsitletakse töökorralduslikke turvameetmeid, sidudes tuvastatud haavatavused neid leevendavate meetmetega ning kujundades käesoleva töö aluseks oleva teoreetilise raamistiku.

Töö teises peatükis otsib autor empiirilise uuringu abil vastuseid töö alguses püstitatud eesmärgile ning kolmele viimasele uurimisülesandele. Esimese alapeatüki eesmärk on kirjeldada ärikirjapettuste vastast võitlust Eesti kontekstis, andes ülevaate toimunud intsidentidest ning neid käsitlevate organisatsioonide praktikatest. Teises alapeatükis kirjeldatakse magistritöö uuringu valimit ja andmekogumisprotsessi. Uuring keskendub kahe avaliku sektori organisatsiooni ostuarvete menetlemise protsessi kaardistamisele, et tuvastada protsessilised haavatavused ning neid tõhusalt leevendavad praktikas rakendatud töökorralduslikud turvameetmed. Analüüsi käigus selgitatakse, millised protsessietapid ja töökorralduslikud toimingud või nende tegemata jätmine võivad soodustada pettuste õnnestumist ning kuidas organisatsioonides rakendatud meetmed toetavad pettuste tõhusat avastamist ja tõkestamist. Empiirilised tulemused esitatakse teise peatüki kolmandas alapeatükis, kus võrreldakse organisatsioonide tegelikke praktikaid töö esimeses peatükis esitatud teoreetilise raamistikuga. Selle põhjal sõnastatakse soovitusel, mida on võimalik rakendada ka teistes organisatsioonides ärikirjapettuste varajaseks tuvastamiseks ja nende mõju leevendamiseks.

Magistritöö autor tänab siiralt oma juhendajaid Kristjan Pulka ja Heidi Reinsoni, kelle väärtuslikud soovitusel, sisukas tagasiside ja toetav suhtumine olid suureks abiks kogu magistritöö valmimise protsessi jooksul. Eriline tänu seisneb ka huvitava ja olulise uurimisteema soovitamisel ning motivatsiooni hoidmisel töö kirjutamise vältel. Autor tänab ka retsensenti Meelis Milderit selge ja edasiviiva tagasiside ning vastutuleliku suhtumise eest. Autor on tänulik kõikidele intervjueeritavatele Riigi Tugiteenuste keskusest ja Riigi IT keskusest, kes leidsid aega, et jagada oma teadmisi, kogemusi ja praktilisi tähelepanekuid.

Märksõnad: Küberturvalisus, Sotsiaalne manipuleerimine, Ärikirjapettus, Arvepettus, Haavatavus, Turvameede

Teaduseriala kood (CERCS): S190 Ettevõtete juhtimine

1. Teoreetiline raamistik

1.1. Ärikirjapettuse olemus ja areng küberkuritegevuses

Digitaalsete tehnoloogiate laialdane kasutuselevõtt on suurendanud ühiskonna toimimise efektiivsust ja ühenduvust. Samal ajal on loonud ka uusi võimalusi kuritegevuseks, mis kasutab ära digikeskkonna eripärasid, sealhulgas anonüümsust, kiirust ja rahvusvahelisust. Tehnoloogilise arengu olulise suunana on esile toodud tehisintellektil põhinevate tööriistade ja suurte keelemudelite laialdane kasutuselevõtt, võimaldades luua veenvaid identiteete, automatiseerida ründe protsesse ning kasutada ära haavatavusi enne, kui organisatsioonid jõuavad neile reageerida (Europol, 2025b; ENISA, 2025b; INTERPOL, 2026; FATF, 2026; RIA, 2026). Küberkuritegevus on viimastel aastakümnetel kujunenud üheks olulisemaks majanduskuritegevuse vormiks. Maailmapanga 2024. aastal koostatud analüüsi järgi on tekitatud kahju majanduslikku ulatust keeruline täpselt hinnata, kuna küberintsidentide hiline avastamine, alaraporteerimine, ebapiisav statistika ning ühtse meetodika puudumine takistavad usaldusväärsete hinnangute kujundamist (Vergara Cobos & Cakir, 2024). Euroopa Keskpanka ja Euroopa Pangandusjärelevalve Asutuse 2025. aasta maksepettuste raportis on toodud, et 2024. aastal oli Euroopa Majanduspiirkonnas raporteeritud pettuslike ülekannete kogukahju suurus 2,5 miljardit eurot (ECB & EBA, 2025). Seejuures on pettuseid nimetatud üheks enim levinumaks rahapesu eelkuriteoks (FATF, 2026; RAM, 2025).

Majandustegevus on muutunud üha rahvusvahelisemaks ning organisatsioonid tegutsevad tarneahelates, kus erinevad protsessid ja süsteemid on omavahel tihedalt seotud. Digitaalsed lahendused ja elektrooniline suhtlus võimaldavad tõhusat koostööd, kuid suurendavad samal ajal sõltuvust ka välistest teenustest ja IT-süsteemidest. Sellises keskkonnas ei pruugi organisatsioonidel olla täielikku kontrolli kogu protsessi toimimise üle, eriti olukordades, kus erinevad tegevused on jaotunud mitme osapoole vahel. Tarneahela keerukuse tõttu võivad ühe lüli nõrkused mõjutada kogu protsessi toimimist ning avalduda erinevates etappides, alates tehnilistest lahendustest kuni igapäevaste tööprotsessideni (OECD, 2026). Eesti avalikus sektoris sõltuvad paljud riigiasutused riigiülestest keskselt hallatavatest IT- ja tugiteenustest, mistõttu võib ühe teenusepakkuja ründamise mõju ulatuda korraga paljude asutusteni. ENISA (2025b) toob näitena 2024. juhtumi, kus küberrünnak Rootsis asuva IT-teenusepakkuja andmekeskuse vastu põhjustas ulatuslikke katkestusi ligikaudu 120 riigiasutuse ja omavalitsuse palga- ning juhtimissüsteemidele.

Küberkuritegevus hõlmab kuritegusid, mille toimepanemisel kasutatakse arvuteid, võrke või muid digitaalseid tehnoloogiaid kas vahendina või sihtmärgina. Eristatakse kahte peamist kategooriat (United Nations Office on Drugs and Crime, UNODC, 2022):

1. Tehnoloogia abil toime pandud kuriteod (*cyber-enabled crime*) – tehnoloegiat kasutatakse traditsiooniliste kuritegude toimepanemiseks, näiteks vargus ja identiteedipettus.
2. Tehnoloogial põhinevad kuriteod (*cyber-dependent crime*) – kuritegu, mida saab toime panna ainult digitaalse keskkonna kaudu, mistõttu on tehnoloogia nii kuriteo sooritamise vahendiks kui ka sihtmärgiks. Näiteks pahavara levitamine ja teenusetõkestusrünne (*distributed denial-of-service* ehk DDoS).

Eesti küberturvalisuse keskusena tegutseva RIA iga-aastase *Küberturvalisuse aastaraamatu* andmetel on organisatsioonide poolt raporteeritud mõjuga küberintsidentide arv Eestis kahe aastaga kolmekordistunud, kasvades 2023. aasta 3314 intsidendilt 2025. aastaks 10 185 intsidendini (RIA, 2026). Küberturvalisuse seaduse (edaspidi KüTS) kohaselt mõistetakse küberintsidendi all võrgu- ja infosüsteemis toimuvat sündmust, mis võib ohustada või on juba kahjustanud süsteemi turvalisust. Mõjuga küberintsidendina käsitletakse juhtumit, mille tagajärjel on häiritud teenuse toimepidevus, lekkinud tundlikud andmed või tekkinud rahaline kahju. (KüTS, 2018) Rünnete edukus ei sõltu üksnes tehnilistest haavatavustest, vaid ka organisatoorsete protsesside ja käitumuslike tegurite nõrkustest, mida ründajad ära kasutavad (Abbas & Michael, 2026; Almutairi et al., 2025b; Cidon et al., 2019; Václavík et al., 2025). RIA praktikud on *Küberturvalisuse aastaraamatus* tõdenud, et tõhus küberturvalisus sõltub sellest, kuidas on lisaks tehnoloogilistele lahendustele kujundatud tööprotsesside ülesehitus, vastutuse jaotus ja tagatud töötajate teadlikkus (RIA, 2026).

Märkimisväärne osa küberrünnetest tugineb sotsiaalsel manipulatsioonil (*social engineering*), kus psühholoogiliste mõjutusvõtete kaudu suunatakse inimest sooritama tegevusi, mida ta ratsionaalselt ei teeks (Cybernetica, n.d.-a; Modic & Lea, 2013; Sethuraman et al., 2024). Psühholoogilist vastuvõtlikkust küberpettustele aitab selgitada kahe protsessi teooria (*dual process theory*), mille kohaselt eristatakse kiiret, automaatset ja heuristikatel ehk vaimsetel rusikareeglitel põhinevat süsteem 1 mõtlemist aeglasest, teadlikust ja analüütilisest süsteem 2 mõtlemisest (Evans, 2008; Kahneman, 2011). Sotsiaalsel manipulatsioonil põhinevate rünnete puhul kasutatakse mõjutusvõtteid nagu ajalise surve tekitamine, emotsionaalse reaktsiooni esilekutsumine ning usaldusväärse osapoolle kehtastamine (Abroshan et al., 2018; Goel et al., 2017; Buse et al., 2023; Pan et al., 2026; Vishwanath et al., 2011; Václavík et al., 2025; Zakari et al., 2026). Heuristikad, näiteks

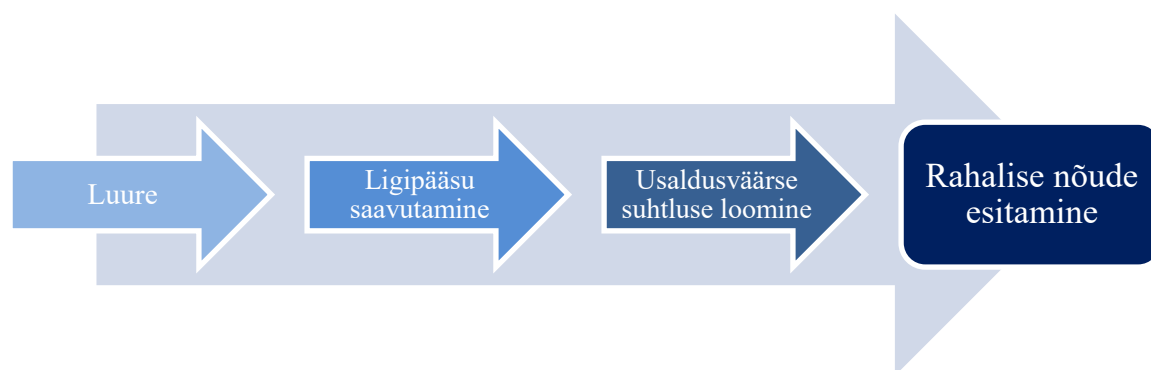
autoriteedile allumine ja tajutud usaldusväärsusele tuginemine on eriti mõjusad olukordades, kus tähelepanu on killustunud (Iuga et al., 2016; Jones et al., 2019). Neid tähelepanekuid toetavad ka Cialdini (2007) mõjutsprintsiihid, mille kohaselt suurendavad kiireloomulisus, autoriteetsus, kohustumus, järjekindlus, meeldivus ja sotsiaalne tõendus märkimisväärselt tõenäosust, et ohvri otsustusprotsessi õnnestub mõjutada (Agrafiotis et al., 2018; Bera et al., 2023; Button & Cross, 2017; Goel et al., 2017; Modic & Lea, 2013; Pan et al., 2026).

Õngitsemist (*phishing*) nimetatakse peamiseks ründevektoriks, kuna inimkäitumise mõjutamine on ründajate jaoks tõhus strateegia, mille kaudu realiseerub suur osa sotsiaalse manipulatsiooni rünnetest (ENISA, 2025; Europol, 2025a; FBI, 2025; Thomas, 2018; Václavík et al., 2025). Tegemist on elektroonilises suhtluses toimuva pettusega, mille abil püüab ründaja saada ohvritl tundlikku teavet (Cybernetica, n.d.-b). Viimastel aastatel on märgatavalt kasvanud sihitud küberrünnete osakaal, mille puhul sõnumid kujundatakse konkreetse sihtmärgi – kas isiku või organisatsiooni – konteksti arvestades. Selline lähenemine suurendab ründajate usutavust ja ründe õnnestumise tõenäosus. Bera et al. (2023) ja Halevi et al. (2015) leidsid, et sihitud rünnete puhul kasutatakse mõjutusvõtetena tugeva emotsionaalse reaktsiooni esilekutsumist (nt hirm, ahnus), identiteedi jäljendamist ja personaliseeritud pöördumist.

Üheks levinumaks sihitud ründe vormiks on ärikirjapettus (*Business Email Compromise, BEC*), mille korral kasutavad ründajad e-posti, kui organisatsioonide igapäevases suhtluses kasutatavat töövahendit. Ründaja edastab ohvrile e-kirja, esinedes tema jaoks usaldusväärse osapoolena eesmärgiga suunata finantstehinguid või saada ligipääs tundlikule teabele (FBI, n.d.-a). Pettuse edukus põhineb otsustusprotsessi mõjutamisel ning organisatoorsete haavatavuste ärakasutamisel, kus pahatahtlik sekkumine on integreeritud organisatsiooni tavapärastrasse töövoogudesse, mistõttu ei ole pettuse keskmes üksnes inimene, vaid ka töökorralduslikud protsessid (Almutairi et al., 2025a, 2025b; Khursheed et al., 2020; Myojin & Babaguchi, 2020; Václavík et al., 2025).

Ärikirjapettus hõlmab mitmeid erinevaid skeemitüüpe, millest Riigi Infosüsteemi Ameti andmetel on Eestis levinumad tegevjuhi nimel esitatavad kiireloomulised maksenõuded ning tarnijatega seotud arvepettused (PM Majandus, 2025; RIA, 2024b). Käesoleva magistr töö fookuses on tarnijapettuse skeem, mille käigus ründaja kompromiteerib või jäljendab teenusepakkuja e-posti kontot ning edastab ohvrile muudetud pangakonto andmetega arve. Ründe elutsükkel on järjestikune, millest iga etapp loob eelduse järgmise edukaks realiseerimiseks (Joonis 1). Ründeks valmistumine algab luuretegevusest,

kus kogutakse teavet sihtmärgiks oleva asutuse struktuuri ja rollide, töövoogude ja partnerite kohta. Järgneb ligipääsu saavutamine kas läbi konto kompromiteerimise või usaldusväärse identiteedi tehnilise jäljendamise. Seejärel toimub usaldusväärse suhtluskonteksti loomine, millele järgneb eesmärgi täitmise ehk soovitud nõude esitamine. (Al-Musib et al., 2023; Almutairi et al., 2025a, 2025b; Atlam & Oluwatimilehin, 2023; Bonhard et al., 2025; Kroll, n.d.; Myojin & Babaguchi, 2020).



Joonis 1. Ärikirjapettuse elutsükkel

Allikas: Autori koostatud, tuginedes allikatele Al-Musib et al., 2023; Almutairi et al., 2025a, 2025b; Atlam & Oluwatimilehin, 2023; Bonhard et al., 2025; Kroll, n.d.; Myojin & Babaguchi, 2020.

Sihtmärgi valimisel võib rolli mängida organisatsiooni suurus, kuna see loob eelduse esitada võimalikult suures summas arve. Ogwo-Ude et al. (2023) leidsid Ameerika Ühendriikides läbi viidud uurimusega, et keskmised ja suured ettevõtted oma protsessilise keerukuse, laiema ründepinna, rahvusvaheliste tarneahelate ja suuremate rahavoogude tõttu eriti haavatavad. Junger et al. (2020) uuringu põhjal esineb tegevjuhi pettust rohkem suurtes ja väga suurtes organisatsioonides (100–250 ja rohkem). Väikestele (kuni 49 töötajat) organisatsioonidele esitatakse sagedamini pettuslikke arveid.

Ärikirjapettuse rünne ei eelda pahavara kasutamist, mis muudab pettuse läbiviimise ründaja seisukohalt tehniliseks lihtsaks. Organisatsioonides kasutatavad turbelahendused ja e-posti autentimisprotokollid võivad vähendada pettuslike sõnumite jõudmist töötajateni, kuid nende tõhusus on piiratud olukordades, kus ründaja kasutab kompromiteeritud kontot või oskuslikult jäljendab usaldusväärset suhtlustrit (Cidon et al., 2019; Khursheed et al., 2020; Sethuraman et al., 2024). Ründeid on keeruline tuvastada, kuna jätavad mulje tavapärasest tegevusest, mis võib jääda tehnoloogilistele turvamehhanismidele märkamatuks. (Al-Musib et al., 2023; Almutairi et al., 2025a, 2025b; Atlam & Oluwatimilehin, 2023; Bonhard et al., 2025; Cidon et al., 2019; Václavík et al., 2025; Zakari et al., 2026) Sageli ei

avastata ründeid hetkeni, kuni finantskahju on juba realiseerunud. Välja petetud raha tagasi saamine on keeruline, kuna maksed suunatakse läbi välisriigi kontode edasi, sageli krüptorahasse (Lazarus, 2025). Krüptovaluuta on krüptograafial põhinev digitaalraha, mida kuritegevuses eelistatakse selle detsentraliseerituse ja tehingukiiruse tõttu (FBI, 2022). Pettusele järgneb organiseeritud kuritegevusele omane rahapesu, mis võimaldab ebaseaduslikult saadud raha päritolu varjata (FBI, 2022; Lazarus, 2025). Rahapesu toimib Europoli (2023) ja Eurojusti (2025) andmetel ulatuslikult legaalse organisatsioonide ja nende töötajate kaudu, mida kinnitab ka Lazaruse (2025) uuring, mis põhines ärikirjapettustega seotud kuritegeliku võrgustiku võtmeisiku intervjuerimisel.

Küberkuritegevuse vastu võitlevad eri riikide õiguskaitse- ja julgeolekuasutused tegelevad sageli samade kuritegelike võrgustike sihtimisega, mistõttu on riikidevaheline koostöö kriminaalse tegevuse tõhusaks tuvastamiseks ja tõkestamiseks vältimatu. Efektiivsuse tagamiseks ja koostöö sujumiseks ja on loodud mitmeid rahvusvahelisi õiguslikke kokkuleppeid, näiteks Arvutikuritegevusvastane konventsioon (nimetatakse ka Budapesti konventsioon) (Council of Europe, 2001) ja Ühinenud Rahvaste Organisatsiooni küberkuritegevuse vastane konventsioon (United Nations, 2024)

FBI IC3 (2025) andmetel moodustasid ärikirjapettused 2024. aastal 3,2% kõigist registreeritud küberkuritegevuse kaebustest ning 14,6% kogu raporteeritud rahalisest kahjust, mistõttu nimetatakse seda üheks peamiseks küberohuks organisatsioonide finantsturvalisusele (ENISA, 2024; Europol, 2025a). Selline asümeetriline suhe illustreerib ärikirjapettuse eripära: sihitud ja kõrge finantskahjuga rünne, kus ühe juhtumi keskmine kahju ületab märkimisväärselt teiste küberkuritegude keskmist kahju, ulatudes ligikaudu 123 000 USA dollarini juhtumi kohta (autori arvutus tuginedes FBI IC3, 2025 andmetele).

Finantskahju on ärikirjapettuse kõige otsesemalt mõõdetav tagajärg, kuid lisaks finantskahjule avaldub ründe negatiivne mõju ka mainekahjuna, kuna kahjustuda võivad suhted nii klientide kui koostööpartneritega (Agrafiotis et al., 2018; Ogwo-Ude et al., 2023). Võimalik mainekahju võib olla üks tegureid, mis vähendab organisatsioonide valmisolekut toimunud juhtumeid raporteerida. Viimastel aastatel on üha enam tähelepanu pööratud ka pettuse ohvri psühholoogilisele mõjule. Uuringud näitavad, et õngitsuspettuste ohvrid kogevad sageli süü- ja häbitunnet ning enesehinnangu langust (Buse et al., 2023; Button & Cross, 2017; Legarda & Nabe, 2026). Lisaks on kirjanduses esile toodud ka protsesside ja töövoogude katkestuste (Ogwo-Ude et al., 2023) ja tehnoloogiliste häiretega

organisatsioonile kaasnevat negatiivset mõju, samuti sotsiaalseid ja ühiskondlikke tagajärgi (Agrafiotis et al., 2018).

Ärikirjapettust käsitletakse ühe kulukama küberkuritegevuse vormina, mille ohvrite hulka kuuluvad mitmed rahvusvaheliselt tuntud organisatsioonid. Sellest tulenevalt on ärikirjapettuste kui suure mõjuga küberpettuse vormi tõhusate leevendusmeetmete tuvastamine käesoleva magistritöö keskne eesmärk. Järgmises alapeatükis analüüsitakse ostuarvete käsitlemisest tulenevaid protsessilisi haavatavusi, mis võivad selliste pettuste õnnestumist mõjutada.

1.2. Arvete menetlemise protsessi töökorralduslik käsitus ja haavatavused

Eelmises alapeatükis käsitleti ärikirjapettuse olemust ning selle toimemehhanisme, keskendudes tehnilistele ja psühholoogilistele teguritele, mille abil ründajad mõjutavad ohvri otsuseid. Käesolev alapeatükk suunab fookuse organisatsiooni sisemistele protsessidele, keskendudes ostuarvete menetlemisele kui finantsarvestuse olulisele komponendile. Esmalt kirjeldatakse protsessi töökorralduslikku ülesehitust ning seejärel analüüsitakse haavatavusi, mis võivad luua eeldused pettuste õnnestumiseks.

Ostuarvete menetlemine on finantsarvestuse alla kuuluv protsess, mille kaudu dokumenteeritakse ja kontrollitakse majandustehingud ning valmistatakse ette nende kajastamine ja tasumine (Raamatupidamise seadus, 2025). Protsessi saab üldistatult käsitleda kolme peamise etapina (Avaliku sektori finantsarvestuse ja -aruandluse juhend, 2025):

1. Arve vastuvõtmine ja registreerimine;
2. Sisuline kontroll ja kinnitamine;
3. Makse teostamine.

Arvete käsitlemiseks on organisatsioonides kasutusel erinevad lahendused. Üha enam on levinud jagatud teenuste keskuste mudel (*Shared Service Centre*, SSC), kus finantsarvestus on tsentraliseeritud ühte organisatsiooni, mis teenindab erinevaid asutusi. SSC mudeli peamiste eelistena tuuakse esile protsesside standardiseerimise kaudu saavutatav kulude vähenemine, mis tuleneb mastaabisäästust. Lisaks võimaldab selline korraldus koondada valdkonnapõhist kompetentsi (Joha & Jannsen, 2011; Seal & Herbert, 2013) ning suurendada aruandluse läbipaistvust (Dong et al, 2025). Zaporowska & Szczepański (2024) on negatiivse aspektina tähelepanu juhtinud standardiseerimisega kaasnevale nõrgemale riskitajule ja organisatsioonide aktiivse riskijuhtimise puudumisele. Varasemates uuringutes on nii kui Herbert & Seal (2011), Raudla & Tammel (2015), kui Xiwen et al. (2021) näidanud, et jagatud teenuste keskustes on oht rollide ebamäärasuse ning vastutuse hajumise

tekkeks. Samuti võivad protsessid muutuda rutiinseks ning erandlikud olukorrad ei pruugi saada piisavat tähelepanu. Seega ei pruugi protsessi tugevdamine ühes osas kõrvalda riski tervikuna, seejuures võib oht esineda ka teistes, vähem reguleeritud etappides. Arvete menetlemise kontekstis tähendab see, et tõhusad turvameetmed makse menetlemise faasis võivad vähendada pettuse tõenäosust olemasolevas etapis, kuid samal ajal säilitada ründe esinemise tõenäosuse varasemates etappides, kus teostatakse sisulist kontrolli. Järgnevalt kirjeldatakse töö autori poolt varasemate uurimustest tuvastatud peamisi ostuarvete menetlemise protsessiga seotud töökorralduslikke haavatavusi, mis võivad mõjutada ärikirjapettuste õnnestumise tõenäosust.

Esimeseks oluliseks ohukohaks on olemasoleva kirjavahetuse usaldamine. Uuringud näitavad, et ärikirjapettuste puhul on määrava tähtsusega ründele eelnev luuretegevus, mille käigus kogutakse teavet suhtlusmustrite, rollide ja tööprotsesside kohta. Ründajad võivad jälgida kirjavahetust ning oodata sobivat hetke protsessi manipuleerimiseks. (Bonhard et al., 2025; Lazarus, 2025; Václavík et al., 2025) Laialt levinud on avaliku teabe põhine luuramine, mille korral ründajad kasutavad veebilehti, sotsiaalmeediat, ajakirjandust ning muid allikaid, mis võimaldavad kaardistada organisatsioonide tööprotsesse ja otsustusahelaid, luues eeldused usutavate ja kontekstipõhiste petuskeemide väljatöötamiseks (Atlam & Oluwatimilehin, 2023; Al-Musib et al., 2023; Europol, 2025b). Vastuolu muutub eriti oluliseks olukordades, kus organisatsioonid peavad samaaegselt tagama läbipaistvuse, efektiivsuse ja turvalisuse. Avalikus sektoris, kus ühiskondlik ootus avatusele ja informatsiooni kättesaadavusele on kõrgem, võib ulatuslik teabe avalikustamine küll toetada usaldusväärset ja vastutust, kuid samal ajal pakkuda väärtuslikku sisendit tööprotsesside ja võtmeisikute kaardistamiseks.

Teiseks haavatavuseks on rollide kattumine. Olukorras, kus sama töötaja vastutab nii arve kinnitamise kui ka makse teostamise eest, kaasneb suurem tõenäosus, et pettuslik tehing võib jääda märkamata. Kui protsessi erinevate etappide eest vastutajad ei ole selgelt määratletud, võib kahtluse korral jääda ebaselgeks, kelle ülesanne on kontrolli teostamine. (Václavík et al., 2025) Unatrac Holding juhtum, kus ettevõtte kaotas ligikaudu 11 miljonit dollarit arvepettustele, illustreerib kohustuste lahususe puudumise tagajärgi (United States Department of Justice, 2019). Sama kinnitas Tecnimont SpA juhtum, kus India üksuse juhti peteti Itaalia tegevjuhti imiteerivate e-kirjade ja professionaalselt lavastatud võltskonverentskõnede abil, mille tulemusel maksti kurjategijate arvelduskontodele 18,6 miljonit dollarit (Dave, 2019).

Kolmandaks teguriks on verifitseerimise nõrkused makseandmete muutuste, eelkõige pangakonto uuendamise korral. Organisatsioonides võib puududa protseduur, mis kohustaks muudatusi kinnitama alternatiivse suhtluskanali kaudu. Selleks saab kasutada näiteks lepingus märgitud kontaktisiku või mõne teise organisatsiooni usaldusväärse töötajaga ühenduse võtmist, arve saatjale helistamist, veebikõne läbiviimist või alternatiivseid tööalase suhtluse kanaleid, näiteks Microsoft Teams rakendust. Topeltkontrolli puudumine võib muuta organisatsiooni eriti haavatavaks olukorras, kus ründajal on õnnestunud luua usutav suhtluskontekst ning esitada makseandmete muutmise palve loogilisena näiva põhjendusega. (Almutairi et al., 2025b). Václavík et al. (2025) kirjeldavad Tšehhi teadusseadmete tootmisettevõttes kuue aasta jooksul kaks korda aset leidnud ärikirjapettuse juhtumeid, milles mõlemal korral oli rahaliseks kannatajaks koostööpartner – esimeses juhtumis Singapuris asuv edasimüüja, kelle e-postikonto oli ründaja poolt kompromiteeritud, ning teises juhtumis Euroopa ülikool, kes langes võltsdomeeni abil esitatud „parandatud arve“ ohvriks. Teise juhtumi puhul õnnestus ülikooli pangal ülekanne peatada ja raha tagasi saada, kuid mõlemad juhtumid näitasid, et ründajad kasutasid ära tootja ja partneri vahelist usalduspõhist suhtlust ning reguleerimata makseandmete verifitseerimise protsessi.

Neljanda aspektina võib haavatavuste realiseerumise tõenäosust mõjutada usaldusväärse isiku identiteedi võltsimine. Levinumad jäljendamise tehnikad on sarnase domeeniga e-posti aadressi kasutamine, saatja nime võltsimine, vastusaadressi (*reply-to*) muutmine ning e-posti konto tehniline kompromiteerimine (Almutairi et al., 2025a; Cidon et al., 2019; Myojin & Babaguchi, 2020; Zakari et al., 2026). Sethuraman et al. (2024) kirjeldavad, et sarnase domeeniga e-posti aadresside kasutamine võib olla tõhus taktika, mis petab erinevate vanuserühmade esindajaid, kuna sageli inimesed ei kontrolli saatja e-posti aadressi. Probleemi süvendavad ka domeenide konfigureerimisvead, mille tõttu jäävad rakendamata vajalikud autentimismehhanismid e-posti aadresside võltsimise ennetamiseks (Bonhard et al., 2025; Ogwo-Ude et al., 2023; Sethuraman et al., 2024). Lazarus (2025) kirjeldab, kuidas küberkuritegevuse võrgustikud uurivad hoolikalt suhtlusmustreid ja rollijaotust ning kompromiteerivad just need kontod, mille kaudu toimub rutiinne kirjavahetus. Sellisel juhul toimib arvete menetlemine organisatsiooni jaoks tavapärasel viisil, kuna sõnumi saatja on tuttav ning identiteedis kahtlemiseks puudub põhjus. Sarnast mustrit kirjeldavad ka Almutairi et al. (2025a) oma esimeses juhtumiuuringus, kus ründaja sai mitmeks nädalaks ligipääsu heategevusorganisatsiooni finantsjuhi e-posti kontole ning tegutses pikalt märkamata, jälgides suhtlust ning ümber seadistades e-posti reegleid, mis

peitsid sissetulevaid kirju. Sobival hetkel edastati finantsjuhile koostööpartneri poolt saadetud arve, mille makseandmed olid protsessi käigus ründaja poolt muudetud. Pettus jäi töötajatele märkamatuks, kuna tegevus vastas tavapärasele suhtlusele ja töökorraldusele.

Myojin ja Babaguchi (2020) analüüsitud arvepettuse juhtum hõlmas mitmeid eelnevalt kirjeldatud haavatavusi, mille abil mõjutati ründaja poolt ohvri otsustusprotsessi järk-järgult. Esmalt jälgiti osapoolte vahelist e-kirjavahetust ning vahetult pärast ametliku arve edastamist saadeti võltsitud domeenilt muudetud makseandmetega arve, mida põhjendati paranduse vajadusega. Seejärel saadeti makseandmete muudatuse kinnitus juba kompromiteeritud e-posti kontolt. Ründaja suutis sekkuda olemasolevasse tööprotsessi viisil, mis muutis sõnumid usutavaks ega tekitanud ohvris vajadust muudatust alternatiivse kanali kaudu üle kontrollida. Juhtum illustreerib, kuidas ühes ründes võivad samaaegselt esineda identiteedi jäljendamine ja domeeni võltsimine, konto tehniline kompromiteerimine ning pettusele eelnev luuretegevus. Samuti näitab intsident, et ründe õnnestumisele võivad kaasa aidata organisatsiooni verifitseerimisprotsessi puudused ja ebapiisav ülesannete lahusus.

Suur töökoormus võib samuti vähendada arvete menetlusprotsessi turvalisust, kuna ajasurve korras tähelepanu hajub ning otsused hakkavad rohkem tuginema rutiinsetele tegevustele (Iuga et al., 2016; Vishwanath et al., 2011). Ründajad kujundavad sõnumid viisil, mis tekitab kiireloomulisust ja suunab ohvrit otsust langetama kiirustades. Junger et al. (2020) viitavad ka hooajalisuse mõjule, leides, et tegevjuhi nimel toime pandud pettused sagenevad suvel, mil juhi kättesaadavus täiendava kinnituse saamiseks võib olla piiratud. Samas tasuti uuringu andmetel tarnija nimel esitatud petuarve eest ligikaudu viis korda madalama tõenäosusega kui ülejäänud aastaaegadel. See-eest edastatakse võltsarveid enim kevadel, mis on raamatupidajate jaoks tipphooaeg. Seega on protsesside disainimisel oluline arvestada, et töötajate koormuse kõrgpunktides võib olla nende võimekus pettuse tuvastamiseks madalam.

Arvete menetlemise haavatavuste avaldumist ei mõjuta üksnes töökorraldus ja protsesside ülesehitus, vaid ka see, kuidas töötajad olukordi tajuvad ja otsuseid vastu võtavad. Otsuste langetamine võib välja kujuneda igapäevaste tööpraktikate ja varasemate kogemuste põhjal. Ohtude märkamist võib mõjutada ka rünnete haruldus. Harva esinevate olukordade puhul võib kujuneda kognitiivne pimedus, mille puhul on töötajate tähelepanu suunatud eelkõige tavapärasele ja sagedamini esinevatele probleemidele. Olukordades, kus IT-süsteemid on pikaajaliselt olnud töökindlad, võib kujuneda tajutud turvalisus ja arusaam, et süsteem tuvastab vea, mis vähendab tähelepanu mitte-tehniliste ohumärkidele. (Ogwo-Ude et

al., 2023; Schneier, 2008; Vaughan, 1996) Kõrge turvalisuse tajumine võib soodustada ka liigse enesekindluse nihke (*overconfidence bias*) esinemist (Halevi et al., 2015; Iuga et al., 2016; Modic & Lea, 2013; Schneier, 2008). Greulich et al. (2024) on leidnud, et just tehniliselt võimekates organisatsioonides võib kujuneda arusaam, et igasugune risk on piisavalt leevendatud, mis omakorda vähendab tähelepanu käitumuslike kõrvalekallete suhtes. Seetõttu võivad muutused suhtluse toonis ja kirja pildis jääda märkamata. Arvepettuste õnnestumine ei pruugi olla seotud üksnes turvameetmete ebapiisavusega, vaid ka sellega, kuidas töötajad olemasolevaid ohusignaale tõlgendavad ja millistele aspektidele tähelepanu suunavad.

Käesolevas töös ei käsitleta kognitiivseid nihkeid iseseisvate haavatavustena, vaid teguritena, mis võivad mõjutada protsessiliste haavatavuste avaldumist. Seetõttu tuleb arvete menetlusprotsessi turvalisust hinnata mitte üksnes turvameetmete olemasolu, vaid ka rakendumise piirangutega kogu protsessi vältel, mille tagajärjel võivad otsused kujuneda usaldusel ja väljakujunenud rutiinidel. Seetõttu on vajalik mõista tuvastatud haavatavuste ja töökorralduslike turvameetmete vahelist vastastikust seost ning kontrollimehhanismide toimivust vastupanuvõime tagamisel. Järgnev alapeatükk peatükk keskendub nende seoste analüüsile.

1.3. Töökorralduslikud turvameetmed haavatavuste leevendamiseks

Elmises alapeatükis käsitleti ostuarvete menetlemise protsessis esinevaid haavatavusi ning toodi esile, et arvepettuste tõkestamine oleneb kontrollimehhanismide tõhususest otsustusahela erinevates etappides. Selgus, et olulised haavatavused kujunevad olukordades, kus otsused võivad tugineda usaldusele, tavapärasele töökorraldusele ja ka eeldusele eelnevate osapoolte poolt kontrolli teostamisele. Käesolev alapeatükk keskendub töökorralduslikele turvameetmetele, mis on suunatud eelnevas alapeatükis kirjeldatud haavatavuste leevendamisele ja organisatsiooni vastupanuvõime suurendamisele arvepettuste ennetamiseks, varajaseks tuvastamiseks ning võimaliku kahju piiramiseks. Meetmed on magistr töö autori poolt tuvastatud teaduskirjanduse ja riikide õiguskaitse- ja julgeolekuasutuste koostatud ülevaadete omavahelisel analüüsimisel.

Ärikirjapettuste toimumisel on tegemist olukorraga, kus protsesside ülesehitus, vastutuse jaotus ja organisatsioonikultuur loovad koos tingimused, milles pettus võib osutada usutavaks ja jääda õigel ajal märkamata. Erinevalt tehnilistest turvameetmetest, nagu identiteedi kontrollimiseks kasutatavad autentimisprotokollid ja tegevuste jälgimist võimaldavad automatiseeritud IT-lahendused, on töökorralduslikud meetmed protseduurilised ja käitumuslikud kontrollimehhanismid, mida rakendatakse organisatsiooni töökorralduses.

Ziorklui et al. (2024) käsitlevad selliseid meetmeid organisatoorsete kontrollidena (*organizational controls*), mille eesmärk on aidata pettusi ennetada läbi töökorralduse, vastutuse jaotuse ja töötajate tegevuse suunamise. Arvete menetlemise protsessis hõlmavad töökorralduslikud meetmed näiteks autoriseerimisprotsesse, tööülesannete lahusust, kinnitusi ja kooskõlastusi, info liikumise korraldust ning lepingulisi kokkuleppeid koostööpartneritega. Sarnast lähenemist kirjeldavad ka Václavík et al. (2025), kelle järgi on arvepettuste ennetamisel oluline roll selgetel pangakonto muudatuste kinnitamise protseduuridel, rollide ja vastutuse jaotusel finantsprotsessis, ametlikel suhtluskanalitel partneritega ning töötajate teadlikkuse tõstmisel. Käsitus on kooskõlas rahvusvahelise infoturbestandardi ISO/IEC 27001 ja Eesti infoturbestandardi E-ITS põhimõtetega, mille järgi eeldab infoturbe tagamine lisaks tehnilistele kontrollimehhanismidele ka poliitikate ja protseduurikirjelduste ning -juhendite koostamist ja nõuete järgimise kehtestamist (Eesti Standardimis- ja Akrediteerimiskeskus, 2023; RIA, 2024c.).

Eelmises alapeatükis tuvastatud rollide kattumisega kaasnev oht viitab vajadusele tagada arvete menetlemisel üksteisest sõltumatud rollid. Vastutuse jaotus on ärikirjapettuste ennetamisel oluline tegur. Ülesannete lahususe põhimõte on eriti oluline olukordades, kus arvete menetlemisega seotud etapid on jaotatud mitme osapoole vahel, kuna see aitab vähendada vastutuse hajumisest tulenevat riski. Arvete menetlemise turvalise toimimise seisukohalt soovitatakse luua mitmetasandiline kinnitamise ring, kus üksteisest sõltumatud rollid on selgelt eristatud erinevate inimeste vahel. Reegli rakendamata jätmine võib suurendada pettuse õnnestumise riski, kuna üks töötaja omab täielikku kontrolli kogu protsessi üle (Ziorklui et al., 2024). RIA on samuti soovitanud kehtestada maksete töötlemiseks kahe silmapaari reegel, mille järgi iga ostuarve peab saama kinnituse vähemalt kahelt töötajalt (RIA, 2024b). Samas tuleb arvestada, et rollide eraldamine ei ole väiksemates organisatsioonides alati võimalik. Sellisel juhul on paindliku alternatiivina soovitatav sõltumatu kinnitaja põhimõtet rakendada kõrge riskiga tehingute puhul. Lisaks saab täiendava kontrollimehhanismina läbi viia regulaarseid auditeid (Ziorklui, 2024). Kuigi ülesannete lahusus moodustab sisekontrolli keskse alustala, ei pruugi see olla üksikmeetmena piisav.

Teiseks oluliseks kaitsekihiks on muudatuse kinnitamine alternatiivse suhtluskanali kaudu. Turvameede kaitseb verifitseerimise nõrkust olukorras, kus ründajal on õnnestunud luua usutav e-postipõhine suhtluskontekst. Eelmises alapeatükis kirjeldatud verifitseerimise nõrkus viitab sellele, et ärikirjapettuse õnnestumine võib sõltuda just sellest, kas organisatsioonil on olemas selge protseduur ebatavaliste või kõrge riskiga muudatuste

kontrollimiseks. Eriti oluline on see makseandmete muutmise korral, kus pettus võib väljenduda näiteks selles, et arvel on esitatud uus arvelduskonto number ning muudatus näib usutav. Sellises olukorras ei tohiks e-kirjas või arvel esitatud teavet pidada piisavaks sisendiks makse tegemiseks, isegi kui see pärineb esmapilgul usaldusväärselt osapoolelt. Soovitatav on arvete menetlusprotsessis kehtestada keskne reegel, mille järgi on arve rekvisiitide ootamatu muutus automaatne signaal täiendava kontrolli teostamiseks. Junger et al. (2020), Myojin & Babaguchi (2020) ja RIA (2026) soovivad maksetega seotud muudatuste kinnitamiseks helistada varasemalt teadaolevale kontaktile, mitte võimalikus petukirjas märgitud telefoninumbrile. Alternatiivse suhtluskanali kasutamine toimimist illustreerib ka Krolli (n.d.) analüüsitud kindlustusmaaklerettevõtte juhtum, kus ründaja kompromiteeris töötaja e-posti konto õngitsuskirja abil ning seejärel edastas kliendile pettusliku arve. Pettus õnnestus ära hoida üksnes tänu klientasutuse töötaja tähelepanelikkusele, kes palus muudatust kinnitada telefoni teel varasemalt teadaoleva kontaktisiku kaudu. Václavík et al. (2025) analüüsitud juhtumi näitel võib alternatiivse kanali rolli täita ka formaalne suhtluskanaliväline protsess. Pangakonto muudatus tuleb kinnitada lepingulise kokkuleppega ning võimalusel tõendada partneri pangapoolse kinnitusega. Praktiline soovitus alternatiivse kanali kasutamiseks hõlmab ka e-kirjale vastamise asemel selle edastamist (*reply-to* asemel *forward*), kuna edastamisel sisestatakse aadress käsitsi, mis vähendab vastusaadressi petliku ümbersuunamise toimimist (Bonhard et al., 2025; FBI, 2022; Zakari et al., 2026).

Esimeses alapeatükis käsitletud kahe protsessi teooria kohaselt suurendab kõrge töökoormus heuristikatel põhineva kiire otsustamise tõenäosust. Bailey & Konstan (2006) on rõhutanud töökatkestuste negatiivset mõju soorituse kvaliteedile. Vishwanath et al. (2011) ja Slifkin & Neider (2023) täiendavad teooriat, et teatud tüüpi katkestused, näiteks ootamatu teisele ülesandele lülitumine, võib soodustada eelmise ülesande unustamist ning seeläbi e-kirja läbimõeldumat lugemist, mis hoopis toetab pettuste tuvastamist. Seega on arve menetlemisprotsessi kujundamisel oluline arvestada inimliku heuristilise mõtlemisega kaasnevate eksimustega ning neid süsteemselt leevendada tehniliste aeglustavate mehhanismide abil. Seeläbi luuakse protsessis katkestus, mis vähendab kiireloomulist otsustamist ning suunab inimest olukorda teadlikumalt hindama. Kasutada on võimalik näiteks visuaalseid hoiatusi kõrge riskiga tehingute korral ning automaatseid teavitusi makseandmete muutumisel. Aeglustavad ja tähelepanu suunavad mehhanismid aitavad

leevendada riski realiseerumist olukorras, kus ründe haruldus ja protsessi rutiinsus võivad vähendada ebatavaliste ohusignaalide märkamist.

Töökorralduslike meetmete toimivus ei sõltu üksnes protseduuride olemasolust, vaid ka sellest, mil määral on töötajad teadlikud varitsevatest ohtudest ning kui toetav on organisatsioonikultuur kahtlemise ja kontrollimise suhtes. Václavík et al. (2025) ja Ziorklui et al. (2024) on rõhutanud juhtkonna rolli usaldusliku ja turvalise õhkkonna loomisel, milles töötajad julgevad küsida ja vajaduse korral kinnitada üle ka juhi otsuseid kõrge rahalise riskiga tehingute puhul. Selleks on võimalik kehtestada põhimõtte, et tavapäratu kiire maksekorraldus ka tippjuhtide poolt on võimalik risk, mitte lihtsalt täitmist vajav ülesanne. Junger et al. (2020) kinnitasid empiiriliselt, et tegevjuhi nimel toime pandud pettust õnnestus ennetada just telefoni teel täiendava kontrollimisega. Kui organisatsioonis puudub selge juhis selle kohta, kuidas käituda olukorras, kus makse tundub küll formaalselt korrektne, kuid sisuliselt ebatavaline, suureneb tõenäosus, et töötajad lahendavad olukorra tavapärase loogika järgi. Just selliste situatsioonide jaoks peab organisatsioon kehtestama erandite käsitlemise põhimõtted.

Ärikirjapettuste ennetamisel on oluline roll ka teadlikkuse tõstmisel ja töötajate koolitamisel. Junger et al. (2020) tuvastasid pettuse tuvastamise kõige efektiivsema kaitsemeetmena töötaja tähelepanelikkuse. Läbi viidud uurimuse järgi koguni 91% juhtudest, kus pettuse katse ebaõnnestus, märkasid töötajad ohusignaale kas visuaalselt ebatavalise e-posti aadressi, ebaloogilise summa või ebatavapärase suhtlusstiili kaudu. Samas ei teki selline tähelepanelikkus üksnes kogemuse kaudu. Mitmed autorid on rõhutanud, et koolitused peavad sisaldama realistlikke simulatsioone ja praktilisi stsenaariume, kuna koolitus, mis ei sarnane olukordadele päriselust, ei pruugi muuta käitumuslikke harjumusi (Iuga et al., 2011; Okumu et al., 2024; Thomas, 2018; Vishwanath et al. 2011). Uuringud on seejuures näidanud, et inimesed kipuvad üle hindama oma suutlikkust õngitsusründeid ära tunda ning alahindama petlikku mõju enda otsustusvõimele, mistõttu võivad nad reaalses olukorras käituda teisiti, kui nad ise eeldavad (Goel et al., 2017; Halevi et al., 2015; Iuga et al., 2016; Modic & Lea, 2013). Inimesed eksivad ennekõike siis, kui nad tunnevad survet ja peavad kiiresti otsustama. Samas ei tohi koolitused keskenduda üksnes hirmu tekitamisele, vaid pakkuma praktilist kogemust ja arusaama sellest, kuidas riskid võivad tööprotsessides avalduda (Bada et al., 2015; Václavík et al., 2025; Van Steen et al., 2020; Ziorklui et al., 2024). Seega peavad koolitused olema kontekstipõhised, sihtrühmaga arvestavad ning mõõdetavate tulemustega, kuna ilma nende elementideta ei pruugi isegi mahukad

koolitusprogrammid positiivset muutust kaasa tuua. Teadlikkuse tõstmine on eriti oluline keskkondades, kus kõrge süsteemne töökindlus võib valvsust vähendada läbi subjektiivselt tajutud turvalisuse.

Isegi hästi kujundatud ennetusmeetmete rakendamisel ei ole võimalik kõiki rünnakuid tõrjuda. Seetõttu on organisatsiooni teadlikkus riskidest ning valmisolek turvaintsidentide kiireks avastamiseks ja käsitlemiseks kriitilise tähtsusega. Riskianalüüside teostamine protsesside nõrkuste kaardistamiseks on ennetava riskijuhtimise alus. (Agrafiotis et al., 2018) ENISA (2025b) andmetel aitavad regulatiivsed nõuded ja infoturbe vastavusraamistikud tugevdada riskijuhtimist, tuvastamis- ja reageerimisvõimekust ning loovad aluse tugevale küberturvalisusele. Intsidendihalduse protsessi loomine on osa terviklikust riskijuhtimisest. Õigeaegne avastamine ja reageerimine on oluline nii konto esialgsel kompromiteerimisel kui ka realiseerunud turvaintsidenti korral. Václavík et al. (2025) juhtumiuuring näitas, et kiire reageerimine võib olla otsustava tähtsusega. Ühes autorite analüüsitud juhtumitest õnnestus pettuslik makse peatada, kuna petetud ülikool teavitas toimunud intsidendist kiiresti pank. Ka RIA (2024b) rõhutab, et eriti oluline on reageerida kiiresti olukorras, kus pettuslik makse on juba tehtud või kohe tegemisel, sest õigeaegne teavitamine võib võimaldada kahju tekkimist vältida.

Kokkuvõtvalt suurendavad töökorralduslikud turvameetmed arve menetlemise turvalisust ja organisatsiooni vastupanuvõimet, samas ei pruugi katta kogu protsessiahelat täielikult. Tugev automatiseeritus ja standardiseeritus võivad küll vähendada vigade hulka teatud etappides, kuid samal ajal võib alles jääda oht protsessi varasemates etappides, kus otsused põhinevad inimlikul hinnangul. Seetõttu tuleb töökorralduslike turvameetmete tõhusust hinnata mitte üksnes nende olemasolu järgi, vaid võtta arvesse, millises etapis need rakenduvad, milliseid haavatavusi leevendavad ning kas need aitavad vähendada riski ka nendes kohtades, kuhu tehniliste meetmete kaitse ei ulatu. Tabel 1 koondab peatükis käsitletud peamised töökorralduslikud haavatavused ning neid leevendavad turvameetmed.

Tabel 1

Haavatavuste ja turvameetmete vaheline seos ostuarvete menetlemise protsessis

Haavatavus	Mõju protsessile	Turvameede	Kontrollmehhanismi mõju
1. Rollide kattumine ja vastutuse hajumine.	Otsustusõigus koondub ühe isiku kätte, mis suurendab pettuste märkamata jäämise tõenäosust.	Ülesannete lahusus ja mitmetasandiline arve kinnitamine.	Vähendab üksiku eksimuse mõju.

2.	Olemasoleva suhtluse usaldamine.	Pettus jääb avastamata tavapärase protsessi jälgendamise tõttu.	Muudatuse kinnitamine alternatiivse kanali kaudu.	Katkestab vaikimisi usaldamise ja lisab täiendava kaitsekihi.
3.	Töökoormus ja ajasurve.	Kiirustades tehtud otsused suurendavad ohusignaalide tähelepanuta jätmist.	IT-süsteemis hoiatus kõrge riskiga maksete korral.	Vähendab tähelepanematuses tingitud vigu.
4.	Surve turvanõuete leevendamiseks.	Protsessi turvalisuse ja pettuste tuvastamise võimekuse vähenemine.	Organisatsiooni- kultuuri kujundamine läbi juhtkonna selge vastutuse ja asutuse- ülestestamise ka erandlikeks olukordadeks.	Toetab turva- meetmete järjepidevat rakendamist ning vähendab sõltuvust üksikisikute initsiatiivil põhinevast turvalisusest.
5.	Tehnoloogia liigne usaldamine ja töötajate madal riskitaju.	Haruldaste ohtude tähelepanuta jätmisel või jääda pettus tuvastamata.	Realistlikud ja regulaarsed koolitused teadlikkuse tõstmiseks.	Parandab ohtude märkamist ja vähendab liigset enesekindlust.
6.	Intsidendihalduse protsessi puudumine.	Pettuse esinemisel tegevuskava puudumine kiireks reageerimiseks ja tekkinud kahju leevendamiseks.	Süsteemitoimingute logimine, intsidendi lahendamise protsessi dokumenteerimine ja seotud osapoolte kaardistamine.	Võimaldab kiiret ja koordineeritud reageerimist ning tõendite kogumist.

Allikas: Autori koostatud, tuginedes allikatele Agrafiotis et al., 2018; Almutairi et al., 2025b; Bera et al., 2023; Goel et al., 2017; Halevi et al., 2015; Iuga et al., 2016; Jones et al. 2019; Junger et al., 2020; Modic & Lea, 2013; Myojin & Babaguchi, 2020; Okumu et al., 2024; RIA, 2024b; Schneider, 2008; Václavík et al., 2025; Vaughan, 1996; Ziorklui et al., 2024.

Haavatavuste ja turvameetmete vaheline seos loob teoreetilise aluse empiiriliseks analüüsiks, milles vaadeldakse, kuidas avalduvad tegurid Eesti avaliku sektori organisatsioonide tegelikes ostuarvete menetlemise protsessides. Seejärel nimetatakse peamised kaitsemehhanismid intsidendide varajaseks avastamiseks ning pettuste realiseerumise tõkestamiseks.

2. Empiiriline uuring

2.1. Ärikirjapettuste avaldumine ja käsitlus Eestis

Magistritöö teoreetiline osa andis ülevaate ärikirjapettuse olemusest ning protsessilistest haavatavustest, mis loovad eeldused kahju tekkimist. Samuti käsitleti praktiliselt rakendatavaid turvameetmeid, mis aitavaid neid leevendada. Varasema teaduskirjanduse süstematiseerimisel seisnes metoodiline piirang selles, et enamik seniseid uuringuid keskendub ärikirjapettuste ja õngitsusrünnete tehnilistele ja psühholoogilistele

teguritele. Arvete menetlemisega seotud töökorralduslikke ja protsessipõhiseid aspekte on käsitletud vähem.

Magistritöö teine peatükk kirjeldab empiirilise informatsiooni kogumise, analüüsimise ja tõlgendamise protsessi ning esitab uurimuse järeldused. Empiiriline osa jaguneb kolmeks alapeatükiks. Esmalt antakse ülevaade Eesti küberturvalisuse hetkeseisust ja tuuakse näiteid avalikustatud ärikirjapettuste juhtumitest. Lisaks tutvustatakse peamisi regulatsioone – nii Eestis kehtestatud kui ka rahvusvahelisi – mis on loodud küberpettuste ennetamiseks. Teises alapeatükis tutvustatakse uuringu metoodikat. Kolmandas alapeatükis analüüsitakse uuringu käigus kogutud teavet ning esitatakse järeldused ja praktilised soovitused ärikirjapettuste tõkestamiseks.

Eestis tegelevad ärikirjapettuste ennetamise ja käsitlemisega mitmed eri valdkonna organisatsioonid. Arvepettus hõlmab endas üheaegselt küberturbe intsidenti, finantspettust, võimalikule rahapesule eelnenud rahvusvahelist majanduskuritegu ning organisatsiooni sisekontrolli puudujääki. Seetõttu sõltub pettuste ennetamine ja käsitlemine mitme organisatsiooni tõhusast koostööst ja selgest rollijaotusest.

Seadusandlikul tasandil vastutab küberturvalisuse tagamise eest Eestis Justiits- ja Digiministeerium (edaspidi JustDigi), mille eesmärk on riigi õiguspoliitika elluviimine ning seeläbi turvalise ühiskonna kujundamine. JustDigi ülesannete alla kuulub küberturvalisuse hoidmine läbi riikliku strateegia kujundamise, küberturvalise seaduse välja töötamise ja vastu võtmise ning regulaarse ajakohastamise (JustDigi, 2026). Küberturvalisuse seadus (edaspidi KüTS) loob Eestis ühtse küberturbe raamistiku, tagamaks ühiskonnale oluliste teenuste toimepidevus ning kaitstus küberohtude eest. Sellest tulenevalt mõjutab ministeeriumi tegevus otseselt ka seda, millisel tasemel rakendatakse avaliku sektori organisatsioonides küberintsidente ennetavaid turvameetmeid. (KüTS, 2018)

Magistritöös on varasemalt esile toodud JustDigi valitsemisalasse kuuluva RIA roll küberturvalisuse tagamisel. RIA tegutseb KüTS-i järgi Eesti küberturvalisuse keskuse ja järelevalveasutusena, mille ülesannete alla kuulub ka küberintsidentide haldamine ja koordineerimine ning küberolukorra analüüsimine ja ohuteavituste edastamine (KüTS, 2018). Küberintsidentide käsitlemiseks on RIA-s loodud eraldi osakond, CERT Eesti ehk CERT-EE (edaspidi CERT), mis kuulub ENISA küberturbemeeskondade võrgustikku *CSIRTs Network*. CERT-i ülesanne on jälgida Eesti digiruumi ning seeläbi tuvastada lubamatud tegevused ja vajadusel asuda tegelema nende lahendamisega. (RIA, 2025) Ärikirjapettuste osas tähendab see, et kuigi RIA ja CERT saavad toetada tehnilise kompromiteerimise, võltsitud domeenide

ja kirjavahetuse väärkasutuse analüüsi, jäävad pettuse ennetamisel ja hilisemal tuvastamisel määravaks organisatsiooni enda tööprotsessid ja kontrollimehhanismid.

Rahandusministeerium (edaspidi RAM) vastutab finantsjuhtimise ja -arvestuse põhimõtete kujundamise eest, millel põhinevad avaliku sektori arvete menetlemise protsessid (RAM, 2024). Ärikirjapettuste kontekstis seisneb RAM-i roll rahapesuvastase tegevuse koordineerimist ja seadusandluse kehtestamist. Kuna ärikirjapettus on sageli rahapesule eelnev kuritegu, mõjutavad RAM-i poliitikad seda, kui tõhusalt on võimalik pettusest saadud rahavoogusid tuvastada ja piirata. RAM-i haldusalasse kuuluva eraldiseisva valitsusasutuse Rahapesu Andmebüroo (edaspidi RAB) eesmärk on finantskuritegevuse tõkestamine. RAB-i ülesandeks on kahtlaste tehingute kohta teabe kogumine ning rahapesu ja terrorismi rahastamise tunnuste esinemise korral info jagamine uurimisasutustega (RAB, 2026).

Politsei- ja Piirivalveamet (edaspidi PPA) on Siseministeeriumi haldusalasse kuuluv Eesti korrakaitse keskasutus, mille ülesanded küberpettuste puhul hõlmavad süütegude ennetamist ja uurimist, tõendite kogumist ning rahvusvahelist koostööd (PPA, n.d.). Sageli liigub pettuse teel saadud raha kiiresti välisriikide arvelduskontodele, mistõttu on tõhus piiriülene suhtlus menetluse edukuse seisukohalt kriitilise tähtsusega. Kuriteo lahendamise tulemuslikkus sõltub nii ohvri kiirest tegutsemisest kui ka sellest, kas organisatsioonil on säilinud vajalikud süsteemiligid, kirjavahetus, maksekorraldused ja muud tõendid. Seetõttu on organisatsioonisisese intsidendihaldusprotsessi olemasolu oluline eeldus juhtumi tõhusaks lahendamiseks ja kahju vähendamiseks.

2026. aasta aprillist töötab Keskkriminaalpolitsei koosseisus kelmuste ennetamise ja lahendamise keskus (KelKe), mille eesmärk on koondada erinevate juhtumite kohta kogutud teavet, tuvastada nende vahelisi seoseid ning seeläbi jõuda suurimat finantskahju tekitavate võrgustikeni. Eesti õiguskaitseasutuste sõnul nähakse petuskeemide taga hierarhilisi ja organiseeritud grupeeringuid, mille tegevuses on võimalik märgata korduvaid mustreid ja rollijaotust (Toompuu, 2025). Samas on teaduskirjanduses leitud, et ärikirjapettustega seotud küberkuritegelikud võrgustikud võivad toimida paindlike ja hajusate koostöömudelitena, mitte traditsioonilise hierarhilise kuritegeliku organisatsioonina. (Lazarus, 2025). Mõlemad käsitlused viitavad siiski sellele, et tegemist on süsteemse ohuga, mille tõkestamisel on oluline organisatsioonidevaheline koostöö.

Pankadel on ärikirjapettuste ennetamisel samuti eriline roll, sest pettuse kahju realiseerub maksetehingu kaudu. Pangad saavad tuvastada ebatavalisi tehingumustreid, rakendada täiendavaid kontrole ning peatada kahtlaseid makseid. Samas on nende roll

piiratud olukordades, kus makse on kliendi poolt kliendi poolt heaks kiidetud ehk autoriseeritud, mis on ärikirjapettuste puhul tavapärane. Sellisel juhul ei pruugi tehing eristuda tavapärasest maksekäitumisest ning panga võimalused pettuse ennetamiseks on piiratud. Ärikirjapettuste puhul liigutatakse raha sageli kiiresti edasi, mistõttu aeg raha tagasikutsumiseks võib olla väga lühike. Seetõttu on pärast pettusliku makse toimumist kahju vähendamisel otsustav nii ohvri kui panga kiire tegutsemine. Pankade rolli saab käsitleda viimase kaitseliinina, mis võib aidata kahju piirata, kuid ei asenda organisatsioonisiseseid ennetusmeetmeid. Eesti pankasid esindab Eesti Pangaliit, mille struktuuri kuulub pettuste tõkestamise toimkond. Toimkonna tegevus keskendub pankadevahelise koostöö arendamisele pettuste ennetamisel ning hõlmab teadlikkuse tõstmist, parimate praktikate jagamist ning koostööd erinevate osapooltega. (Eesti Pangaliit, n.d.).

Eesti õiguslik raamistik on suurel määral kooskõlas Euroopa Liidu küberturvalisuse ja finantssektori regulatsioonidega. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 ehk Küberturvalisuse 2. direktiivi (*Network and Information Security*, NIS2) eesmärk on saavutada Euroopa Liidus võrgu- ja infosüsteemide kõrge küberturvalisuse tase (European Commission, 2026). Eesti kontekstis on NIS2 ülevõtmine seotud KÜTS-i muutmisega, mille tulemusel laieneb seaduse kohaldamisala ühiskonna toimimise seisukohalt kõikidele oluliste ja elutähtsate teenuse osutajatele. Vastavalt KÜTS-ile peavad avaliku sektori organisatsioonid küberturvalisuse tagamisel lähtuma reguleeritud infoturbe raamistikust, millele vastavust kontrollib asutuseväline sõltumatu infoturbeaudiitor. RIA on välja töötanud Eesti infoturbestandardi (edaspidi E-ITS), mis kirjeldab infoturbe halduse süsteemi rajamise ja rakendamise nõudeid ning sisaldab tüüpiliste organisatsioonide tegevust kaitsvaid turvameetmeid, mida nimetatakse etalon-turbekataloogiks. E-ITS on Eesti konteksti järgi kohandatud infoturbemeetmete kogu, mille aluseks on Saksa päritolu BSI IT-Grundschutzi etalon-turbe meetodika. E-ITS on kooskõlas rahvusvaheliselt tunnustatud infoturbestandardiga ISO/IEC 27001 (RIA, 2024c). Ärikirjapettuste kontekstis loob E-ITSi rakendamine organisatsioonidele praktilist väärtust, kuna suunab määratlema infoturbe vastutust, dokumenteerima turbeprotsesse, rakendama riskipõhist juhtimist ning looma toimiva intsidendihalduse. E-ITS toetab ka töökorralduslike protsesside turvalisuse tagamist, mida käesolev magistritöö käsitleb ärikirjapettuste tõkestamisel kesksetena. Avalikul sektoril on võimalik E-ITSi asemel lähtuda ka mõnest alternatiivsest infoturbestandardist, kuid KÜTS-ist tulenevalt kaasneb kohustus valitud standardile vastavust regulaarselt tõendada.

Maksepettuste vähendamise seisukohalt on oluline ka Euroopa Liidu täiendatud makseteenuste direktiiv (EL) 2015/2366 (*Payment Service Directive 2*, PSD2), mis ühtlustab makseteenuste regulatiivset raamistikku ning kehtestab elektroonilistele maksetele rangemad turvanõuded. PSD2 keskseks mehhanismiks on tugev kliendi autentimine, mis on kohustuslik kõigile internetis tehtavatele pangaülekannetele ning mille eesmärk on suurendada maksete turvalisust ja vähendada volitamata tehingute riski. (European Parliament and the Council of the European Union, 2015). Siiski on ärikirjapettuste puhul selle mõju piiratud, kuna pettuslik makse võib vastata tehnilistele nõuetele ja olla kinnitatud organisatsiooni töötaja poolt, mis kinnitab käesoleva töö keskset mõtet: tehnilised turvameetmed on vajalikud, kuid need ei suuda täielikult asendada töökorralduslikke kontrollimehhanisme, mis on ärikirjapettuste ennetamisel otsustava tähtsusega.

Eesti on digitaalse ühiskonnana üha enam ärikirjapettuste sihtmärgiks. RIA on kirjeldanud mitmeid Eestis toimunud juhtumeid, mis illustreerivad erinevate ärikirjapettuse skeemide toimimist praktikas. Avaliku sektori näitel on tähelepanuväärne 2020. aastal aset leidnud juhtum, kus ründajad kasutasid riigihangete registri avalikke andmeid ning kehastasid hankevõitjat, esitades haiglale üle 10 000 euro ulatuses usutavaid võltsarveid. 2022. aastal viidi kolmanda sektori asutuses läbi tegevjuhi petuskeem, kus raamatupidajale saadeti kolm järjestikust maksekorraldust näiliselt juhi nimel. Pettuse kogukahju ületas 53 000 eurot. 2023. aastal langes sõidukite müügiga tegelev ettevõtte arvepettuse ohvriks. Äripartneri kompromiteeritud kontolt saadeti võltsarve, mille alusel kandis Eesti ettevõtte ligi 30 000 eurot kurjategijatele (RIA, 2023a; 2025a). 2023. aastal toimus arvepettus, milles kannatas kahju välispartner, kuna kompromiteeriti Eesti põllumajandusettevõtet (Matson Kald, 2023). 2025. aastal tehti masinatööstusettevõtte finantsjuhile petukõne, mille käigus saadi kätte vajalikud andmed tema nimele Smart-ID konto loomiseks. Kahe tunni jooksul tehti 52 makset kogusummas 1,6 miljonit eurot, millest alla poole õnnestus tagasi saada (Jõgi, 2026). 2026 aastal kaotas Eesti ettevõtte arvepettuse tõttu ligi 167 000 eurot (Sildmets, 2026). Juhtumid näitavad, kuidas autoriteetsus, ajasurve ja ebatavaline olukord võivad viia tagajärjeni, et kontrollimehhanismid ei rakendu või neid ei peeta vajalikuks. Ärikirjapettuste raporteeritud kogukahju Eestis oli 2025. aastal 2,7 miljonit eurot (Annom, 2026). Magistritöö autorile teadaolevalt on seni suurimad Eestis avalikustatud ärikirjapettuste kahjud organisatsioonidele olnud kahe maksega tekitatud 1,6 miljoni euro suurune kahju (Saarmann, 2026) ning teisele organisatsioonile samuti kahest maksest koosnev 1,7 miljoni euro suurune kahju (Vasli, 2025). Tabelis 2 esitab magistritöö autor valiku Eestis aset leidnud

ärikirjapettuste juhtumitest, mis on tuvastatud avalike allikate põhjal. Juhtumite valikul eelistati sisult erinevaid ja suurema mõjuga juhtumeid, mis võimaldavad illustreerida ärikirjapettuste toimepanemise viise ning protsessilisi haavatavusi.

Tabel 2.

Eestis toimunud ärikirjapettuste juhtumid

Ohver	Aasta	Kahju suurus	Ründemeetod	Organisatsiooni nõrkus
Automüügi ettevõtte (RIA, 2024b)	2019	60 000 €	Ostja ja välismaise automüügifirma meilivestlusesse sekkuti ning muudeti e-kirjade sisu ning arve rekvisiite.	1. E-posti vestluse kompromiteerimist ja võltsarve esitamist ei märgatud.
Anonüümne ettevõtte (RIA, 2024b)	2019	29 000 €	Ettevõtte e-posti kontole saadeti muudetud kontonumbriga, kuid tavapärase välimusega arve liikmemaksu tasumiseks.	1. Puudus protseduur makseandmete kontrollimiseks. Muutus ei tekitanud kahtlust mitme inimese poolt läbitud kooskõlastusringil. 2. Esialgselt jäi märkamata ka tavapärasest kohmakam kirjastiil.
Avalik sektor (haigla) (RIA, 2020)	2020	>10 000 €	Ründajad kasutasid riigihangete registri andmeid. Kompromiteeriti hanke võitja e-posti konto, mille kaudu saadeti haiglale võltsitud arved.	1. Tarnija identiteeti ei kontrollitud enne maksete sooritamist. 2. Avalikult kättesaadavad andmed võimaldasid personaliseeritud pettust.
Spordialaliit (RIA, 2020)	2020	~4 000 €	Kurjategijad kompromiteerisid spordialaliidu e-posti konto ja jälgisid kirjavahetust. Sobival hetkel esitasid spordialaliidu partnerina palve arvelduskonto muutmiseks.	1. E-posti konto ülevõtmist ei tuvastatud. 2. Kriisiolukord (COVID-19) võis tekitada ajasurvet ja vähendada tähelepanelikkust. 3. Puudus arvelduskonto muutuse kinnitus alternatiivse kanali kaudu.
Automüügi ettevõtte (RIA, 2023a)	2021	~30 000 €	Kompromiteeriti äripartneri e-posti konto ja esitasid Eesti ettevõttele võltsarve.	1. Arvelduskonto muudatust ei kontrollitud teise suhtluskanali kaudu.
Mittetulundusühing (RIA, 2025a)	2022	~53 000 €	Raamatupidajale saadeti e-kiri, mis näis pärinevat tegevjuhilt. Kolme päeva jooksul tehti kolm makset välisriigi kontodele.	1. Tegevjuhi isikut ei kontrollitud alternatiivse kanali kaudu. 2. Kolm järjestikust suures summas pangaülekannet ei tekitanud ohusignaali.
Masinaehitusettevõtte (RIA, 2025a)	2024	>1 000 000 € (Algselt 1,6 mln, millest osa	Tervisekassa töötajana helistati finantsjuhile, kellelt saadud andmete põhjal loodi Smart-ID	1. Finantsjuhil puudus teadlikkus telefonivestluses identiteedi tuvastamisega kaasnevast riskist.

		saadi tagasi)	konto. Seejärel kehastati pangatöötajat ja politseinikku, mille abil pääseti finantsjuhi arvutisse ja sooritati makseid.	2. Kaugligipääsu rakendus oli kasutatav ilma autentimisnõudeta. 3. Puudus reaalajas anomaaliate tuvastamine.
Anonüümne ettevõtte (Vasli, 2025)	2025	1 700 000 €	Äripartneri e-posti konto kompromiteeriti, mille abil saadeti muudetud rekvisiitidega arved.	1. Pangakonto muudatust ei kontrollitud teise suhtluskanali kaudu.

Allikas: Autori koostatud RIA poolt avaldatud andmetele tuginedes

Juhtumite põhjal on näha, et Eestis esineb mitmeid erinevaid ärikirjapettuse vorme: arvepettust, tegevjuhi pettust, meilikonto kompromiteerimist ning kombineeritud sotsiaalse manipulatsiooni skeeme. Petuskeemid on peamiselt keskendunud tarnijate identiteedi jäljendamisele, makseandmete muutmisele või olemasoleva usaldussuhte ärakasutamisele.. Mitmed pettused avastati töötajate tähelepanelikkuse, mitte automatiseeritud IT-lahenduste abil. Samas esineb ka juhtumeid, kus pettus jääb pikaks ajaks märkamata või avastatakse alles pärast kahju tekkimist. Analüüsist ilmneb, et kuigi ründemeetodid võivad erineda, on nende aluseks sarnane loogika, kus ründaja loob usaldava suhtluskonteksti ning manipuleerib otsuse tegemist viisil, mis ei tekita kahtlust esitatud nõude seaduslikkuse osas. Sellest lähtuvalt on vajalik uurida, millised töökorralduslikud ja protsessipõhised tegurid võimaldavad sellistel rünnetel õnnestuda ning ka seda, kuidas organisatsioonid riske tajuvad ja käsitlevad.

2.2. Uuringu metoodika ja andmekogumine

Käesolevas alapeatükis kirjeldatakse empiirilise uurimuse metoodikat ning andmekogumise ja tulemuste tõlgendamise protsessi. Uurimisprobleemi püstitamine lähtus praktilisest vajadusest paremini mõista, millised on praktikas rakendatavad meetmed ostuarvete menetlemise protsessi kaitsmiseks. Ärikirjapettustega seotud rünnete arv ja nende tekitatud kahju on viimastel aastatel kasvanud, mistõttu on organisatsioonide finantsprotsesside turvalisuse tagamine muutunud aina olulisemaks.

Magistritöös viidi läbi kvalitatiivne juhtumiuuring, mille eesmärk oli analüüsida avaliku sektori ostuarvete menetlemise töökorraldust ning tuvastada võimalikud ohukohad ning nõrkuseid leevendavad turvameetmed, mis mõjutavad ärikirjapettuste õnnestumist. Uuring käsitleb ühte protsessi, mille raames on vastutus jagatud kahe organisatsiooni vahel. Nii teenuseosutaja kui kliendi vaatenurga analüüsimine võimaldas kujundada tervikliku arusaama vastutuse jaotusest ja olemasolevate kontrollimehhanismide toimimisest.

Kvalitatiivne lähenemine sobib teemat süvitsi uurivate nähtuste käsitlemiseks. Sisuline dialoog praktikutega aitab protsesside ülesehitust paremini mõista.

Andmekogumise põhimeetodina kasutati poolstruktureeritud individuaalseid intervjuusid. Individuaalintervjuude formaadi abil luuakse tundliku teemaga seotud sisu avamiseks usalduslikum keskkond kui rühmavestluse korral. Eesmärk on intervjueeritavate kogemusi ja tõlgendusi sügavamalt mõista. Poolstruktureeritud intervjuud lubavad uurijal paindlikult suunata vestlust vastavalt selle kulgemisele. (Bryman, 2012) Intervjuukava koostamisel lähtuti uuringu eesmärkidest ja töö alguses püstitatud uurimisülesannetest (Lisa B). Küsimused kohandati vastavalt intervjueeritava rollile ja organisatsiooni vastutusvaldkonnale. Lisaks intervjuudele analüüsiti protsessikirjeldusi ja kasutusjuhendeid. Dokumentide analüüsi käigus võrreldakse intervjueeritavate kirjeldatud tegevusi dokumenteeritud nõuetega, sealjuures tähelepanu pöörates ka võimalikele erinevustele tegelike praktikate ja kirjalikult kehtestatud põhimõtete vahel.

Uuritavate valik moodustati mittetöenäosusliku sihipärase valimi põhimõtete järgi, mis on kvalitatiivses uurimises levinud lähenemine, kuna võimaldab valida osalejaid nende teadmiste, kogemuste ja fookuses oleva protsessi tundmise põhjal (Bryman, 2012). Sellise valimi eesmärk on kaasata osapooled, kes omavad nähtuse kohta kõige asjakohasemat ja sisukamat teadmist.

Valimisse kuulub kaks avaliku sektori organisatsiooni: Esimene on Riigi Tugiteenuste Keskus (edaspidi RTK), kes osutab finantsarvestusteenust ja muid tugiteenuseid Eesti avaliku sektori organisatsioonidele. RTK-st intervjueriti nelja inimest, kelle rollid katavad ostuarvete menetlemise protsessi erinevaid etappe. Intervjueeritute hulka kuulusid finantsarvestuse talituse juhataja–pearaamatupidaja (edaspidi talituse juhataja) (intervjuudes ja analüüsis tähistatud: RTK I1 ja RTK I3), raamatupidaja (RTK I2) ning tarkvarakonsultant (RTK I4). Talituse juhataja peamised ülesanded on meeskonna juhtimine ja finantsarvestuse koordineerimine. Raamatupidaja roll keskendub ostuarvete igapäevasele menetlemisele, sealhulgas arvete rekvisiitide, summade ja konteeringute kontrollimisele. Tarkvarakonsultant tegeleb majandustarkvaras andmete haldamisega. Tema ülesannete hulka kuulub Hankijakaartide loomine, pangaandmete sisestamine ja õigsuse kontrollimine enne maksete tegemist, mistõttu täidab arvete menetlemise protsessis olulist rolli.

Teisena on uurimusse kaasatud Riigi Info- ja Kommunikatsioonitehnoloogia Keskus (edaspidi RIT), kes kuulub RTK klientide hulka ning kellele osutatakse finantsarvestusteenust. RIT on valitud kliendi vaate esindajana, andes sissevaate sellesse,

kuidas jagatud finantsarvestuse teenust kasutav organisatsioon käsitleb arve menetlemise protsessi ning tajub sellega seotud riske. RIT-ist intervjueriti arvestusspetsialisti, kellega viidi läbi kaks intervjuud (RIT I1 ja RIT I2). Tema ülesanded hõlmavad Fitekisse saabuvate ostuarvete vastuvõtmist, tellija tuvastamist ning arvete suunamist vastavale osapoolale kinnitamiseks. Arvestusspetsialist tegutseb kinnitusringis nii protsessi esimese kui ka viimase lülina. Pärast kinnituste saamist konteerib ta arve ja edastab RTK-le menetlemiseks. Tema roll eeldab pidevat koostööd nii RTK kui ka organisatsiooni sisuosakondadega, et tagada toimingute sujuvus ja korrektsus. Valik vastab sihipärase valimi loogikale, mille kohaselt kaasatakse uurimusse osapooled, kellel on otsene kokkupuude uurimisteedega ning kes saavad pakkuda mitmekülgseid perspektiive (Bryman, 2012).

Empiiriline andmekogumine toimus etapiviisiliselt. Esmalt viidi läbi intervjuud RTK esindajatega, et kaardistada arvete menetlusprotsessi töökorraldus ja sellega seotud kontrollimehhanismid teenuseosutaja perspektiivist. Seejärel kaasati analüüsi sama protsessi kliendipoolne vaade, intervjuerides RIT-i arvestusspetsialisti. Viimase intervjuu näol lisati uuringusse ka RTK tarkvarakonsultant, kuna nii RTK esindajad kui ka magistratöö autor leidsid, et tarnijaandmete haldamise ja kontrollimisega seotud tegevused on protsessi terviklikuks mõistmiseks olulised. Valitud lähenemine võimaldas analüüsida protsessi erinevate rollide vaatenurgast. Lisaks intervjuudele koguti andmeid organisatsioonides kehtestatud dokumentide abil: RIT-i finantsprotsesside kirjeldused (RIT, 2025), FitekIN arvekeskuse ja SAP majandustarkvara kasutamisejuhendid (RTK, 2021, 2024a, 2024b, 2026), Justiitsministeeriumi valitsemisala finantsarvestuse toimemudel (RTK, 2023), mis sisaldab RTK ja RIT-i vahelist rollide ja vastutuse jaotust.

Intervjuud viidi läbi 2026. aasta aprilli ja mai jooksul Microsoft Teams-i vahendusel. Osalejate nõusolekul salvestati intervjuud ning andmete analüüsimiseks transkribeeriti salvestised veebirakenduse tekstiks.ee abil. Intervjuude kestus jääb vahemikku 47 kuni 83 minutit. Transkriptsioone magistratöösse ei lisata, et kaitsta organisatsioonide poolt edastatud konfidentsiaalset teavet. Samuti ei lisata magistratöösse andmete analüüsimisel kasutatud RIT-i asutusesiseseks kasutamiseks mõeldud finantsprotsesside kirjeldusi. Helisalvestised ja kirjalikud transkriptsioonid kustutati pärast andmete analüüsi lõpetamist. Intervjuude toimumisajad ja kestused on esitatud tabelis 3.

Tabel 3

Ülevaade toimunud intervjuudest

Kuupäev	Intervjueeritav	Ametinimetus	Kestus
13.04.2026	RTK I1	Talituse juhataja– pearaamatupidaja	67 minutit
14.04.2026	RTK I2	Raamatupidaja	63 minutit
20.04.2026	RTK I3	Talituse juhataja– pearaamatupidaja	73 minutit
22.04.2026	RIT I1	Arvestusspetsialist	61 minutit
23.04.2026	RIT I2	Arvestusspetsialist	47 minutit
08.05.2026	RTK I4	Tarkvarakonsultant	83 minutit

Allikas: Autori koostatud

Uurimuse eripärana tuleb esile tuua autori professionaalne taust infoturbe valdkonnas. Kuigi autor ei ole olnud otseselt seotud uuritavate protsessidega, võib põhjalikum teadmine küberturvalisuse ja riskide teemadel mõjutada rõhuasetusi. Braun ja Clarke'i (2006; 2019) refleksiivse temaatilise analüüsi käsitluses tõlgendatakse uurija positsiooni analüütilise ressursina, mis aitab nähtusi mõtestada. Autor teadvustab ja jälgib kogu analüüsi vältel oma eelteadmiste mõju tulemuste tõlgendustele. Analüüsiprotsessi algfaasis lähtutakse Mayringi (2014) kvalitatiivse sisuanalüüsi põhimõtetest, mille abil struktureeritakse intervjuuandmed esialgsetesse kategooriatesse ja teemadesse ning koondatakse kirjeldavatesse tabelitesse (Lisa C). Selline süsteemne organiseerimine võimaldab kogutud andmeid korrastada ja luua alus edasiseks tulemuste tõlgendamiseks. Põhianalüüs viiakse läbi refleksiivse temaatilise analüüsi põhimõtetele, mille eesmärk on tuvastada korduvaid mustreid ja tähendusi seoses uurimisülesannetega (Braun & Clarke, 2006).

2.3. Uurimistulemused ja järeldused

Järgnevalt analüüsitakse kuue intervjuu põhjal, kuidas on kahes Eesti avaliku sektori organisatsioonis üles ehitatud ostuarvete menetlemise protsess, millised on kasutusel olevad kontrollimehhanismid ning kus võivad avalduda töökorralduslikud haavatavused. Analüüs ühendab teoreetilises raamistikus tuvastatud haavatavused ja turvameetmed intervjuude empiiriliste leidudega ning kõrvutab neid uuritavate organisatsioonide töökorralduslike dokumentidega, võimaldades seeläbi hinnata, mil määral vastavad praktikas rakendatud meetmed teoreetilistele soovitudele. Kumbki uuritav organisatsioon ei ole magistritöö autorile teadaolevalt arvepettuse ohver olnud. Seetõttu hinnatakse turvameetmete tõhusust teoreetilisel raamistikul põhineva protsessianalüüsi kaudu ning analüüsitakse, kas rakendatud

meetmete olemus ja ulatus on arvepettuste tõkestamiseks asjakohane ja piisav. Alapeatükk lõpeb magistritöö autori poolt koostatud soovitusetega arvepettuste ennetamiseks.

RTK ja tema finantsarvestusteenuse klientide vahelist koostööd reguleerib iga ministeeriumi jaoks eraldi koostatud toimetamudel (RTK, 2023), milles on määratletud osapoolte rollid, vastutus ja tööjaotus, sealhulgas maksefailide esitamise tähtsajad. RTK talituse juhataja sõnul peavad klientasutused edastama RTK-le arved vähemalt neli päeva enne maksetähtaega. Justiitsministeeriumi valitsemisala toimetamudeli järgi peavad arved jõudma SAP-i hiljemalt neli tööpäeva enne maksetähtaega. Sellest tulenevalt eeldab protsess, et juhul kui kliendi poolt edastatakse arve RTK-le minimaalse lubatud ajavaruga, peab RTK raamatupidaja tegema vajalikud toimingud samal tööpäeval.

Eesti avaliku sektori organisatsioonidel on vastavalt Raamatupidamise seadusele kohustus riigisiseste tehingute korral aktsepteerida üksnes e-arveid. Piirangu eesmärk on ühtlustada arvete menetlemise protsesse ning vähendada käsitsi andmesisestusega kaasnevat ajakulu ja vigade tekkimise riski. E-arve on ühtse standardi alusel koostatud masintöödeldav majandustehingut tõendav algdokument, mille digitaalne töötlemine aitab tagada tehingute turvalisuse ja tõhususe (ITL, 2013).

Intervjuude põhjal selgus, et arvete menetlemiseks kasutatakse kahte omavahel integreeritud infosüsteemi, mille kasutustingimused ja -juhendid on avalikult kättesaadavad RTK veebilehel. FitekIN (edaspidi Fitek) on arvete haldamise tarkvara, kus toimub e-arvete vastuvõtmine, nende suunamine menetlusse, kinnitusringide haldamine, konteerimine ning arvete edastamine SAP-i (RTK, 2021). SAP on ressursiplaneerimise infosüsteem ehk majandustarkvara (*enterprise resource planning*, ERP). Ostuarvete menetlusprotsessi kontekstis kasutatakse SAP-i hankijate andmete loomiseks ja haldamiseks, arvete käsitlemiseks, maksefailide koostamiseks ning pangaandmete töötlemiseks (RTK, 2024b, 2026). Koostatud maksekorraldused edastatakse Rahandusministeeriumi valitsemisalas tegutsevasse Riigikassasse, mis haldab riigiasutuste makseid, juhib rahavoogusid ning korraldab finantsvarade ja kohustuste juhtimist. (RAM, 2021).

RTK talituse juhataja kinnitas, et Eesti-sisesed arved edastatakse riigiasutustele üksnes e-arve operaatorite kaudu. Tema sõnul:

„Seadus näeb ette, et avalik sektor võib võtta vastu ainult e-arveid. Arve ei saa liikuda otse käest kätte.” (RTK I1)

Kliendipoolne esindaja kinnitas sama põhimõtet, mille järgi on e-arveldamine ainus võimalus (RIT I1).

Menetlusahelasse sisenemiseks on vajalik kasutada e-arve operaatorit, mille kasutamine eeldab isiku tuvastamist ja ettevõtte registrikoodi edastamist. Turvanõue ei kõrvalda arvepettuse riski täielikult, kuid piirab Eesti-sisesel arvete edastamisel olulisel määral teoreetilises raamistikus käsitletud makseandmete võltsimise ja e-kirja manusega manipuleerimise skeemide toimivust.

Välisarvete menetlemise protsess erineb mõnevõrra Eesti-siseste arvete omast. Kuna Eesti seadus ei laiene välisriikide ettevõtetele, saabuvad välisarved klientasutuse töötaja e-posti aadressile, kes edastab need seejärel Fiteki digiteerimisaadressile. See muudab arve digitaalseks ehk automaatika abil koostatakse PDF-arvest XML-formaadis masinloetav e-arve. Fitek arvekeskuse juhend täpsustab, et digiteerimisaadressile saab saata üksnes PDF-vormingus manuseid ning arved tuleb digiteerimisele saata asutuse enda meiliaadressilt. (RTK, 2021). RIT arvestusspetsialist (I1) kinnitas protsessi samamoodi:

„Kuna nemad meie e-arve keskkonda kasutada ei saa, siis nemad peavad saatma PDF-kujul arve. Kulujuht saadab seejärel digiteerimisele ning Fiteki keskkond ise muudab selle e-arveks.”

Arve saatmine kulujuhi e-postkastist Fitek digiteerimisaadressile on protsessis koht, kus sisendi usaldusväärsuse hindamine toetub inimese subjektiivsele hinnangule, mitte süsteemi tehnoloogial põhinevale kontrollmehhanismile. Teoreetilises raamistikus on rõhutatud, et just sellised etapid loovad eelduse pettuste realiseerumiseks, kuna arvepettused kasutavad sageli usaldusel põhinevaid suhtluskanaleid (Al-Musib et al., 2023; Atlam & Oluwatimilehin, 2023).

Fiteki juhendi järgi kuvatakse arvetel, mille tarnijal puudub SAP-i hankijakood, silt „Uus tarnija” ning selliste arvete puhul edastatakse tarkvarakonsultandile automaatne teavitus hankija loomiseks (RTK, 2021). RTK talituse juhataja (I3) kinnitas kontrollimehhanismi praktikas rakendamist ja toiminguga kaasnevat kontrollikihti järgmiselt:

„Nemad vaatavad veel kolmanda pilguga üle, kas soov tundub loogiline.”

RTK tarkvarakonsultant (I4) kirjeldas protsessi üksikasjalikumalt, mille järgi makseandmete muutumise või uue hankija lisandumisel küsitakse kliendilt kooskõlastust enne SAP kirjete loomist:

„Enne ma SAP-is mitte mingit liigutust ei tee, kui mul ei ole vastust. Ma olen väga järjekindel selles.”

Mõlema organisatsiooni töötajad kinnitasid, et ostuarvete menetlemine on mitmeastmeline protsess ning tugineb selgele tööjaotusele teenuseosutaja ja kliendi vahel. RIT-is algatab arvestusspetsialist kinnitusringi, kasutades vajalike osapoolte tuvastamiseks arvelt saadud infot. Kinnitusring on üles ehitatud summapõhiselt. Osapoolte arv sõltub ostutehingu väärtusest: kuni 14 999 euro suurused kulud kinnitab kulujuht, kes kontrollib arve sisulist vastavust ning lisab e-arve keskkonnas arvele juurde eelarvererea viite. 15 000 kuni 49 999 euro piires lisandub ka eelarvejuhi kinnituse nõue ning üle 50 000 euro väärtusega arved vajavad direktori heakskiitu (RIT, 2025). Protsessijuhendi vooskeemi järgi läbitakse kõik sammud enne järgmisele kinnitustasemele jõudmist ning ühtegi etappi ei ole võimalik vahele jätta. Intervjueeritav kinnitas:

„Kõik, kes peavad seal olema, need ka kinnitavad. Kinnitusringist me ei lähe mööda.“
(RIT I2)

Selline ülesehitus vastab teoreetilises raamistikus käsitletud ülesannete lahususe põhimõttele (Ziorklui et al., 2024), mis vähendab riski, et üks isik saab vastu võtta suure rahalise väärtusega otsuseid iseseisvalt.

Intervjuude põhjal osaleb RTK poolel protsessis vähemalt kolm osapoolt: raamatupidaja, kes kontrollib arvet Fitekis ja edastab SAP-i; maksefailide koostaja; maksete panka edastaja. Vajaduse korral kaasatakse neljas lüli – SAP tarkvarakonsultant. Intervjuudes kirjeldatud protsess on kooskõlas Fitek ja SAP juhenditega (RTK, 2024a, 2024b, 2026). RTK tarkvarakonsultant kinnitas, et kasutusel olev mitmeastmeline arvete kinnitamine on tõhus viis vigade tuvastamiseks ja pettuste ennetamiseks:

„Mina usun, et erasektoril ei ole sellist kontrollmehhanismi, nagu on meil. Meil tõesti väga paljud silmad vaatavad.“ (RTK I4)

Olulise leiuna tuvastati intervjuudega, et kinnitusringist ei minda mööda ka kiireloomuliste maksete korral. RIT-i arvestusspetsialist vastas põhimõttekindlalt:

„Jah, kohustuslik, sellest me ei lähe mööda. Sellisel juhul jääbki arve õigel ajal maksmata.“ (RIT I2)

RTK talituse juhataja kinnitas protsessi teise osapoole perspektiivist, et kiireloomuliste maksete korral pigem suureneb osalejate arv, mitte ei vähendata kohustuslikke etappe:

„Ka kiireid asju saame menetleda Fiteki kaudu. Kui on tõesti vaja täna maksta, siis on juba seal rohkem inimesi kaasatud. Me talituse siseselt konsulteerime omavahel.” (RTK I3)

Ärikirjapettuste korral on kiireloomulisus üks levinumaid psühholoogilisi mõjutusvõtteid (Khursheed et al., 2020; Ferreira et al., 2020), mistõttu on see empiiriline leid turvalisuse seisukohalt oluline. Pigem toob kiire makse kaasa täiendavat tähelepanu.

Vastutuse jaotuses on mõlema osapoolle arusaam ühine: arve sisuline kontroll on kliendi kohustus. See on ametlikult kokku lepitud RTK ja ministeeriumi vahel kehtestatud toimetamisel. RTK talituse juhataja sõnastas põhimõtte järgmiselt:

„Seda meie, RTK poolt hinnata ei saa, sest meie ei ole olnud kaasas tellimisel. Meie jaoks on see juba kindlus, et ta on käinud läbi nende inimeste käest, kes on seda tellinud.” (RTK I1)

RIT arvestusspetsialist kinnitas vastutust arve sisuõigsuse ees ning rõhutas, et kulujuht peab tehingu korrektsuse hindamiseks võrdlema arve sisu lepinguga (RIT I1). Arvestusspetsialisti sõnul ei eelda kinnitusring pangakonto numbri õigsuse kontrollimist.

„Seda kohustust me ei ole pannud, et kulujuht vaataks lepingus välja toodud arvelduskonto numbrit.” (RIT I1)

Hüpoteetilise stsenaariumi puhul, kus arve sisu, summa ja tarnija näivad korrektsed, kuid kontonumber on muudetud, hindas RIT, et kliendi poolel sellist kõrvalkallet tõenäoliselt ei tuvastataks, küll aga märkaks seda RTK raamatupidaja (RIT I2). RTK raamatupidaja kinnitas, et tema ülesannete hulka kuulub e-arve keskkonnas arve rekvisiitide, summa ja raamatupidamise konteeringute kontrollimine (RTK I2). See loob organisatsioonidevahelise usaldusahela, kus teenuseosutaja tugineb kliendi tehtud sisulisele kontrollile, samal ajal klient eeldab, et makseandmete korrektsuses veendub teenuseosutaja. Tegemist on varasemas kirjanduses jagatud teenuste mudeli puhul esile toodud ohukohaga, kus osapoolte vastastikused eeldused võivad jätta tähelepanuta olukorra, mis vajab terviklikku ülevaadet protsessist (Herbert & Seal, 2011; Raudla & Tammel, 2015). Siiski on intervjuuandmed kooskõlas toimetamisel kehtestatud kokkuleppega, mille järgi vastutab RTK õige maksetähtaja, makse summa ning makse saaja pangakonto eest SAP-is, samas kui asutus vastutab majandustehingu toimumise õiguspärasuse, saadud kaupade ja teenustega seotud info õigsuse ning arvestusobjektide eelarvereeeglitele vastavuse eest

Välishankijate andmete kontrollimine toimub RTK-s eraldiseisva protsessina. SAP tugimeeskonnas tegutsev RTK tarkvarakonsultant kinnitas, et juhul kui saadud arve kontonumber või nimi ei vasta varasemalt sama tarnija juures kasutusel olevatele andmetele, tuvastab SAP mittevastavuse. Seejärel edastab konsultant RTK raamatupidaja kaudu kliendile korralduse valideerida makseandmete muudatus koostööpartneriga üle:

„Mina saadan RTK raamatupidajale teavituse, et seoses arvepettustega, palun kooskõlastada arve esitajaga panga andmed.” (RTK I4)

Intervjuueritav täpsustas, et kooskõlastus on vajalik ka uue tarnija lisandumisel ning kinnitas järjekindlalt, et turvanõuete osas järeleandmisi ei tee:

„Ennem ma SAP-is mingit liigutust ei tee, kui mul ei ole vastust.” (RTK I4).

Tarkvarakonsultant tõi samuti esile, et ta ei aktsepteeri kliendi vabas vormis edastatud kooskõlastust ning talle on seetõttu edastatud ka arve esitaja pangapoolseid kinnitusi. Samuti kontrollib ta andmete õigsust riikide registrite ja teiste avalike allikate abil ning eurot kasutavate riikide puhul valideerib internetipanga kaudu saaja nime ja arvelduskonto vastavust (RTK I4).

Kontrollimehhanismi tõhusust illustreerib raamatupidaja poolt kirjeldatud juhtum, kus regulaarne liikmemaks oli varasemalt tasutud Inglismaa pangakontole, kuid ühel arvel oli märgitud Poola kontonumber. Kuna kontot ei olnud SAP hankijakaardil registreeritud, suunas süsteem arve tagasi Fitekisse. Seejärel veenduti muudatuse õigsuses kliendi käest põhjendust küsides ning SAP-i spetsialisti poolt täiendavalt internetipõhist taustauuringut tehes (RTK I2). Juhtumiga ilmnes, et kontrollimehhanism toimis: kontonumbri muutus tekitas süsteemis tõrke, kõrvalekallet märgati ning selle kinnitamiseks kasutati täiendavat kontrolli. Siiski ilmnes intervjuudest, et RTK-s puudub kirjalikult kehtestatud protseduur alternatiivse kanali kasutamiseks selliste muudatuste kontrollimisel. RTK talituse juhataja selgitas:

„Sellele tuleb terve mõistusega läheneda.” (RTK I3)

Ka tarkvarakonsultandi sõnul ei ole tema poolt isiklikult tuvastatud ja regulaarselt rakendatavad ning senise kogemuse põhjal tõhusalt toimivad kontrollimehhanismid kirjalikult kehtestatud ega organisatsiooniüleselt standardiseeritud. Teadmine ja vilumus on kujunenud praktilise kogemuse kaudu, mistõttu ei ole lihtsasti kolleegidele jagatav:

„Enam ei oska seda infot ka edasi teistele anda, et mida ma vaatan ja kuidas ma vaatan. Mul on mõned asjad juba automaatselt käe sees.” (RTK I4)

Intervjueritav täiendas, et osakonnas toimib tõhus koostöö ning uusi tähelepanekuid ja võimalikke ohukohti jagatakse üksteisega regulaarselt. (RTK I4).

Sarnane lähenemine ilmnes ka RIT-is. Arvestusspetsialist kirjeldas partneri pangakonto muudatuse juhtumit, mille puhul veenduti muudetud makseandmete õigsuses eelnevalt teadaoleva allika abil:

„Me kirjutasime enda välja otsitud kontaktile, kes meil lepingus on välja toodud. Me selliseid üldaadresse üldjuhul ei usaldanud ka varem.” (RIT I1).

Kuigi alternatiivset suhtluskanalit, mida nii Junger et al. (2020), Myojin & Babaguchi (2020) kui Václavík et al. (2025) on esile toonud olulise ennetusmeetmena, uuritavates organisatsioonides praktikas kasutatakse, põhineb selle rakendamine eelkõige töötaja initsiatiivil ja teadlikkusel ning riskitajul. Loogikale tuginemine on nõrgem kaitsemeede kui selgelt määratletud kohustuslik protseduur, kuna ei pruugi olla piisav erandlikes olukordades, kus puuduvad varasemad kontaktandmed koostööpartneri kohta. Samuti ei taga ühe töötaja kogemusel ja teadmistel põhinevad kontrollimehhanismid jätkusuutlikkust puhkuste ja asenduste korral või töötaja ootamatul lahkumisel organisatsioonist (Ogwo-Ude et al., 2023; Ziorklui et al., 2024). SAP ostumooduli juhend kirjeldab küll uue hankija loomise protsessi, kuid ei täpsusta, milliseid täiendavaid kontrole peab SAP tugitiim muutuvate ohtude kontekstis rakendama (RTK, 2024b). Organisatsiooni vastupanuvõime selles etapis toetub personaalsel teadlikkusel, mitte protseduurilistel kontrollimehhanismidel.

Kaks olulist täiendavat kontrollimehhanismi, mida teoreetiline raamistik ei käsitle eraldiseisvalt, kuid mis ilmnesid empiirilisest analüüsist, on RIT-is rakendatav eelarvestamise ja üleandmise-vastuvõtmise akti nõue. RIT finantsprotsesside juhendi järgi on kulujuhi ülesanne kontrollida arve sisulist vastavust lepingule või aktile. Lepingulise vastavuse kinnitamiseks lisab ta e-arvele juurde sobiva eelarverea viite. Juhul kui arve väljastamise aluseks on kahepoolse akti olemasolu, siis lisab ka allkirjastatud aktile viitava dokumendihaldussüsteemi veebiaadressi. RIT arvestusspetsialist selgitas reegli majanduslikku vaatenurka:

„See on kinnitus, et raha on eelarvestatud.” (RIT I1)

Lepingulise teenuse puhul tähendab akti kohustus, et fiktiivse arve alusel makse tegemine eeldaks allkirjastatud dokumendi olemasolu, mida pettuse korral ei ole võimalik esitada. Seda täiendab RTK talituse juhataja märkus, et avaliku sektori eelarvedistsipliin sunnib organisatsioone iga makset hoolikalt jälgima, kuna eelarve on piiratud (RTK I3).

Intervjuus ilmnes, et eelarvedistsiipliini järgimise vastutus on finantsosakonnal tugevam kui sisuosakondades, mistõttu teevad arvestusspetsialistid pisteliselt täiendavat kontrolli. Käitumuslikku valvsust illustreerib ka arvestusspetsialisti kirjeldus ebatavalise arve kohta:

„Meile tuli üks arve, mis oli pool vene keeles, pool eesti keeles. Kuna seal ei olnud ühtegi nime, kellele see arve peab kuuluma, kirjutasin firmasse ja küsisin, kas see on teie poolt saadetud arve. Ma ei saanud vastust ja kustutasin selle arve ära.” (RIT I1)

Pärast maksetähtaja möödumist selgus, et tegemist oli seadusliku ostutehinguga ning teenuse tellinud isik palus partneril esitada parandatud arve.

RTK tarkvarakonsultant hindas lepingus kehtestatud tingimuste abil protsessi kaitsmist üheks tõhusaimaks meetmeks. Ta soovitab teenust tellides kokku leppida, millisele arvelduskontole makstakse ning fikseerida põhimõte, et kontonumber ei tohi kehtivuse jooksul muutuda. Intervjueeritav kirjeldas näitega turvanõude ranget järgimist:

„Oli juhus, kus mina ei olnud nõus andmeid sisestama. Klient saatis varasemalt pildi lepingust, kus oli on teine IBAN. Seal oli kirjas, et ei tohi muutuda kontonumbrid. Miks partner muutis?” (RTK I4).

Ostuarvete menetlemise lõppfaasis lisandub protsessi pangapoolne täiendav kontroll. Kui makse saaja nimi ja kontonumber ei vasta teineteisele, siis raamatupidaja sõnul tagastatakse makse (RTK I2). RTK tarkvarakonsultant kinnitas, et alates 2025. aasta oktoobrist on pangakonto numbri ja nime vastavuse kontroll kohustuslik kõigile Eesti-sisestele maksetele. Välisarvete puhul on nõuded veelgi rangemad, hõlmates lisaks saaja aadressi ning teatud riikide puhul ka telefoninumbri esitamist. Siiski tõi ta täiendavalt esile piirangu, mis vähendab selle kontrolli täielikku efektiivsust:

„Salvestatud maksekorralduste kontroll saaja ja IBAN-i vahel toimub öö jooksul. Seal on ohukoht, kuna kohese täitmisega maksed võivad minna läbi ilma täiendava kontrollita.” (RTK I4)

Intervjueeritav selgitas, et kontrollimehhanism toimib tõhusalt juhul, kui maksekorraldus koostatakse eelnevalt ning täidetakse kõige varasemalt järgmisel päeval. Selline praktika toimib ka teoreetilises osas käsitletud protsessi aeglustava mehhanismina.

Induktiivse leiuna ilmnes samuti, et ka Riigikassa likviidsuse planeerimise protsess piirab erakorraliste ja ajasurvel põhinevate maksete tegemise võimalust. Ööpäeva maksete

summale on kehtestatud limiit, mistõttu ei ole vabad vahendid igal hetkel kättesaadavad (RTK I1).

Töökoormusega seotud riskid avaldusid intervjuudes erinevalt. RTK talituse juhataja hinnangul aitab rollide selge jaotus hoida töökoormust kontrolli all, kuna arvetega tegelev töötaja ei pea samaaegselt täitma teisi finantsarvestuse ülesandeid (RTK I3). Raamatupidaja kinnitas, et kuigi töömaht suureneb periooditi – näiteks kuu alguses ning puhkuste ja asenduste ajal – on see üldjuhul hallatav (RTK I2).

RIT-i puhul on arve sisulise korrektsuse hindamine kulujuhtide ülesanne ning mõnes osakonnas võib sellega kaasnev töökoormus olla märkimisväärne. Arvestusspetsialist tõi näitena välja, et ühe konkreetse kulujuhi menetleda võib olla mõnel perioodil kuni 200 arvet kuus ning teisel kulujuhil esineb aeg-ajalt arveid, millel võib olla kuni sada rida, mille õigsust tuleb eraldi kontrollida (RIT I2). Teoreetilises raamistikus käsitletud lähenemise kohaselt soodustavad suur töökoormus ja rutiinsed tööülesanded heuristilist otsustamist (Jones et al., 2019; Junger et al., 2020), mistõttu võib suure töökoormusega kaasneda risk, kus tähelepanu koondub tavapärastele vigadele, samas kui harva esinevad kõrvalekalded jäävad märkamata. Võimalikku tähelepanematuses tulenevat riski aitab siiski leevendada kinnitusringi mitmeastmelisus.

Teoreetilises kirjanduses on esile toodud tajutud turvalisuse efekti, mille kohaselt hästi toimivad IT-süsteemid võivad vähendada mittetehniliste ohusignaalide märkamist (Greulich et al., 2024; Schneier, 2008). RIT arvestusspetsialist kinnitas sarnast arusaama:

„Seda märkab kindlasti RTK raamatupidaja. Meie pigem mitte.” (RIT I1)

See viitab, et RIT-i poolel on kujunenud usaldus RTK teenuse suhtes, mis võib viia olukorrani, kus enda kontrollimehhanismide tugevus väheneb.

Koolituste taseme osas on organisatsioonide hinnangud mõnevõrra erinevad. RTK talituse juhataja pidas olemasolevat teadlikkust piisavaks, rõhutades töökogemuse olulist rolli:

„Me oleme väga kaua seda tööd teinud. Mina märkan kogu aeg neid uudiseid. Võib-olla on tõesti see niinimetatud professionaalne kretinism.” (RTK I3)

Tema seisukoht on kooskõlas Junger et al. (2020) leiuga, mille kohaselt tuvastati 91% ebaõnnestunud pettusekatsetest töötajate tähelepanelikkuse kaudu. Samas on vajalik rõhutada, et erialane tähelepanelikkus on individuaalne ning ei ole ülekantav uutele töötajatele ega tagatud asenduste korral.

RIT arvestusspetsialist hindas olukorda pärast raamatupidamiskonverentsil kuuldot kriitilisemalt:

„Mulle tundus, et meil on võib-olla tõesti natukene see koolitus liiga üldine. Et see sobib tervele majale ja meile ka kindlasti, aga võib-olla rohkem sellistest juhtumitest, et milliseid arveid saadetakse.” (RIT I1)

RTK tarkvarakonsultant tunnistas, et tema enda teadlikkus pärineb peamiselt meediast, mitte koolitusprogrammidest:

„Ei ole mingeid koolitusi läbinud [arvepettuste ennetamiseks]. Ma tarbin meediat ja teen järeldused. Niimoodi ma selle teema peale sattusin ja enda ülesandeks võtsin.” (RTK I4).

See leid on teoreetilise kirjanduse seisukohalt oluline tõestus sellest, et organisatsioonide praegune koolitusvõimekus tugineb osaliselt üksikisikute isiklikule initsiatiivile, mis ei ole organisatsiooniliselt jätkusuutlik.

Mõlemas organisatsioonis viiakse läbi kohustuslikke infoturbekoolitusi, kuid koolituste maht ja regulaarsus erinevad märkimisväärselt. RTK töötajad läbivad infoturbekoolituse koos sellele järgneva testi üks kord aastas, samas kui RIT-i töötajatel on kohustus läbida infoturbe õpiampse igakuiselt. Siiski ei toonud ükski intervjuueeritavatest esile finantspersonalile suunatud arvepettuste stsenaariumipõhiseid koolitusi. Varasemad uuringud on näidanud, et üldised küberhügieenikoolitused ei pruugi valdkonnapõhiste ohtude kontekstis käitumuslikke harjumusi mõjutada (Iuga et al., 2016; Van Steen et al., 2020). Seega peavad koolitused olema kontekstipõhised, sisaldama praktilisi arvepettuste stsenaariume ning katma ka sisuosakondade kulujuhte, kes vastutavad arve sisulise kontrolli eest, kuid kelle finantspetuskeemide teadlikkus võib finantstöötajatest madalam olla.

Täiendava kaitsekihina tõi RTK talituse juhataja esile IT-teenusepakkuja poolt seadistatud e-posti turvapiirangud, mille tulemusel suunatakse osa kirju meililüüsi, kus kirja saaja peab nende turvalisust täiendavalt hindama. Selline lahendus on kooskõlas e-posti turvalisuse praktikatega, mille kohaselt rakendatakse meiliserveris autentimis- ja filtreerimisreegleid, et vähendada domeeni võltsimise abil loodud petukirjade edastamise võimalust.

Organisatsioonikultuuri tasandil kerkis esile RIT-i finantsarvestuse osakonna roll olemasolevate kontrollimehhanismide säilitamisel. Intervjuueeritava sõnul on püütud arvete menetlemise protsessi lihtsustada:

„Meie osakonda on püütud päris mitmel korral ära rääkida, et jätame eelarverea Fitekisse lisamise ära. Aga meie oleme raiunud just vastu, et see on juba turvalisuse pärast.”
(RIT I2)

Näide viitab sellele, et turvameetmed ei püsi organisatsioonis iseenesest. Kui meetmeid tajutakse tülikatena, võib tekkida surve nende lihtsustamiseks. Ziorklui et al. (2024) rõhutavad, et ilma juhtkonna selge toetuseta kandub turvameetmete säilitamise vastutus üksikisikutele. Intervjuude põhjal sõltub olemasolevate kinnitusringi reeglite säilimine finantsosakonna põhimõttekindlusest.

Magistritöö autor tõstas intervjuudes küsimuse RTK veebilehel avaliku sektori makseid koondava makseandmiku võimalikust kasutamisest ärikirjapettuste luureallikana. Rahandusministeeriumi (RAM, 2023) sõnul on andmete avaldamise eesmärk võimaldada ülevaadet sellest, kellelt ja millises mahus avalik sektor teenuseid ostab või toetusi maksab. Talituse juhataja selgitas, et makseandmike esitamise nõue tuleneb Justiits- ja Digiministeeriumi suunistest ning selle eesmärk on toetada korruptsiooniennetust, kuid RTK ei näe sellises ulatuses avalikustamisel otsest vajadust:

„Seal on tõesti väga avalik kõik, et igaüks võib vaadata kellele, kui palju, millal on makstud.” (RTK I3)

RIT-i poolt väljendati sarnast seisukohta:

„Võib-olla jah, et kui vaatad, kellega me tehinguid teeme, siis oma kurjad näpud sinna vahele toppida. Ma arvan, et tänapäeva maailmas ei peaks selliseid suuremaid tehinguid ja summasid pigem kõigile näitama.” (RIT I2)

Makseandmik võimaldab tuvastada tehingupartnerid, maksete regulaarsuse ja summad, mis on arvepettuse luurefaasis kasutatav sisend (Lazarus, 2025; Europol, 2025b). Seetõttu on põhjendatud küsimuse tõstatamine, kas korruptsiooniennetuse eesmärgil avalikustatava info ulatus on proportsionaalne sellega kaasnevate riskidega.

Intsidendide käsitlemise osas ilmnes, et RIT-i töötajal on üldine arusaam sellest, kelle poole pettuse kahtluse korral pöörduda, kuid puudub selgelt dokumenteeritud tegevusjuhised. Intervjueeritav kirjeldas olukorda järgmiselt:

„Ma arvan, et meil on lihtsalt omavahel kokku lepitud, et kui midagi on, teavitame esmalt osakonnajuhatajat, seejärel RTK raamatupidajat, Rahandusministeeriumi ja infoturvet.” (RIT I2)

Lisaks puudub RIT-il otsene ligipääs Riigikassa väljavõtetele, mis piirab pettuse iseseisvat kiiret tuvastamist. Václavík et al. (2025) juhtumiuuringus näidati, et just kiire panga teavitamine võimaldas ühel juhul pettuslik makse peatada. Selge juhise puudumisel võivad viibida kriitilised tegevused ja makse peatamine. Aeg on arvepettuse korral otsustava tähtsusega (RIA, 2024b).

Empiirilise analüüsi tulemused võimaldavad hinnata rakendatud meetmete struktuurset korraldust ja ulatust, kuid mitte nende tõhusust statistilises mõttes. Kuna tegemist on kvalitatiivse juhtumiuuringuga ning kumbki organisatsioon ei ole magistritöö autorile teadaolevalt arvepettuse kahju kannataja olnud, ei ole võimalik tõhusust reaalse juhtumianalüüsi kaudu hinnata. Pettuste mitte realiseerumine on kooskõlas sellega, et protsess sisaldab mitmeid tugevaid kontrollimehhanisme.

Kaudseks tõendiks meetmete toimivuse kohta on RTK tarkvarakonsultandi kinnitus pettuskatse mitteõnnestumise kohta:

„On olnud, aga need pole läbi läinud.” (RTK I4)

Analüüs tervikuna näitab, et nii RTK kui RIT on rakendanud mitmeid tugevaid töökorralduslikke turvameetmeid: kohustuslik mitmeastmeline kinnitusring, ülesannete lahusus, SAP tugimeeskonna täiendav kontroll välishankijate puhul ning erakorraliste maksete piirangud Riigikassa kaudu. Empiirilise analüüsi käigus tuvastati täiendavate kontrollimehhanismidena ka eelarvestamise nõue ja üleandmise-vastuvõtmise akti kohustus. Uuring kinnitas, et ärikirjapettuse realiseerumine ei ole üksnes tehniliste kontrollide abil ennetatav. Risk võib avalduda seal, kus töötaja peab hindama sisendi usaldusväärsust või üks osapool tugineb teise osapoole poolt teostatud kontrollile.

Kokkuvõtvalt joonistub välja kolm peamist nõrkust. Esiteks ilmneb osapooltevaheline vastutuse hajumine. Jagatud teenuste mudel loob organisatsioonidevahelise usaldusahela, kus teenuseosutaja tugineb kliendi tehtud sisulisele kontrollile, samal ajal klient eeldab, et makseandmed kontrollitakse teostatakse teenuseosutaja poolt. Kuigi mõlemad eeldused on eraldi vaadatuna põhjendatud, võib nende vahele jääda erandlik ning kurjategijate poolt osavalt manipuleeritud olukord. Oht avaldub eeskätt protsessi algfaasis, kus uued makseandmed sisestatakse süsteemi, sealjuures andmete muutmise kinnitus saadetakse kliendile tarnija kompromiteeritud e-posti kontolt.

Teise nõrkusena kerkis esile alternatiivse kanali kasutamise kohustusliku protseduuri puudumine. Kuigi intervjuudest selgus, et töötajad on praktikas kasutanud erinevaid allikaid andmete kontrollimiseks, on see toimunud peamiselt individuaalse hinnangu ja kogemuse,

mitte ühtselt kehtestatud reeglite alusel. Protseduurilise reegli puudumine muudab kaitse sõltuvaks üksikisiku teadlikkusest, mis ei ole personalivoolavuse ega kõrge töökoormuse tingimustes jätkusuutlik.

Kolmanda nõrkusena toob autor välja valdkonnaspetsiifiliste koolituste puudumise. Olemasolevad koolitused keskenduvad peamiselt üldisele küberturbe teadlikkusele ega käsitle piisavalt arvete menetlemisega seotud petuskeeme ega töötajate reageerimisvõimet realistlikes olukordades. Eriti murettekitav on, et praegune valdkonnapõhine teadlikkus pärineb olulises osas üksikisikute isiklikust meediatarbimisest ja töökogemusest.

Tulemused näitasid, et uuritud organisatsioonides rakendatud meetmed on võimaldanud tuvastada tavapärase makseandmete muutmise. Empiirilise uuringu põhjal võib järeldada, et olemasolevad töökorralduslikud meetmed kaitsevad lihtsamate arvepettuste eest, kus ründaja tugineb üksnes e-kirja teel edastatud pettuslikule arvele. Kinnitatud pettusjuhtumi puudumine ei võimalda statistilist tõhususe hindamist, kuid osutab, et kontrollimehhanismid on seni toiminud või et uuritud organisatsioon ei ole sihitud. Keerukamate rünnete puhul, näiteks tarnija e-posti konto tegeliku kompromiteerimise korral, kus kogu suhtlus toimub usaldusväärse kanalina näiva e-posti konto kaudu, ei ole pettuste samaväärne tuvastamine kindel. Tabel 4 annab kokkuvõtliku ülevaate uuringu käigus tuvastatud haavatavustest, viitab empiirilisele alusele ning esitab protsessi täiendavaks kaitsmiseks sobivad kontrollimehhanismid.

Tabel 4.

Empiiriliselt tuvastatud haavatavuste leevendamiseks soovitatavad meetmed

Nr	Haavatavus	Empiiriline alus tsitaadina	Soovitus organisatsioonidele	Seos teoreetilise raamistikuga
1	Välisarved saabuval kliendile PDF-formaadis.	<i>„Peavad saatma PDF-kujul arve“; „Klient saadab Fitekiisse“.</i>	Käsitleda PDF-arveid kõrge riskiga arve-liigina. Kehtestada kontrollimiseks eraldi reeglid.	Olemasoleva kirjavahetuse usaldamine (Bonhard et al., 2025; Václavík et al., 2025).
2	Alternatiivse kanali kasutamine ei ole kehtestatud kohustusliku nõudena.	<i>„Sellist reeglit ei tea“; „Tuleb terve mõistusega läheneda“.</i>	Kehtestada reegel, et makseandmete muudatus kinnitatakse üksnes eelnevalt teadaoleva ja kokkulepitud suhtluskanali kaudu. E-kirja asemel eelistatavalt telefonikõnega.	Verifitseerimise nõrkus (Junger et al., 2020; Myojin & Babaguchi, 2020;).
3	Kontonumbri kontroll ei ole klientasutuse kontrolli osa.	<i>„Kulujuhil ei ole kohustust vaadata lepingus olevat arvelduskontot“; „Meie pigem ei märka“.</i>	Määratleda ja selgelt kokku leppida, kuidas kontrollib arve rekvisiitide muutumise korral klient sisendandmete õigsust.	Rollide hajumine ja vastutuse jaotus (Almutairi et al., 2025b; Ziorklui et al., 2024).

4	Uue tarnija loomisel puudub varasem võrdlusbaas.	„Välisarve esmakordsel tasumisel ei liigu arve Fitekist enne edasi, kui IT loob hankija“.	Uue tarnija loomist käsitleda kõrge riskina ning kehtestada andmete kontrollimise viisid.	Riskide paiknemine protsessi algfaasis (Zaporowska & Szczepański, 2024).
5	Fitek loeb PDF-arve pealt sisse uued andmed.	„Fitek ei tuvasta muutust, vaid tuvastab andmed, mis on arve peal“.	Lisada arvekeskusesse automaatne teavitus, kui arvel olev kontonumber erineb hankijakaardil olevast.	Tajutud turvalisus; tehnoloogia ülemäärane usaldamine (Greulich et al., 2024; Modic & Lea, 2013; Slifkin & Neider, 2023)
6	Kodumaiste hankijate andmeid saavad finants-spetsialistid lisada.	„Ma saan tarnijate registris muuta kõike. Pangakontot, nime ja registrikoodi“.	Kehtestada andmete muutmisele täiendavad piirangud.	Ülesannete lahusus (Almutairi et al., 2025b; Ziorklui et al., 2024).
7	Kinnitusringi reeglite leevendamisele tekib organisatsiooni-sisene surve.	„On püütud veenda, et jätame selle ära“.	Juhtkonna toel põhjendada kontrollimehhanismide säilitamise vajadust.	Organisatsioonikultuur; juhtkonna roll (Ziorklui et al., 2024).
8	Koolitused on üldised ega keskendu arvepettuste stsenaariumidele.	„Raamatupidamiskonverentsil räägiti nendest ohtudest ja imelikust arvetest. Ja mulle tundus, et meil on võib-olla tõesti see koolitus liiga üldine“.	Valdkonnaspetsiifilised koolitused, mis sisaldavad realistlikke stsenaariume (muutunud arvelduskonto, kompromiteeritud konto, kiireloomuline makse).	Tähelepanelikkus, riskitaju (Bada et al., 2015; Goel et al., 2017; Halevi et al., 2015; Van Steen et al., 2020).
9	Kõrge töömaht võib vähendada erandite märkamist.	„Mõnel arvel on kuni 100 rida“.	E-arve süsteemi tuleks luua riskipõhised märguanded ja eranditega seotud reeglid.	Töökoormus, heuristiline otsustamine (Iuga et al., 2016; Jones et al., 2019).
10	Kiireloomulised maksed.	„Kinnitusringist ei minda mööda“; „Kiire makse toob lisasuhtluse“.	Säilitada põhimõte, et kiireloomulisus suurendab kontrolli.	Ajasurve tekitamine (Khursheed et al., 2020; Ferreira et al., 2020).
11	Makseandmik toetab luuretegevust.	„Igaüks võib vaadata, kellele, kui palju on makstud“.	Avaliku teabe avaldamisel tuleb hinnata positiivse ja negatiivse mõju vahelist tasakaalu.	Luuretegevus; avaliku teabe kuritarvitamine (Bonhard et al., 2025; Lazarus, 2025).
12	Intsidendi käsitlemise protsess ei ole ühtselt kehtestatud.	„Lihtsalt omavahel kokku lepitud“.	Eksisteerima peab arusaadav ja praktiline tegevusjuhis.	Intsidendi kiire avastamine ja kahju piiramine (Junger et al., 2020; Václavík et al., 2025).

Allikas: autori koostatud intervjuuandmete ja teoreetilise raamistiku põhjal.

Magistritöö empiiriline panus seisneb eelkõige arvepettustega seotud ohukohtade kaardistamises ostuarvete menetlemise protsessis ning nende leevendamiseks rakendatavate kontrollimehhanismide süstematiseerimises. Analüüsi põhjal ilmneb, et risk seisneb sisendandmete valideerimises ja osapoolte eeldustes. Seetõttu peaksid arvepettuste ennetamise soovitusel keskenduma kogu protsessile, alates arve saabumisest ja tarnija andmete loomisest kuni makse kinnitamise ja võimaliku intsidendi lahendamiseni.

Uurimuse tulemuste tõlgendamisel tuleb arvestada mitmete piirangutega. Esiteks on tegemist kvalitatiivse üksikjuhtumi uuringuga, mille eesmärk ei ole statistiline üldistamine, vaid protsessipõhine mõistmine. Kuigi arvete menetlemisega seotud töökorralduslikud praktikad ja protsessi kaitsmiseks suunatud meetmed on tõenäoliselt sarnased ka teistes organisatsioonides, võib konkreetsete haavatavuste avaldumine ning kontrollimehhanismide rakendamise võimekus erineda.

Teine piirang seisneb olemasoleva teaduskirjanduse fookuses. Varasemad uuringud käsitlevad ärikirjapettusi peamiselt tehniliste ja psühholoogiliste aspektide kaudu, mistõttu oli piiratud hulk allikaid, mis käsitleksid teemat tööprotsessidega seotud haavatavuste vaatenurgast. Sellest tulenevalt oli teoreetilise raamistiku kujundamisel vajalik kaasata ka teaduskirjandust, mis käsitleb ärikirjapettustele sarnaseid nähtusi, nagu õngitsemine (*phishing*) ja harpuunimine ehk sihitud õngitsemine (*spear phishing*) (Cybernetica, n.d.-c), tarneahela turvalisus ning organisatsioonide sisekontrollid. Selline lähenemine võimaldas koguda sisukamat teavet protsessipõhiste riskide ja turvameetmete mõistmisel.

Kolmanda piiranguna tuleb arvestada, et uuritav teema hõlmab tundlikku finants- ja infoturbealast teavet. Seetõttu võivad intervjueeritavad teavet valikuliselt esitada. See piirab teatud määral võimalust käsitleda kõiki nähtuse mõistmiseks vajalikke aspekte.

Hoolimata uuringu piirangutest võimaldas empiiriline analüüs saada selge ülevaate sellest, milliseid töökorralduslikke kontrollimehhanisme on võimalik ostuarvete menetlemise protsessi kaitsmiseks rakendada. Empiiriline analüüs näitas, et uuritud organisatsioonides rakendatud töökorralduslikud meetmed toetavad tõhusalt tavapäraste arvepettuste ennetamist ja tuvastamist. Protsessis ilmneseid haavatavused, mis on seotud vastutuse hajumise, alternatiivsete kanalite puudumisega teabe täiendavaks valideerimiseks ning üksikisikute teadlikkusest sõltuvate kontrollimehhanismidega. Tulemused kinnitavad teoreetilises raamistikus käsitletud seisukohta, et ärikirjapettuste tõkestamine ei sõltu üksnes tehnilistest turvameetmetest, vaid organisatsiooni protsesside terviklikust ülesehitusest, ning süsteemselt kehtestatud ja standardiseeritud protsessijuhenditest.

Kokkuvõte

Magistritöö uurimisobjektiks oli arvepettus kui ärikirjapettuse alaliik, mille eripära seisneb selles, et rünne realiseerub organisatsiooni tavapärase ostuarvete menetlemise protsessi kaudu. Töö lähtekohaks oli probleem, et arvepettus on rahvusvaheliselt kujunenud ulatuslikku finantskahju põhjustavaks küberohuks. Sealjuures olemasolev teaduskirjandus keskendub peamiselt tehnilistele turvameetmetele ja psühholoogiliste mõjutusvõtete tuvastamisele. Arvete menetlemisega seotud töökorralduslike haavatavusi, nende leevendamiseks rakendatavaid kontrollimehhanisme ja meetmete tegelikku mõju on empiiriliselt uuritud vähem. Empiiriline analüüs võimaldas hinnata, mil määral vastavad uuritud organisatsioonides rakendatud kontrollimehhanismid teoreetilises raamistikus kirjeldatud töökorralduslikele turvameetmetele ning millistes protsessietappides võivad avalduda haavatavused.

Teoreetilise raamistiku koostamisel ilmnas, et ärikirjapettused on sotsiaalmanipulatsioonil põhinevad hübriidsed ohud, mille edukus sõltub erinevate tegurite koosmõjust. Varasemate käsitluste analüüs näitas, et arvepettuste õnnestumist soodustavad eelkõige olukorrad, kus kontrollimehhanismid põhinevad usaldusel või eeldusel, et tegemist on tavapärase ja rutiinse tööprotsessiga. Olulisemateks riskiteguriteks tõusid kirjanduse põhjal ülesannete lahususe ja alternatiivsete kontrollikanalite puudumine, töökoormusest tingitud kiire otsustamine, organisatsioonisisene surve kontrollide lihtsustamiseks, ebapiisav teadlikkus küberohtudest ning liigne usaldus tehniliste süsteemide vastu. Samuti rõhutas teoreetiline osa, et kõige tõhusamad kaitsemeetmed on mitmeastmelised ning ühendavad tehnilised meetmed töökorralduslike ja käitumuslikega.

Empiirilise uurimuse tulemused kinnitasid, et uuritud organisatsioonides on rakendatud mitmeid turvameetmeid, mis vastavad teoreetilises raamistikus käsitletud põhimõtetele. Ostuarvete menetlemise protsess põhineb standardiseeritud e-arveldusel, omavahel integreeritud infosüsteemidel ning mitmeastmelisel kinnitusringil. Uuringust selgus, et Eesti avaliku sektori kohustus kasutada e-arveid piirab märkimisväärselt selliste pettuste toimimist, mis tuginevad võltsitud e-posti aadressidel või manipuleeritud arvetel. Samuti näitas analüüs, et ülesannete lahususe põhimõte on uuritud organisatsioonides läbivalt rakendatud. Arvete menetlemises osaleb mitu erinevat töötajat ning suuremate summade või erandlike olukordade puhul lisanduvad täiendavad kontrollikihid. Olulise leiuna ilmnas, et kinnitusringist ei minda mööda ka kiireloomuliste maksete korral. Vajadusel kaasatakse

protsessi täiendavaid osapooli. Teoreetiline kirjandus käsitles ajasurvet ühe peamise ärikirjapettustes kasutatava mõjutusvõttena, mistõttu on empiiriline avastus oluline.

Uuringu käigus kaardistati ka protsessilised haavatavused, mis võivad luua eeldused arvepettuste realiseerumiseks. Kõige olulisemaks riskikohaks osutus organisatsioonidevaheline vastutuse hajumine. Kogutud andmete analüüs näitas, et jagatud teenuste mudelis tugineb teenuseosutaja kliendi tehtud sisulisele kontrollile, samal ajal kui klient eeldab, et makse seaduslikkust kontrollitakse teenuseosutaja poolt. Selline usaldusahel toimib tavapärastes olukordades tõhusalt, kuid võib jätta tähelepanuta stsenaariumid, kus arve sisu näib korrektne ja makseandmete muutmine kinnitatakse kompromiteeritud e-posti konto kaudu. Analüüs kinnitas, et risk avaldub eelkõige osapoolte eeldustes selle kohta, kes konkreetset kontrolli tegelikult teostab.

Teise olulise haavatavusena ilmnes alternatiivse suhtluskanali kasutamise kohustusliku protseduuri puudumine. Kuigi intervjuudest selgus, et töötajad kasutavad praktikas makseandmete muudatuste kontrollimiseks varasemalt teadaolevaid kontaktisikuid, ei olnud selline tegevus kirjalikult standardiseeritud. Samuti võib olla just selle kontakti e-posti konto kurjategijate käsutuses. Seega sõltub meetme rakendumine ning toimivus suurel määral töötaja kogemusest, ajaressursist ja tähelepanelikkusest. Teoreetiline raamistik rõhutas, et protseduurilised kontrollimehhanismid on tõhusamad, kui üksikisiku kogemusel tuginevad praktikad.

Kolmanda leiuna tõusis esile asjaolu, et uuritud organisatsioonides sõltub osa protsessi vastupidavusest konkreetsete töötajate teadlikkusel ja isiklikul initsiatiivil. Tugevalt ilmnes olukord uute tarnijaandmete loomise ja makseandmete kontrollimise etapis, kus olulised toimingud ei olnud dokumenteeritud ega organisatsiooniüleselt standardiseeritud. Varasemate uuringute põhjal käsitleti sellist olukorda organisatoorse haavatavusena, kuna ühe isiku põhised tegevused ei ole jätkusuutlikud.

Uuring näitas ka, et töökoormus võib mõjutada töötajate tähelepanelikkust. Eriti tõusis see esile olukordades, kus kulujuhid peavad menetlema palju arveid. Teoreetiline raamistik käsitles selliseid olukordi heuristilise otsustamise ohuna, kus tähelepanu keskendub tavapärastele vigadele ning harva esinevad kõrvalekalded võivad jääda märkamata. Samas aitas uuritud organisatsioonides seda riski leevendada mitmeastmeline kinnitusring.

Uurimuse teoreetilise osa üks oluline järeldus oli, et tehnilised süsteemid võivad luua töötajates liigse turvatunde, mis vähendab mittetehniliste ohusignaalide märkamist. Empiiriline analüüs kinnitas sarnast tendentsi ka uuritud organisatsioonides. Intervjuudest

ilmnes, et osa töötajaid eeldab, et võimaliku kõrvalekalde märkab mõni teine protsessiosaline või infosüsteem. See näitab, et tehnilised kontrollid võivad küll tugevdada protsessi turvalisust, kuid samal ajal vähendada individuaalset valvsust. Seetõttu kinnitab uuring käsitlust, mille kohaselt ei ole ärikirjapettuste tõkestamine üksnes tehniline küsimus, vaid sõltub organisatsiooni terviklikust töökorraldusest ja riskiteadlikkusest.

Empiiriline uuring võimaldas tuvastada ka mitmeid täiendavaid kontrollimehhanisme, mida töö esimene peatükk eraldi ei käsitletud. Nendeks olid näiteks eelarvestamise nõue, üleandmise-vastuvõtmise akti kohustus, arve lepinguline kontroll ning panga kaudu rakenduvad piirangud. Need meetmed toimivad täiendavate kontrollikihtidena, mis raskendavad pettuslike maksete realiseerumist. Samuti selgus uurimusega, et pangapoolse kontrolli tõhusus sõltub makse ajastusest.

Töös ilmnes ka vajadus arendada valdkonnaspetsiifilisi koolitusi. Kuigi mõlemas organisatsioonis viiakse läbi infoturbekoolitusi, keskenduvad need peamiselt üldisele küberhügieenile ega käsitle piisavalt arvete menetlemise protsessiga seotud keeruka iseloomuga petuskeeme. Mitmed intervjuueeritavad tõid välja, et nende teadlikkus arvepettustest pärineb peamiselt isiklikust meediatarbimisest ja töökogemusest. Varasema kirjanduse ülevaade viitas samamoodi sellele, et üldised infoturbekoolitused ei pruugi mõjutada töötajate käitumist spetsiifiliste ohtude kontekstis. Seetõttu peaksid koolitused sisaldama realistlikke arvepettuste stsenaariume ning hõlmama kõiki töötajaid, kes on arvete menetlemisega seotud.

Magistritöö peamine panus seisneb ärikirjapettuste ennetamiseks rakendatavate töökorralduslike turvameetmete võimaluste kaardistamises ning nende tegeliku kasutamise analüüsimises avaliku sektori ostuarvete menetlemise protsessis. Uuring näitas, et kaitsevõimekus sõltub protsessi terviklikust ülesehitusest, kus tehnilised, töökorralduslikud ja käitumuslikud kontrollimehhanismid toetavad üksteist. Analüüsi põhjal võib järeldada, et kõige tõhusamad meetmed ärikirjapettuste tõkestamiseks on tööülesannete lahusus, makseandmete sõltumatu valideerimine alternatiivsete kanalite kaudu, protseduuride standardiseerimine ning valdkonnaspetsiifiliste koolituste läbiviimine. Samuti näitas uuring, et organisatsioonide vastupidavus ärikirjapettustele sõltub olulisel määral sellest, kas turvameetmed on kehtestatud ametlike protseduuridena või põhinevad üksikisikute teadlikkusel ja kogemusel.

Viidatud allikad

1. Abbas, R., & Michael, K. (2026). Socio-technical theory: A review. In S. Papagiannidis (Ed.), *TheoryHub Book*. Retrieved from <https://open.ncl.ac.uk/theories/9/socio-technical-theory>
2. Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2018). Phishing attacks root cause. *Lecture Notes in Computer Science*.10694, 187–202. DOI: 10.1007/978-3-319-76687-4_13
3. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1), ty006. DOI: 10.1093/cybsec/tyy006
4. Al-Musib, N. S., Al-Serhani, F. M., Humayun, M., & Jhanjhi, N. Z. (2023). Business email compromise (BEC) attacks. *Materials Today: Proceedings*, 81(2), 497–503. DOI: 10.1016/j.matpr.2021.03.647
5. Almutairi, A. M., Kang, B., & Alhashimy, N. (2025a). Business email compromise: A comprehensive taxonomy for detection and prevention. In *Proceedings of the 2024 7th International Conference on Information Science and Systems*, 49–54. Association for Computing Machinery. DOI: 10.1145/3700706.3700714
6. Almutairi, A., Kang, B., & Alhashimy, N. (2025b). Business email compromise: A systematic review of understanding, detection, and challenges. *Computers & Security*, 158, 104630. DOI: 10.1016/j.cose.2025.104630
7. Annom, B. J. (2026, 19. jaanuar). *Kelmid petsid Eesti inimestelt välja 29 miljonit eurot*. Politsei- ja Piirivalveamet. Retrieved from <https://www.politsei.ee/et/uudised/kelmid-petsid-eesti-inimestelt-vaelja-29-miljonit-eurot-13196>
8. Arvutikuritegevusvastane konventsioon. (2001, 23. november). *RT II 2003*, 9, 32. Retrieved from <https://www.riigiteataja.ee/akt/78566>
9. Atlam, H. F., & Oluwatimilehin, O. (2023). Business email compromise phishing detection based on machine learning: A systematic literature review. *Electronics*, 12(1), 42. DOI: 10.3390/electronics12010042
10. Avaliku sektori finantsarvestuse ja -aruandluse juhend (2025, 3. jaanuar). Riigi Teataja I. Retrieved from <https://www.riigiteataja.ee/akt/103012025007>

11. Bera, D., Ogbanufe, O., & Kim, D. J. (2023). Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions. *Decision Support Systems*, 171, 113977. DOI: 10.1016/j.dss.2023.113977
12. Bonhard, S. K., Garcia Villalta, P., Rosés, O., & Pegueroles, J. (2025). A review of tactics, techniques, and procedures (TTPs) of MITRE framework for business email compromise (BEC) attacks. *IEEE Access*, 13, 50761–50776. DOI: 10.1109/ACCESS.2025.3552523
13. Braun, V., & Clarke. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. DOI: 10.1191/1478088706qp063oa
14. Braun, V., & Clarke. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, 11(4), 589–597. DOI: 10.1080/2159676X.2019.1628806
15. Bryman, A. (2012). Social research methods (4th ed.). *Oxford University Press*. Retrieved from <https://arunodayauniversity.ac.in/wp-content/uploads/2025/01/Social-Research-Methods-4th-Edition-Bryman.pdf>
16. Buse, J. H. M., Ee, J., & Tripathi, S. (2023). Unveiling the unseen wounds – A qualitative exploration of the psychological impact and effects of cyber scams in Singapore. *Psychology*, 14(11), 1728–1742. DOI: 10.4236/psych.2023.1411101
17. Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. *Routledge*. DOI: 10.4324/9781315679877
18. Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York, NY: HarperCollins.
19. Cidon, A., Gavish, L., Bleier, I., Korshun, N., Schweighauser, M., & Tsitkin, A. (2019). High precision detection of business email compromise. *Proceedings of the 28th USENIX Security Symposium*, 1291–1307. USENIX Association. Retrieved from <https://www.usenix.org/conference/usenixsecurity19/presentation/cidon>
20. Council of Europe. (2001). *Convention on Cybercrime (CETS No. 185)*. Retrieved from <https://rm.coe.int/1680081561>
21. Council of the European Union. (n.d.). *Cyber defence*. Retrieved from <https://www.consilium.europa.eu/en/policies/cyber-defence/>
22. Cybernetica AS. (n.d.-a). *Social engineering*. Retrieved from <https://akit.cyber.ee/term/290-social-engineering>

23. Cybernetica AS. (n.d.-b). *Phishing*. Retrieved from <https://akit.cyber.ee/term/44-kalastus-ongitsemine>
24. Cybernetica AS. (n.d.-c). *Spear phishing*. Retrieved from <https://akit.cyber.ee/term/1382-spearphishing>
25. Cybernetica AS. (n.d.-d). *Spoofing*. Retrieved from <https://akit.cyber.ee/term/971-spoofing>
26. Dave, S. (2019, 10. jaanuar). *How Chinese hackers pulled off the Italian job, a Rs 130-crore heist*. The Economic Times. Retrieved from <https://economictimes.indiatimes.com/tech/internet/how-chinese-hackers-pulled-off-the-italian-job-a-rs-130-crore-heist/articleshow/67458176.cms>
27. Dong, W., Meng, Y., Chen, J., & Ke, Y. (2025). Financial shared service centers and corporate misconduct: Evidence from China. *Journal of Business Ethics*, 199, 113–139. DOI: 10.1007/s10551-024-05825-6
28. Eesti Infotehnoloogia ja Telekommunikatsiooni Liit. (2013). *Eesti e-arve kirjelduse juhend: E-arve pankas saatmine ja e-arve presenteerimine pangas (versioon 1.05)*. Retrieved from https://wp.itl.ee/files/E_arve_saadmine_ja_presenteerimine_pangas_ver_1_0_5_EST.pdf
29. Eesti Pangaliit. (n.d.). *Pettuste tõkestamise toimikond*. Retrieved from <https://pangaliit.ee/uldteave/toimikonnad/pettuste-tokestamise-toimikond>
30. Eesti Standardimis- ja Akrediteerimiskeskus. (2023). *EVS-EN ISO/IEC 27001:2023+A1:2024. Infoturbe, küberturbe ja privaatsuskaitse. Infoturbe halduse süsteemid. Nõuded*. Retrieved from EVS-EN ISO/IEC 27001:2023+A1:2024 - EVS standard evs.ee | et
31. European Central Bank. (2025). *Financial Stability Review*, May 2025. Retrieved from <https://www.ecb.europa.eu/press/financial-stability-publications/fsr/html/ecb.fsr202505~0cde5244f6.en.html>
32. European Union Agency for Cybersecurity. (2025a). *NIS Investments 2025: Main report*. Retrieved from <https://www.enisa.europa.eu/sites/default/files/2026-02/NIS%20Investments%202025%20-%20Main%20report.pdf>
33. European Union Agency for Cybersecurity. (2025b). *ENISA sectorial threat landscape: Public administration* (Version 1.1). Publications Office of the European Union. Retrieved from <https://www.enisa.europa.eu/publications/enisa-sectorial-threat-landscape->

public-administration[https://www.enisa.europa.eu/sites/default/files/2025-12/ENISA Public Administration TL 2024 - v1.1.pdf](https://www.enisa.europa.eu/sites/default/files/2025-12/ENISA_Public_Administration_TL_2024_-_v1.1.pdf)

34. European Union Agency for Cybersecurity. (2025c). *ENISA threat landscape 2025* (Version 1.2). Publications Office of the European Union. Retrieved from

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

35. Eurojust. (2025). *Annual report 2024*. Publications Office of the European Union. Retrieved from <https://www.eurojust.europa.eu/sites/default/files/assets/files/eurojust-annual-report-2024-en.pdf>

36. Eurojust & Europol. (2025). *Common challenges in cybercrime: 2024 review*.

Publications Office of the European Union. Retrieved from

<https://www.europol.europa.eu/publications-events/publications/common-challenges-in-cybercrime>

37. European Parliament and the Council of the European Union. (2015). *Directive (EU) 2015/2366 on payment services in the internal market*. Retrieved from <https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng>

38. Europol. (2023a). *Online fraud schemes: A web of deceit (Europol Spotlight Report Series)*. Publications Office of the European Union. Retrieved from

<https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023>

39. Europol. (2023b). *European financial and economic crime threat assessment 2023: The other side of the coin*. Publications Office of the European Union. Retrieved from

<https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime>

40. Europol. (2025a). *The changing DNA of serious and organised crime*. Publications Office of the European Union. Retrieved from <https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime>

41. Europol. (2025b). *Steal, deal and repeat: How cybercriminals trade and exploit your data (IOCTA 2025)*. Publications Office of the European Union. Retrieved from

<https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data>

42. Evans, J. S. B. T. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. *Annual Review of Psychology*, 59, 255–278. DOI:

10.1146/annurev.psych.59.103006.093629

43. Federal Bureau of Investigation. (2022). *FY 2022 FBI congressional report: Business email compromise and real estate wire fraud*. Retrieved from <https://www.fbi.gov/file-repository/reports-and-publications/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view>
44. Federal Bureau of Investigation. (n.d.-a). *Business Email Compromise*. Retrieved from <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise>
45. Federal Bureau of Investigation. (n.d.-b). *Business Email Compromise (BEC)*. Internet Crime Complaint Center (IC3). Retrieved from <https://www.ic3.gov/CrimeInfo/BEC>
46. Federal Bureau of Investigation Internet Crime Complaint Center. (2026). *2025 IC3 annual report*. Retrieved from https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
47. Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In *Human aspects of information security, privacy, and trust*, 36–47. Springer. DOI: 10.1007/978-3-319-20376-8_4
48. Financial Action Task Force. (2025). *Annual report 2024–2025*. FATF. Retrieved from <https://www.fatf-gafi.org/content/dam/fatf-gafi/annual-reports/fatf-annual-report-2024-2025.pdf>
49. Financial Action Task Force. (2026). *Cyber enabled fraud: Digitalisation and ML/TF/PF risks*. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/cyber-enabled-fraud-paper.pdf.coredownload.inline.pdf>
50. Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1), 22–44. DOI: 10.17705/1jais.00447
51. Greulich, M., Lins, S., Pienta, D., & Thatcher, J. B., & Sunyaev, A. (2024). Exploring contrasting effects of trust in organizational security practices and protective structures on employees' security-related precaution taking. *Information Systems Research*, 35(4), 1586–1608. DOI: 10.1287/isre.2021.0528
52. Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2544742

53. Herbert, I. P., & Seal, W. B. (2012). Shared services as a new organisational form: Some implications for management accounting. *The British Accounting Review*, 44(2), 83–97. DOI: 10.1016/j.bar.2012.03.006
54. INTERPOL. (2026). *Global financial fraud threat assessment*. INTERPOL General Secretariat.
<https://www.interpol.int/content/download/24291/file/INTERPOL%20Global%20Financial%20Fraud%20Threat%20Assessment%202026.pdf>
55. Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, 6(1). DOI: 10.1186/s13673-016-0065-2
56. Joha, A., & Janssen, M. (2011). Types of shared services business models in public administration. In *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*, 26–35. Association for Computing Machinery. DOI: 10.1145/2037556.2037562
57. Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLoS ONE*, 14(1). DOI: 10.1371/journal.pone.0209684
58. Justiits- ja Digiministeerium. (2026, 6. veebruar). *Tutvustus ja struktuur*. Retrieved from <https://www.justdigi.ee/tutvustus-ja-struktuur>
59. Jõgi, E. (2025, 21. august). Hekotekist varastati küberrünnakuga sadu tuhandeid. Suuromanik süüdistab finantsjuhti. *Äripäev*. Retrieved from <https://www.aripaev.ee/uudised/2025/08/21/hekotekist-varastati-kuberrunnakuga-sadu-tuhandeid-suuromanik-suudistab-finantsjuhti>
60. Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science*, 9(13). DOI: 10.1186/s40163-020-00119-4
61. Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY: Farrar, Straus and Giroux.
62. Khursheed, B., Pitropakis, N., McKeown, S., & Lambrinoudakis, C. (2020). Microtargeting or microphishing? Phishing unveiled. *Lecture Notes in Computer Science: Trust, privacy and security in digital business*, 12395, 89–105. Springer. DOI: 10.1007/978-3-030-58986-8_7

63. Kroll. (n.d.). *Business Email Compromise Attack Investigation and Remediation for Insurance Broker*. Retrieved from <https://www.kroll.com/en/publications/cyber/case-studies/business-email-compromise-attack-investigation>
64. Küberturvalisuse seadus (2025, 30. detsember). Riigi Teataja I. Retrieved from <https://www.riigiteataja.ee/akt/130122025015>
65. Legarda, L.L., & Nabe, N.C., (2026). Breaking the silence: A qualitative inquiry into the plight of fraud victims in Davao region, Philippines. *European Journal of Social Sciences Studies*, 12(1). DOI: 10.46827/ejsss.v12i1.2121
66. Lazarus, S. (2025). Cybercriminal networks and operational dynamics of Business Email Compromise (BEC) scammers: Insights from the “Black Axe” confraternity. *Deviant Behavior*, 46(4), 456–480. DOI: 10.1080/01639625.2024.2352049
67. Matson Kald, A. (2023, 26. aprill). Eesti põllumajandusfirma sai 100 000 eurot kahju tegevjuhi küberpetuskeemiga. *Äripäev*. Retrieved from <https://www.aripaev.ee/uudised/2023/04/26/eesti-pollumajandusfirma-sai-100-000-eurot-kahju-tegevjuhi-kuberpetuskeemiga>
68. Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution*. Klagenfurt. Retrieved from https://www.ssoar.info/ssoar/bitstream/handle/document/39517/ssoar-2014-mayring-Qualitative_content_analysis_theoretical_foundation.pdf
69. Modic, D., & Lea, S. E. G. (2013). Scam compliance and the psychology of persuasion. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2364464
70. Myojin, S., & Babaguchi, N. (2020). A logical consideration on fraudulent email communication. *Artificial Life and Robotics*, 25(3), 475–481. DOI: 10.1007/s10015-020-00597-4
71. European Commission. (2026, 20. jaanuar). *NIS2 Directive: Securing network and information systems*. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
72. OECD. (2026). *Financial protection against catastrophic risks: Floods, fires and other major risks*. OECD Publishing. DOI: 10.1787/32a3acd7-en
73. Ogwo-Ude, O. (2023). Business Email Compromise challenges to medium and large-scale firms in USA: An analysis. *Open Journal of Applied Sciences*, 13(6), 803–812. DOI: 10.4236/ojapps.2023.136064

74. Pan, T. B., Yang, Q., Cole, A. J., Wilson, R., & Woodard, D. L. (2026). Psychology of phishing emails: Quantifying persuasion principles and simulating detection with large language models. *Expert Systems with Applications*, 313, 131507. DOI: 10.1016/j.eswa.2026.131507
75. PM Majandus. (2025, 20. november). Kurjategijad ründavad sotsiaalmeedias aktiivseid ettevõtteid. *Postimees*. Retrieved from <https://majandus.postimees.ee/8365148/kurjategijad-rundavad-sotsiaalmeedias-aktiivseid-ettevotteid>
76. Politsei- ja Piirivalveamet. (n.d.). *PPA lugu ja väärtused*. Retrieved from <https://www.politsei.ee/et/ppa-lugu-ja-vaeartused>
77. Rahandusministeerium. (2025). *Eesti riikliku riskihinnangu aruanne rahapesu tõkestamise valdkonnas 2020–2024*. Retrieved from https://fin.ee/sites/default/files/documents/2025-10/NRA%202025%20RP%20raport_01.10.pdf
78. Rahandusministeerium. (2023). *Valitsussektori maksed*. Retrieved from <https://www.fin.ee/riigi-rahandus-ja-maksud/riigi-raamatupidamine/valitsussektori-maksed>
79. Rahandusministeerium. (2024, 4. oktoober). *Ministeeriumi tutvustus*. Retrieved from <https://fin.ee/ministeerium-uudised-ja-kontakt/organisatsioon/ministeeriumi-tutvustus>
80. Rahandusministeerium. (2021, 3. detsember). *Riigikassa*. Retrieved from <https://www.fin.ee/riigi-rahandus-ja-maksud/riigikassa>
81. Raamatupidamise seadus. (2025, 10. juuli). Riigi Teataja I. Retrieved from <https://www.riigiteataja.ee/akt/110072025003>
82. Rahapesu Andmebüroo. (2026, 14. aprill). *Asutusest*. Retrieved from <https://fiu.ee/asutusest-kontakt/asutusest>
83. Raudla, R., & Tammel, K. (2015). Creating shared service centres for public sector accounting. *Accounting, Auditing & Accountability Journal*, 28(2), 158–179. DOI: 10.1108/AAAJ-06-2013-1371
84. Riigi Infosüsteemi Amet. (2025, 14. august). *Küberintsidentide käsitlemine CERT-EE*. Retrieved from <https://www.ria.ee/kuberturvalisus/kuberintsidentide-kasitlemine-cert-ee>
85. Riigi Infosüsteemi Amet. (2024c, 29. mai). *Eesti infoturbestandardi (E-ITS) tutvustus*. Retrieved from <https://eits.ria.ee/et/avalehe-menuueue/tutvustus/ueldine>
86. Riigi Infosüsteemi Amet. (2020, 4. august). Juunis iseloomustasid Eesti küberruumi arvepettused, meilikonto kompromiteerimised ja õngitsuskirjad. Retrieved from

<https://www.ria.ee/uudised/juunis-iseloomustasid-eesti-kuberruumi-arvepettused-meilikonto-kompromiteerimised-ja>

87. Riigi Infosüsteemi Amet. (2022a, 6. mai). Olukord küberruumis – aprill 2022.

Retrieved from <https://www.ria.ee/uudised/olukord-kuberruumis-aprill-2022>

88. Riigi Infosüsteemi Amet. (2022b, 7. juuli). Olukord küberruumis – juuni 2022.

Retrieved from <https://ria.ee/uudised/olukord-kuberruumis-juuni-2022>

89. Riigi Infosüsteemi Amet. (2023a, 6. juuli). Juuni küberruumis: ohtrad õngitsused ja arvepettused. Retrieved from <https://www.ria.ee/uudised/juuni-kuberruumis-ohtrad-ongitsused-ja-arvepettused>

90. Riigi Infosüsteemi Amet. (2023b). *Küberturvalisuse aastaraamat 2023*. Retrieved from https://www.ria.ee/sites/default/files/documents/2023-02/RIA_kyberturvalisuse_aastaraamat_2023.pdf

91. Riigi Infosüsteemi Amet. (2024a). *Küberturvalisuse aastaraamat 2024*. Retrieved from *Küberturvalisuse aastaraamat 2025 | RIA*

92. Riigi Infosüsteemi Amet. (2024b, 1. detsember). Levivad arvepettused! Kontrolli, enne kui maksad. Retrieved from <https://www.ria.ee/blogi/levivad-arvepettused-kontrolli-enne-kui-maksad>

93. Riigi Infosüsteemi Amet. (2025a). *Küberturvalisuse aastaraamat 2025*. Retrieved from *Küberturvalisuse aastaraamat 2026 | RIA*

94. Riigi Infosüsteemi Amet. (2025b, 24. november). Küberrünnak pole IT probleem, vaid juhtimisküsimus. Retrieved from <https://www.ria.ee/blogi/kuberrunnak-pole-it-probleem-void-juhtimiskusimus>

95. Riigi Infosüsteemi Amet. (2025c, 4. september). August küberruumis: petturid suvepuhkust ei võtnud. Retrieved from <https://ria.ee/uudised/august-kuberruumis-petturid-suvepuhkust-ei-votnud>

96. Riigi Info- ja Kommunikatsioonitehnoloogia keskus. (2025. 1. jaanuar). RIT finantsprotsessid alates 01.01.2025) [Asutusesisene dokument]

97. Riigi Tugiteenuste Keskus. (2024, 29. november) *FitekIN arvekeskuse administraatori, sh raamatupidaja juhend..* Retrieved from <https://pilv.rtk.ee/s/3cMJANAcMPZizL?dir=undefined&openfile=293222>

98. Riigi Tugiteenuste Keskus. (2021, 19. mai) *FitekIN arvekeskuse juhend.* Retrieved from <https://pilv.rtk.ee/s/3cMJANAcMPZizL?dir=undefined&openfile=249551>

99. Riigi Tugiteenuste Keskus. (2023, 5. mai) *Justiitsministeeriumi valitsemisala finantsarvestuse toimetud_05.05.2023*.
https://pilv.rtk.ee/s/ocR5ZbyBTYxLB3z/download?path=%2FJustiitsministeerium&files=Justiitsministeeriumi%20valitsemisala%20finantsarvestuse%20toimetud_04.05.2023.xlsx
100. Riigi Tugiteenuste Keskus. (2024, 19. september) SAP (ET) *Ostumooduli juhend*. Retrieved from <https://pilv.rtk.ee/s/xkyPd5wD44npkMY?dir=undefined&openfile=257859>
101. Riigi Tugiteenuste Keskus. (2026, 2. veebruar) SAP (ET) *Pank juhend*. Retrieved from <https://pilv.rtk.ee/s/f2TaPenE8YtMRTN>
102. Saarmann, T. (2026, 17. aprill). Eesti ettevõtte kaotas kelmuse tõttu 1,6 miljonit eurot. *Delfi Ärileht*. Retrieved from <https://arileht.delfi.ee/artikkel/120569422/eesti-ettevõtte-kaotas-keelmusega-1-6-miljonit-eurot>
103. Schneier, B. (2008). The psychology of security. In Progress in Cryptology – *AFRICACRYPT 2008. Lecture Notes in Computer Science*, 5023, 50 – 79. Springer. DOI: 10.1007/978-3-540-68164-9_5
104. Seal, W., & Herbert, I. (2013). Shared service centres and the role of the finance function: Advancing the Iron Cage? *Journal of Accounting & Organizational Change*, 9(2), 188–205. DOI: 10.1108/18325911311325951
105. Sethuraman, S. C., V S, D. P., Reddi, T., Reddy, M. S. T., & Khan, M. K. (2024). A comprehensive examination of email spoofing: Issues and prospects for email security. *Computers & Security*, 137, 103600. DOI: 10.1016/j.cose.2023.103600
106. Sildmets, K. (2026, 23. veebruar). Eesti ettevõtte kaotas kelmidele ligi 170 000 eurot. *Delfi Ärileht*. Retrieved from <https://arileht.delfi.ee/artikkel/120438256/eesti-ettevõtte-kaotas-keelmidele-ligi-170-000-eurot>
107. Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business and Management*, 13(6). DOI: 10.5539/ijbm.v13n6p1
108. United Nations. (2024). *United Nations Convention against Cybercrime (Chapter XVIII-16)*. United Nations Treaty Series. Retrieved from https://treaties.un.org/doc/Treaties/2024/12/20241224%2001-27%20PM/Ch_XVIII_16.pdf
109. United Nations Office on Drugs and Crime. (2022). *Digest of cyber organized crime* (2nd ed.). Retrieved from https://www.unodc.org/documents/organized-crime/tools_and_publications/Digest_of_Cyber_Organized_Crime_2nd_edition_English.pdf

110. United States Department of Justice. (2019). *Affidavit in support of criminal complaint: United States v. Obinwanne Okeke*. Retrieved from <https://embed.documentcloud.org/documents/6299590-Obinwanne-Okeke-Affidavit>
111. Václavík, L., Špatenka, J., & Petrová, K. (2025). Resilience against business email compromise: A corporate case study. *Ekonomika Misao i Praksa-Economic Thought and Practice*, 34(2), 1–19. DOI: 10.17818/EMIP/2025/41
112. Van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, 6(1), tyaa019. DOI: 10.1093/cybsec/tyaa019
113. Vasli, K. (2025, 28. mai). Kelmid varastasid Eesti firmalt salakavala petukirja abil 1,7 miljonit eurot. Retrieved from *Delfi*. <https://www.delfi.ee/artikkel/120380586/kelmid-varastasid-eesti-firmalt-salakavala-petukirja-abil-1-7-miljonit-eurot>
114. Vergara Cobos, E., & Cakir, S. (2024). *A review of the economic costs of cyber incidents*. World Bank. <https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf>
115. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), 576–586. DOI: 10.1016/j.dss.2011.03.002
116. Xiwen, L., Xu, D., & Shiyu, S. (2021). Research on the internal control problems faced by the financial sharing center in the digital economy era1 – An example of financial sharing Center of H Co. Ltd. *Procedia Computer Science*, 187, 158-163. DOI: 10.1016/j.procs.2021.04.047
117. Zakari, A., Abiodun, O., Omolara, O., Owolabi, O., Adeyinka, O., & Oluwadare, O. (2026). Adversarially resilient detection of business email compromise using hybrid machine learning. *Journal of High-Frequency Communication Technologies*, 4(2), 466–480. DOI: 10.58399/ECFA6495
118. Zaporowska, Z., & Szczepański, M. (2024). Risk management in diffused structures: Analysis for shared services centers. *Ekonomia*, 29(2), 59–75. DOI: 10.19195/2658-1310.29.2.4

119. Ziorklui, J. E. K., Ampofo, F. O., Nyonyoh, N. & Antwi, B. (2024). Effectiveness of internal controls mechanisms in preventing and detecting fraud. *Finance & Accounting Research Journal*, 6(7), 1259–1274. DOI: 10.51594/farj.v6i7.1322

LISA A

Kasutatud lühendid

RIA – Riigi Infosüsteemi Amet

RIT – Riigi Info- ja Kommunikatsioonitehnoloogia keskus

RTK – Riigi Tugiteenuste keskus

BEC – Business Email Compromise (Ärikirjapettus)

CERT – Computer Emergency Response Team (Intsidentide käsitlemise üksus)

E-ITS – Eesti Infoturbestandard

ENISA – European Union Agency for Cybersecurity (Euroopa Liidu
Küberturvalisuse Amet)

EUROJUST – European Union Agency for Criminal Justice Cooperation (Euroopa
Liidu Kriminaalõigusalase Koostöö Amet)

EUROPOL – European Union Agency for Law Enforcement Cooperation (Euroopa
Liidu Õiguskaitsekoostöö Amet)

EVS – Eesti Standardimis- ja Akrediteerimiskeskus

INTERPOL – International Criminal Police Organization (Rahvusvaheline
Kriminaalpolitseiorganisatsioon)

ISO – International Organization for Standardization (Rahvusvaheline
Standardimisorganisatsioon)

ITL – Eesti Infotehnoloogia ja Telekommunikatsiooni Liit

FATF – Financial Action Task Force (Rahapesuvastane töögrupp)

FBI IC3 – Federal Bureau of Investigation Internet Crime Complaint Center
(Ameerika Ühendriikide Föderaalne Juurdlubüroo Interneti Kuritegude Kaebuste Keskus)

KüTS – Küberturvalisuse seadus

NIS – Network and Information Security (Võrkude ja infosüsteemide turvalisus ehk
Küberturvalisuse direktiiv)

OECD – Organisation for Economic Co-operation and Development
(Majanduskoostöö ja Arengu Organisatsioon)

PPA – Politsei- ja Piirivalveamet

PSD2 – Payment Service Directive 2 (Makseteenuste 2. direktiiv)

UNODC – United Nations Office on Drugs and Crime (Ühinenud Rahvaste Organisatsiooni narkootikumide ja kuritegevuse büroo)

LISA B

Intervjuuküsimused

Andmekogumisel kasutati poolstruktureeritud intervjuukava, mis võimaldas vastuste täpsustamiseks esitada täiendavaid küsimusi. Intervjuud viidi läbi 2026. aasta kevadel Microsoft Teamsi rakenduses. Tulenevalt intervjuude poolstruktureeritud iseloomust ei esitatud kõigile intervjuueeritavatele kõiki küsimusi. Küsimuste valik sõltus vastaja rollist ja vastuste sisust. Järgnevalt on esitatud intervjuueerimisel kasutatud küsimused.

A. Roll ja vastutus

1. Palun kirjeldage oma rolli organisatsioonis ja seost arvete menetlemisega.
2. Selgitage osapoolte vahelist vastutuse jaotust (nii organisatsioonisisene kui teenuseosutaja ja kliendi vaheline).
3. Kuidas jaguneb pettuse realiseerumisel vastutus erinevate osapoolte vahel?

B. Arvete menetlemine

4. Kirjeldage ostuarvete menetlemise protsessi.
5. Milliseid IT-lahendusi kasutatakse arvete menetlemiseks?
6. Kuidas erineb välisarvete menetlemine Eesti-sisestest arvetest?
7. Selgitage kinnitusringi/kooskõlastusringi olemust ja osapoolte arvu ning vastutust.
8. Millistel juhtudel tehakse kinnitusringile kehtestatud reeglite täitmisel erandeid?

C. Kontrollimehhanismid

9. Milliseid meetmeid kasutatakse arvete menetlusprotsessi turvalisuse tagamiseks?
10. Mille alusel kontrollitakse arve õigsust?
11. Kuidas tuvastatakse arve tavapäraste rekvisiitide muutus ja millised tegevused sellele järgnevad?
12. Kas olete kokku puutunud olukorraga, kus arve rekvisiidid olid muudetud? Millised tegevused sellele järgnesid?
13. Kuidas toimub tarnijaandmete muutmine?

D. Erakorralised maksed ja erandid

14. Kuidas käsitletakse kiireloomulisi või erakorralisi maksid?
15. Kas makset on võimalik teostada arve saabumisele samal päeval?

16. Millised piirangud kehtivad arvete tasumisel?

E. Töökoormus

17. Kuidas jaotub erinevate osapoolte töökoormus arvete menetlemisel (nt kuu või aasta lõikes)?

F. Koolitused ja teadlikkus

18. Kirjeldage (küberturvalisuse) koolituste sisu ja regulaarsust ning hinnake nende piisavust valdkondlike ohtude teadvustamisel.

19. Kas koolitused käsitlevad ka finantsvaldkonnaga seotud ohte (nt arvepettused)?

H. Intsidendihaldus ja auditeerimine

20. Kas eksisteerib dokumenteeritud intsidendihalduse protsess?

21. Kuidas käitutakse pettuse või kahtlust äratava juhtumi korral?

22. Kas finantsarvestuses viiakse läbi siseauditeid?

23. Kuidas hindate makseandmike avalikustamist avaandmetena?

LISA C

Intervjuuandmete kategoriseerimine ja kodeerimine

Kategooria 1 – Ostuarvete menetlemise protsessi etapid ja rollid

Kood	Teema	Allikas + Tsitaat
K1.1.1	E-arve kohustus	RTK I1: Arved liiguvad ainult e-arvena, kuna seadus näeb ette, et avalik sektor võib võtta vastu ainult e-arveid. Ehk siis see on juba üks selline väike kiht ees, et arve ei saa liikuda otse kuskilt käest kätte, vaid see arve liigub ainult e-arve operaatorite kaudu. RIT I1: Riigiasutustel ongi ainult e-arved, teist varianti ei olegi.
K1.1.2	E-arve piirang	RTK I1: Välismaa ettevõtetele e-arve kohustus muidugi ei laiene. Sest nemad ei ole meie raamatupidamisseaduse subjektid. RTK I1: Juba üsna palju välismaa arve esitajaid on Peppoliga liitunud, mis on Euroopasisene e-arve süsteem, kus arve liigub samamoodi operaatorite vahel. Fiteki, meie teenusepakkuja, on ka Peppoliga ühenduses. Kui klient saadab arve Peppoli kaudu, siis see jõuab Fitekiisse samalaadselt, nagu e-arve Eestist. RTK I1: Suurem osa välisarvetest tuleb endiselt PDF-i kujul. RTK I2: Välisarve tuleb asutuse kontaktile... neile tuleb PDF arve ja siis saadetakse see Fitekiisse. RIT I1: Välismaiste puhul ongi niimoodi, et kuna nemad meie e-arve keskkonda kasutada ei saa, siis nemad peavad saatma PDF-kujul arve. Meiepoolsele teenuse tellijale saadetakse meilile, üldiselt siis kulu- või eelarve juht. Igal asutusel on oma unikaalne digiteerimisaadress. Kulujuht saadab PDF-i sellele meiliaadressile ja Fiteki keskkond ise muudab selle e-arveks. RIT I1: Kuna nemad meie e-arve keskkonda kasutada ei saa, siis nemad peavad saatma PDF-kujul arve.
K1.1.3	Kinnitusring on mitmeastmeline	RTK I1: Iga arve, mis sisse tuleb, käib läbi päris paljude inimeste käest. RTK I3: Võib ka öelda neli, kui see käib SAP help'ist läbi. [Menetlemise protsessis on 3-4 RTK töötajat] RTK I2: Enne mind on finantstöötaja, kellega minul on otsesuhtlus. Kui mul mingid küsimused tekivad, siis ma pöördun selle finantstöötaja poole. Mina olen kinnitusringi viimane kinnitaja. RTK I2: Kolm või kaks kindlasti enne mind. Või on niisugused tavaarved, mis

		igakuiselt tulevad, võib-olla rentide ja üüridega ja mis on püsiarved iga kuu, nendel ilmselt on vähem. RTK 12: Ma kinnitan selle makse ära, ja see läheb maksmata arvetesse. Ja maksmata arvetest, see töötaja, kes pangaga tegeleb, siis teeb maksefailid. RTK 12: Ja siis teine inimene saadab maksed ära. Ja ma tean, et see inimene, kes saadab makset pankka, siis kui tema märkab, et kaardil näiteks ei ole aadressi või kus on vaja telefoni, siis tema küsib. Ta ei saada üldse neid enne äragi, kui küsib meie käest, et me täpsustaksime neid andmeid. RIT 11: Kindlasti peale eelarve või kuljuhti peab olema uuesti arvestusspetsialist, enne kui see läheb kas otse RTK-sse või siis veel direktorile. Viimane kooskõlastaja on RTK raamatupidaja. Kontrollimine toimub Fitekis. RIT 12: Eelarverea panemine tundub kõigile väga suur kohustus ja tüütu asi. Ja meie osakonda on püütud päris mitmel korral ära rääkida, et jätame selle ära. Aga meie hädaga oleme raiunud vastu, et see on juba turvalisuse pärast. Ja see, et sa oled selle kulu planeerinud. RTK 14: Ma lihtsalt ei anna võimalust makset teostada, kui mul ei ole kindlust. RTK 14: Mina saadan RTK raamatupidajale teavituse, et seoses arvepettustega palun kooskõlastada arve esitajaga panga andmed. RTK 14: Kui nüüd seesama euroarve on ikkagi, ütleme 10 000 või 20 000 suurune, siis ma palun igal asutusel kooskõlastada arve andmed arve esitajaga. RTK 14: Kui arve on viisteist tuhat dollarit USA-st, siis ma tegelikult palun kooskõlastust. Sest neid ma kontrollida, mitte mingi nipiga ei saa. USA-d on üldse keeruline jälgida ja neid ma palun küll kontrollida ja kooskõlastada peaaegu alati, olenemata summast. RTK 14: Me kunagi koosolekul rääkisime ja sealt kakskümmend tuhat jäi. See on nagu selline, et alla kahekümne tuhande lihtsalt petturid ei viitsiks panustada. Nemad jahivad ju suuri summasid. RTK 14: Ennem ma SAP-is mitte mingit liigutust ei tee, kui mul ei ole vastust. Ma olen väga järjekindel selles. RTK 14: Kammin interneti läbi – mul on nimekiri erinevate riikide registritest. RTK 14: Tegelikult samal ajal, kui nendele jõuab arve kooskõlastusringi Fitekisse, mina juba toimetan selle tarnijaga. Kas loon ta SAP-i või täiendan SAP-i andmeid või mis iganes. See käib kõik paralleelselt. RTK 14: Asutus näeb seda uue tarnija sildiga arvet ja mina näen ka. Menetlusring ei puuduta minu tööd üldse. RTK 14: Mina usun, et erasektoril ei ole sellist kontrollmehhanismi, nagu on meil. Meil tõesti väga paljud silmad vaatavad. See on ka üks põhjus, miks mina endale selle ülesande täiesti ise võtsin.
K1.1.4	Kinnitusring on summa-põhine	RIT 11: Kui arve on rohkem kui 15 000 eurot, siis läheb eelarve juhile. Alates 50 000 direktorile.
K1.1.5	Kinnitusring on kohustuslik	RIT 12: Jah, kohustuslik, sellest me ei lähe mööda. Sellel juhul lihtsalt jääbki see arve õigel ajal maksmata. RTK 11: Ka kiireid asju me saame menetleda Fiteki kaudu. No kui nüüd on tõesti vaja täna maksta, on seal juba rohkem inimesi kaasatud, siis me räägime sellest kliendiga tõenäoliselt telefoni teel. Sest et kui see jõuab raamatupidajani, kes arvet menetleb, ega ta ka üksi ei otsusta, ta konsulteerib meil seespool. Ja kui vaja, siis meie töötaja, kes tegeleb meil pangaga, võib küsida Riigikassast, kas saab. Me oma talituse siseselt seda ikkagi konsulteerime omavahel.
K1.1.6	Lepingu ja üleandmise-vastuvõtmise akti nõue	RIT 11: See on kinnitus, et raha on eelarvestatud. RIT 11: Arve ei lähe enne maksmisele, kui on olemas allkirjastatud akt, kahepoolne. RTK 13: Kuna kõigil on eelarvetega väga kitsas käes, siis nad jälgivad kullipilgul iga oma makset. Sest just nimelt, raha on piiratud hulk, ja võib-olla see aitab ka kaasa, et nad vaatavad väga hoolega üle.
K1.1.7	Alternatiivse kanali kasutamine	RTK 12: Liikmemaks läks kogu aeg ühele Inglismaa kontole. Ja siis äkki arvel oli Poola konto, mis tekitas kohe muidugi kahtluse. Mul tuli see arve tagasi e-arve keskusesse, kuna mul ei olnud sellisel hankijal seda pangakontot küljes. Mina saatsin edasi, SAP helpi, et palun lisada sinna selline pangakonto. Siis mul tuli sealt meil, et palun kontrollida, et kas nad ikka soovivad sellele kontole, et kas

		see on õige. Siis ma sellest asutusest küsisin järele ja asutus saatis mulle meili, kus oli kirjas, et palun tasuda selline arve, ja et juhime tähelepanu, et arveldusarve on muutunud. Meili allkirjastaja oli inimene, kes oli ka toodud kodulehel ära kontaktisikuna. SAP kontrollis selle üle ja siis alles tegime. Välisbankijaid väga kontrollitakse. RTK I3: Sellist reeglit ma ei tea otseselt, et meil oleks kuidagi mingisugused kohustuslikud sammud. Sellele tuleb terve mõistusega läheneda. RIT II: Ühel hetkel Bolt tegi konto LHV-sse. Aga ta andis meile meili teel teada, et alates sellest arvest võime maksta sinna kontole. Pöördusime inimese poole, kellega me kogu aeg suhtleme ja kes lepingus on välja toodud meie kontaktina. Me kirjutame enda välja otsitud aadressile ja küsisime üle ja ütlesime, et nad peavad kindlasti selle konto tooma välja ka enda arve peal. RTK I4: Arvel olevad pangaandmed on kõige olulisemad ja kooskõlastamist küsida mingi teise kanali kaudu, mitte arvel olevate kontaktide alusel. RTK I4: Pange lepingutesse alati kirja, mis kontodele makstakse. Panga andmed ei tohi lepingu kehtivuse perioodil muutuda. See on, ma arvan, üks kõige turvalisem meede, kui on lepingus fikseeritud, et kõik maksed selle lepingu raames lähevad sellele kontole. RTK I4: Kas nemad päriselt küsivad üle, ma kindel olla ei saa. Aga kui asutus vastab, et jah, kinnitan, et arvel olevad andmed on õiged, siis seda ma ei aktsepteeri. RTK I4: Mulle on saadetud arve esitaja pangast sertifikaadi väljavõte. RTK I4: Ei ole. [protseduurid kirjalikult dokumenteeritud]. Enam ei oska seda infot ka edasi teistele anda, et mida ma vaatan ja kuidas ma vaatan. Mul on mõned asjad juba automaatselt käe sees. RTK I4: Palun pange lepingutesse alati kirja, mis kontodele makstakse, lepingujärgselt tasud. Pangaandmed ei tohi lepingu kehtivuse perioodil muutuda. Kui on lepingus fikseeritud, et kõik maksed selle lepingu raames lähevad sellele kontole. RTK I4: Oli juhus, kus mina ei olnud nõus sisestama, lepingus on teine IBAN. Saatsite mulle üks kord pildi lepingust, ja seal on kirjas, et ei tohi muutuda kontonumbrid. Miks partner muutis? Ja siis tuli juba tolle riigi pangast pikk kiri, kus oli kõik seletatud. RTK I4: Uutega on kõik andmed uued ja ka siis, kui muutuvad pangaandmed – need on kõige rohkem tähelepanu nõudvad. RTK I4: Kammin interneti läbi – mul on nimekiri erinevate riikide registritest. RTK I4: Kooskõlastamist küsida mingi teise kanali kaudu.
K1.1.8	Krediitkaardi makse	RIT I2: On juhtusid, kus tõesti saab teha ainult oste, kus pead kohe ära tasuma. Muidu ei olegi võimalik osta või on ost äärmiselt palju soodsam, kui oleks arvega. Tema [töötaja X] võib kasutada ainult selliste litsentside ostuks, millele ei väljastata e-arvet või sa saadki näiteks tasuda ainult internetis, ja sa saad pärast arve. Sa ei või teha kauplusest oste, sa ei või sularaha välja võtta. Sa ei saa mitte minu kaardi andmeid, vaid sa teed selle tehingu minuga koos.
K1.1.9	Klient saadab PDF-kujul välisarved Fitekisse	RTK I1: Kliendile tuleb PDF arve ja siis see arve saadetakse selle sama töötaja poolt Fitekisse digiteerimisele. Igal asutusel on digiteerimisadressid, kust Fitek võtab vastu PDF-välisarveid. Meil on selline reegel, et ta tohib võtta vastu ainult selle asutuse domeeniga aadressilt arveid. See on kokkulepitud reegel. Ma ei tea, kuidas see tehniliselt Fiteki poolt toimib, aga see on nõue, mis peab olema täidetud. RTK I2: Klient ise sisestab arve digitaliseerimiseks. RIT II: Selle, kes tellis selle teenuse meie poolt, üldiselt siis kulu- või eelarve juht, meilile saadetakse. Ja igal asutusel on oma unikaalne emaili aadress. Kulujuht saadab selle PDF-i sellele meiliaadressile ja Fiteki keskkond ise muudab selle e-arveks.
K1.2.1	SAP tuvastab uue hankija	RTK I3: Kui välisbankija on esmakordselt selline, kelle arvet tasutakse, siis ta ei liigu Fitekist enne edasi, kui see info läheb meie IT poolele, kes loob selle hankija kõigepealt. Ehk siis selle välistarnija kohta tuleb teha SAP-i hankija kood, enne ta ei liigu Fitekist edasi. Välisbankijate infot sisestab IT osakond. Nemad vaatavad veel kolmanda pilguga üle, et kas see soov tundub loogiline. RTK I2: Kui tuleb SAP-i arve, millel Fitekist kontonumbrit tulnud ei ole, siis ta

		läheb Fitekisse tagasi, teatega, et puudub IBAN näiteks või puutub kontonumber. RTK 12: Kui nimi natukene muutub, I asemel on l, siis Fiteki jaoks on see juba uus tarnija. RTK 12: Kui on välishankija või tarnija, siis sel juhul teeb seda SAP tugi, kes kontrollib oma süsteemides ja nende kodulehtede pealt, ja kas on tegu õige arvega ja õige tarnijaga, nemad väga täpselt kontrollivad. Kui tarnijat ei ole Fitekis, siis tuleb märge, et „uus tarnija“ ja sel juhul saab SAP-i tiim otsida ja lisada uued tarnijad, kui kõik on õige. Kui ei ole õige või tahavad täpsustada, siis täpsustavad meilt ja täpsustavad asutusest järele. SAP-i tiim saadab mulle meili, kus palub täpsustada aadressi näiteks. Pank ju nõuab ka välishankijate puhul, et oleks saaja aadress peal. RTK 14: Kui seda tunnist ei ole [nt uus kontonumber], siis raamatupidaja võib kinnitada, aga arve ei jõua SAP-i, ta jääb maa ja õhu vahele rippuma. RTK 14: Arve saab Fitekist külge uue tarnija sildi ja selle sildiga arve ei hakka Fitekist SAP-i poole liikuma. Ootab, millal saab SAP-i tunnused külge.
K1.2.2	Pangapoolne kontroll	RTK 11: Minu teada pankadel on ju ka makse saaja nime ja pangakonto omavaheline kontroll. RTK 12: Kui saaja nimi ja pangakonto ei klapi, siis meil tuleb selle teavitusega tagasi makse. Sel juhul me küsime asutuselt uuesti, et kas nad on panka teise nime andnud, me ei tea, meie võtame arve pealt need andmed. Aga kui pangas midagi on teistmoodi, siis pank ei lase seda läbi, ta tuleb meile tagasi, kui saaja nimi ja konto ei ole vastavuses. RTK 12: Ma arvan, et ei tohiks juhtuda, [vale või pettuslik makse] sest nüüd ka pangad väga täpselt ju nõuavad saaja nime. Saaja nimi peab olema kõikidel andmetel. Välisarvetel peab olema alati saaja aadress ka peal. Ja näiteks ma võin tuua Lõuna-Korea, kuhu maksame. Nemad tahavad telefoninumbrit saada. Muidu ta ei lähegi edasi, nad ka kontrollivad sealt üle. RTK 14: Ma panen tarnija nime ja IBAN-i ning pank ütleb, kas nimi ja IBAN klapiavad RTK 14: See, et pangad kontrollivad, on suurepärane asi, enam ei saa selliseid asju juhtuda. RTK 14: Kontonumbri ja nime vastavuse kontroll muutus kohustuslikuks 2025 oktoobrist. RTK 14: Riigikassa kontrollib ainult SWIFT koodi. Kommertspank on see, kes saadab tagasi. Eesti-siseselt enam ei saa see esineda sellisel kujul. RTK 14: Salvestatud maksekorralduste kontroll saaja ja IBAN-i vahel toimub öö jooksul, ehk siis kui salvestad maksekorralduse, ära kohe maksa. Seal on ohukoht. RTK 14: Hetkelised maksed võivad minna läbi ilma reaajas kontrolli läbimata. Näiteks tahan maksta viis erinevat makset ja panen nad järjest. Sisestan ära ja salvestan ja pärast panen korraga maksesse, siis varem seda kontrolli ei olnud, nüüd on kontroll olemas, aga alles järgmine päev. RTK 14: Saatsin Swedbanki kirja, et mulle see ei meeldi. See oli ohukoht, et nad ei kontrollinud, sest meie ka ju saadame liidestega portsu ära. Meie suur ports makseid, mis liigub panka, käituvad tehniliselt nagu salvestatud maksekorraldused, kas järgmine päev nad kontrollivad seda või ei kontrolli? Ma vastust ei saanud sealt. RTK 14: Riigid küsivad, miks te tahate meie riigis avada kontot. See on just rahapesu tõttu. RTK 14: Kui mina lähen füüsilise isikuna panka ja panen sinna konto ja nimi ei klapi, siis ma saan tegelikult hoiatuse, mida ma saan ignoreerida. RTK 14: Mina arvan, et see kehtib ikkagi kõigile. Kui sa näiteks saadad makse USA-sse ja too pank ei leia sellele kontole vastavat nime. Süsteem hakkab otsima sellele rahale kohta, kuhu laekuda. Kui ta ei leia, siis makse saadetakse tagasi.
K1.2.3	Fitek logiandmed	RTK 12: Fitekis on ajalugu näha, kes midagi selle arvega teinud on, seal on absoluutselt kõik liigutused näha. Nii see, kas on muudetud maksesaaja andmeid või on muudetud raamatupidamiskonteeringut, et see ajalugu säilib seal. Absoluutselt kõik ülekirjutamise järjekorras lähevad, mis kuupäeval, mis kellaajal ta seda muutis ja milleks muutis ja mis oli endine.
K1.2.4	Fitek ei	RTK 13: Fitek tuvastab lihtsalt andmed, mis on arve peal... seda, et on varem

	tuvasta kontonumbri muutust	olnud erinev konto, minu arust ei tuvasta. RIT 12: Fitek võtab kontonumbri PDF-faili pealt. RTK 14: Masin saab lugeda ainult neid andmeid, mis on selle konkreetse paberi peal olemas. Loeb need ära, paneb vastavasse vormi, nagu Fitekis peab olema. Fitek on andmevahendaja, SAP on andmete kontrollija. Fitekis ei toimu mitte mingisuguseid võrdlusi. RTK 14: Arve saab Fitekist külge uue tarnija sildi.
K1.2.5	Fitek võimaldab Eesti hankija andmeid muuta	RTK 11: Ta tohib võtta vastu ainult selle asutuse domeeniga aadressilt arveid. RTK 12: Kodumaiste arvetega teinekord on ka, et tuleb tagasi, et konto ei vasta, näiteks ei ole kontot SAP-is olemas. Üldjuhul on arve peal ka teine konto toodud, nii et me lisame selle, kuhu nad tahavad saada. Aga seda saab raamatupidaja ise lisada. RIT 12: Jah, ma saan tarnijate registris muuta kõike. Pangakontot, isegi nime ja registrikoodi. RTK 14: Kui seda tunnust ei ole, siis raamatupidaja võib kinnitada, aga ta ei jõua SAP-i. RTK 14: SAP-i andmeid ei saa Fiteki kaudu ümber kirjutada. See ei puuduta SAP-i. RTK 14: Kui e-arvena tuleb Fitekisse arve kodumaiselt ja see tarnija on juba olemas meil SAP-is vana kontonumbriga, siis uue tarnija silti ei teki. Aga süsteem ei kirjuta seda uut kontonumbrit SAP-i. See tuleb käsitsi lisada. RTK 14: Üldjuhul ma ei ole õpetanud ka mitte kedagi [kliente], sest need, mida nemad Fitekisse ükskõik mis kujul sisestavad, see ei jõua SAP-i. RTK 14: Fiteki tarnija kaardilt võetakse maksele kaasa aadressi andmed, aga mitte telefoni. Telefoninumber pannakse maksele selgituse reale eraldi juurde.
K1.2.6	Toimemudel	RTK 11: Meil on toimemudel, mis reguleerib meie omavahelist tööjaotust. Toimemudelis on kirjas, et arve peab olema RTK-le edastatud neli päeva enne makse väljaminekut. Ja seal on tegelikult öeldud, et tavakorras, kui meile tuleb arve, siis maksmisele läheb ta ülehommel. Ta võib minna ka homme, aga reeglina mitte kiiremini. Me valmistame dokumendi ette ja ta on meil ootel maksmata arvete nimekirjas... see on meie üldine reegel, et me maksame välja maksetähtajal. RTK 12: Minul on igas asutuses oma kindel finantstöötaja. Väliskliendiga ma ei suhtle.
K1.2.7	Klient vastutab sisu õigsuse eest	RTK 11: Reeglina kliendipoolne kinnitusringi viimane inimene on finantstöötaja, kes siis omakorda vaatab üle. Kuna ta on selle asutuse töötaja, siis võiks eeldada, et ta on ka kursis, et mida ostetakse, tellitakse, et milliseid kulutusi asutuses tehakse. Eelarve poole pealt ta juba tõenäoliselt teab. [RIT-i vastuste põhjal ei ole see fin.töötaja kohustus, kuigi ta pisteliselt kontrollib] RTK 11: Muidugi me vaatame ju ka peale oma pilguga, et kas seal ei ole mingisuguseid ebakõlasid või selliseid asju, mis tunduvad mingis mõttes kahtlased. Kui see hakkab silma, siis seda me ikka täpsustame kliendiga. RTK 11: Arve õigsust meie, RTK poolt hinnata ei saa, sest meie ei ole olnud kaasas selle tellimisel. Meie jaoks on see juba kindlus, et ta on käinud läbi nende inimeste käest, kes on seda tellinud. RTK 12: Kui ma näen, et arve peal on kõik rekvisiidid õiged ja on kinnitusringil ära käinud, siis ma ei saa milleski kõhklema hakata. Summasid mina vaatan arve pealt. Kas see on õige või ei ole, seda kontrollib juba klient. Mina seda ei tea. RTK 12: Ma arvan, et eks iga asutus loeb oma raha ka lõpuks. Ma eeldan, et need arved, mis minuni jõuavad, on ka kontrollitud juba sisuosakondade poolt ja finantsjuhi poolt. RIT 11: Kui on lepinguline arve ja lepinguline töö või mingi ost, siis kululuht tegelikult peab võrdlema ka Deltas oleva lepinguga, et kas selle arve summa ja sisu vastab sellele, mille eest mulle see arve siis esitati. Et kas selles on eelnevalt nagu kokku lepitud. RIT 11: No meie vastutame kindlasti selle arve sisuõigsuse eest. RIT 11: Meie vastutame, et see summa on planeeritud meil eelarvesse. See arve ei liigu enne maksmisele, kui tal on eelarveprogrammist Veera vastav kulurida olemas.
K1.2.8	Teenuse-	RTK 11: Üldiselt me vaatame tema pangakontosid, me vaatame, et kas

	osutaja vastutab makse rekvisiitide õigsuse eest	pangakonto on normaalne, kas asutus on normaalne, et mis tema nimi ja kõik sellised asjad, mida on meile niikuinii vaja. RTK I1: Selleks, et makse välismaale saata, tuleb ju panna SWIFT-i koodid, pangakoodid ja erinevad tunnused. Nüüd on ju nõutud ka välismaale makstes saaja aadressid ja panga aadressid ja selline täiendav info, mis peab arve pealt tulema, et seda saaks teha. Ja muidugi maksukoodid on meile olulised. Sest et kui see teine pool on käibemaksukohustuslane, et siis, kas meil on vaja seda pöördmaksustada. RTK I1: Kui arve esitaja ei ole öelnud kliendile, et tal on arveldusarve muutunud, siis ma pigem arvan, et meie klient seda infot võib-olla ei vaata. Aga see tuleb välja kindlasti SAP-is, kus on arvelduskonto info küljes ja ta ei lähe sealt edasi. Ehk et siis tuleb SAP-is lisada uus arveldusarve külge. RTK I2: E-arve keskuses kontrollin arved ära, vaatan, kas kõik need rekvisiidid, mis on vajalikud, on õiged, kas arve summa on õige. Vaatan raamatupidamiskonteeringud üle. Ja siis saadan arve raamatupidamisprogrammi, meil on see SAP. RTK I2: Kui hankija on SAP helpi poolt loodud sama arvelduskontoga, siis mina eeldan, et see on õige, see on kontrollitud. SAP help ei loo mulle enne seda, kui ei ole kontrollitud. Kui tuleb uus, teine arvelduskonto, siis seda kontrollib ka SAP help. RIT I1: Seda kohustust me ei ole pannud, et kulujuht vaataks lepingus välja toodud arveldusarve numbrit. RIT I2: Seda märkab kindlasti RTK raamatupidaja. Meie pigem mitte, jah. [Kontonumbri muudatust] RIT I2: RTK kindlasti võrdleb, ilmselt nagu praegu pangadki võrdlevad kontonumbrit ja saaja nime, et kas need kokku lähevad. RTK I4: Kui tema on tulnud eurot kasutavast riigist, siis ma lähen oma isiklikku panka, panen tarnija nime, panen IBAN-i, ja pank ütleb mulle, kas nimi ja IBAN klapivad. RTK I4: Mina kontrollin IBAN-i ja nime vastavust peaaegu kõigil arvetel, olgu tema siis kuuskümmend eurot või kuussada tuhat eurot. Kontrollin oma pangas, kas nimi ja konto klapivad.
K1.2.9	Muutunud makseandmete kontroll	RTK I4: Kui tema on tulnud eurot kasutavast riigist, siis ma lähen oma isiklikku panka, panen tarnija nime ja IBAN-i, ja pank ütleb mulle, kas nimi ja IBAN klapivad. RTK I4: Enam ei oska seda ka edasi teistele anda, et mida ma vaatan, kuidas ma vaatan, mul on mõned asjad juba automaatselt käe see.
K1.3.1	Pettuse realiseerumine	RTK I2: Ma väga arvan, et ei lähe läbi. [pettus] RTK I2: Ma arvan, et see on kliendi vastutus, [realiseerunud pettus] sest nemad ju teevad lepingud. Kui nad tahavad mingit teenust saada, nad teevad ju lepingu. Lepingus on toodud ära, kes on makse saaja, summad ja kuhu nad tahavad saada makse, näiteks uuele arvelduskontole. Kui oleks võltsarve saadatud, siis mina ju ei tea, kas nad on tellinud selle teenuse või ei ole. Nii mitu inimest käib kinnitusringist läbi. Kui tuleb vale arve ja keegi leiab, et ta ei ole seda teenust selle inimese või firma käest tellinud, kas nad siis lasevad arve läbi või? RIT I2: Võib-olla hakatakse meilt küsima, et miks me kontonumbrit ei võrrelnud. Järgmine on RTK, et miks ta ei võrrelnud seda, mis on arve peal ja kuhu makse tegelikult läks. RTK I4: Ütlen ära, et on, aga need pole läbi läinud. Aga ma arvan, et see ei ole avalik info. [Pettuskatsetest. Täpsemalt ei olnud intervjueritav nõus kirjeldama]
K1.3.2	Auditeerimine	RTK I3: Riigikontroll kontrollib riigiasutusi finantsarvestuse poole pealt ja on väga põhjalik. Sügisel nad teevad vaheauditiit, mis kestab mitu kuud. Uue aasta alguses alustavad eelmise aasta aruandlusega, majandusaasta auditiga. Selle nad lõpetavad 30.-ks juuniks, nii et nad tegelevad tegelikult väga pikalt. RTK I3: Ma arvan, et meie siseauditor on Rahandusministeeriumis.

Kategooria 2 – Organisatsioonikultuur ja teadlikkus

K2.1.1	Töömaht	RTK I2: Ta on täiesti optimaalne praegu. Kuu alguses on olnud rohkem... Muidugi intensiivne on siis, kui kedagi asendad näiteks. Haiguste ja puhkuste ajal on ka kiiremaid perioode. Üldjuhul on mul ka asendatavate asutuste
--------	---------	---

		finantstöötajad tutvavad, ja meil on kontaktid antud, kellega kontakteeruda. Ja minu meelest arve menetlemine on sama protsess [erinevate klientide puhul], võib-olla natuke võtab kauem aega, et peab natuke mõtlema seal, igal asutul on ka oma omapära. RTK I2: Kui ma saadan SAP-i ära hankija arve ja kui ta leiab seal midagi, ütleme kontot ei ole näiteks, siis kontonumbrit nagu tookord oli, sest ma ei käi kõiki neid üle, siis igal juhul, kui kontonumbrit ei ole, ta tuleb mulle igal juhul tagasi, sest mul on väga palju arveid. RTK I3: Töökoormus on muidugi suurem aasta alguse perioodil, siis kui me teeme eelmise aasta lõpetamist. Jaanuar, veebruar, ka pool märtsi on kõige kiirem hooaeg. RTK I3: Meil on nii palju muid tegevusi ja ülekoormus puudutab teisi kohti. Kuna meil on töö jaotatud, siis pigem see inimene, kes teeb arveid, tema on vabastatud ju teistest töökohustustest. RIT I2: Ma arvan, et tema [Kulujuht X] kinnitab võib-olla 200 arvet kuus. RIT I2: Temal (Kulujuht Y) on sellised arved, millel võib olla näiteks ühel arvel 100 rida. Ta peab need kõik read läbi käima ja vaatama, et me tõesti näiteks oleme selle asja tellinud, mille eest meilt raha küsitakse. 100% kindlalt vaatab, ta on tohutult kohusetundlik. RTK I4: Kuna meie raamatupidajatele läks lihtsalt nii suureks see maht, siis võttis meie meeskond selle üle ja toimetame ise.
K2.1.2	Erakorralised maksed	RTK I1: Ka kiireid asju me saame menetleda Fiteki kaudu. Igal täistunnil on SAP-i ja Fiteki vaheline liiklus.gramma Saame vajadusel teha ka täna. Aga reeglina ei ole asju, mis ei kannataks homseni. RTK I1: Kui on nii kiire, et see tuleks samal päeval teha, siis üldjuhul asutus ekstra palub meilt. Saadab meili või ütleb, et tähtaeg on käes, et ole hea, palun maksame ära. RTK I1: Kui nüüd on tõesti vaja täna maksta, siis on juba rohkem inimesi kaasatud, siis me räägime sellest kliendiga tõenäoliselt telefoni teel. Sest et kui see jõuab raamatupidajani, kes arvet menetleb, ega ta siis üksi otsusta, ta konsulteerib meil seespool. Ja kui vaja, siis meie töötaja, kes tegeleb meil pangaga, siis tema võib küsida Riigikassast, kas saab. Me oma talituse siseselt seda siis konsulteerime omavahel. RTK I2: Kui on välismakse, mis kella kümnese seansiga tuleb, siis ma jõuan täna maksta, sest pank saab saata kella 11-ni, kui on vaja kohe täna ära maksta. Kodumaiseid makseid saab teha ka kella kolmeni, kui on vaja väga kiiresti täna ära maksta veel. Aga üldjuhul me maksame ikkagi kas maksetähtajal või siis kiired arved esimesel võimalusel. Tavaliselt me siis järgmiseks päevaks paneme. RIT I2: Sellel juhul lihtsalt jääbki see arve õigel ajal maksmata. Meil on olnud juhtusid, kus on vaja tõesti kiiresti maksta, aga siis ongi nii, et finantsosakond jälgib kinnitusringi, kui üks inimene on ära kinnitanud, siis kui järgmise juurde jõuab, võetakse kohe ühendust, et arve on sinu juures, nüüd on vaja tegutseda. Aga reeglilt, et nad peavad olema selle eelarvestanud, kontrollitakse, sellest me kindlasti kinnitusringi lühemaks ei tee. Kõik, kes peavad seal olema, need ka kinnitavad, jah. Kinnitusringist me ei lähe mööda. RTK I4: Maksetähtaeg ei saa olla homme, see lihtsalt ei käi nii.
K2.1.3	Riigikassa	RTK I1: Erakorralistest makseteks on limiit. Meil ei ole võimalik maksta suuri summasid kohe. Seda piirab Riigikassa. Riigikassa peab oma likviidseid vahendeid planeerima selleks, et riigi makseid teha. Ja igal hetkel tal ei ole kõik raha saadaval ja selle tõttu on meil broneeringute süsteem, et Riigikassa vaatab igal hommikul selleks päevaks tulnud makseid, või mis on selleks päevaks broneeritud. Kui meie oleme SAP-is oma kande ära sisestanud, siis on see makseks vajalik summa juba nii-öelda selles broneeringute süsteemis sees. RTK I2: Riigikassasse pärast kella 11 välismakset enam ei saa teha, siis ta läheb järgmise päeva maksesse. RTK I4: Riigikassa kontrollib ainult, et selline SWIFT kood on maailmas olemas. Riigikassa ei tee kontrolle, ta ei ole klassikalises mõttes pank.
K2.2.1	Infoturbe-koolitus	RTK I2: Üks kord aastas kindlasti... meil tuleb koolitus kõigepealt, loeme läbi, siis tuleb test pärast. [RIA küberkoolitus/test on 1x a kohustuslik] RIT I1: [Üks kord kuus tuleb õpiamps meilile]

K2.2.2	Info jagamine küberturvalisusest	RTK 12: Majakoosolek toimub iga kuu läbi Teamsi, kus räägitakse ka juhtumitest, kui on kuskil turvariskid või kuskil midagi on toimunud, siis antakse sellest ka teada ja hoiatatakse. Ühesõnaga sellest räägitakse, et väga-väga tähelepanelik peab olema. Iga nädal osakonna koosolek, ka siis räägitakse, kui on midagi tähelepanu vajavat. RTK 13: Infoturbspetsialist on eraldi teinud meile majakoolitusel täiendavat teavitamist... tõi näiteid. RTK 13: Võib ju erineval kujul olla teavitamine, vaevalt, et kõik teavad iseenesest kõike, mis maailmas toimub. Kui on mingi selle valdkonna teema, mida oleks hea teada, siis see võiks nii olla. RTK 14: Kirjutage juurde ka näiteks tekst, et kuidas oleks olnud õigem teha, nii et see inimene, kes loeb seda näidet, oskaks samastada. See peab olema väga lihtsate näidetega. [RIA jt teiste ekspertide poolt edastatud soovitusel meedias] RTK 14: ajalehes on kolm punkti, et kontrolli andmeid. Kontrolli veel kord andmeid ja küsi üle. See ei anna tavalisele inimesele, kelle igapäevatöö ei ole selline nagu minul, mitte midagi, see peab olema väga lihtsate näidetega, väga eluliste näidetega. Inimesed loeksid siis rohkem neid, kui on näidetena. Konkreetselt ei pea ütleva nimesid, ei pea summasid ütleva, aga tooge näide ja kirjutage, mida oleks saanud teha, et seda ei toimuks. Väga lihtsas keeles peab olema. RTK 14: Seletage ära, mis asi on alternatiivne kanal. Kust ta vaatab seda. Praktilised soovitusel peavad olema, mitte see, et kontrolli, kontrolli veel kord ja küsi üle, nagu ühes kohas oli. No mida see inimene teeb selle teadmise. Anna talle juhised kätte, kuidas ta kontrollib, kust ta kontrollida saab. Kirjeldage, et kirjuta Google'i otsingusse niimoodi, kasuta nime kuju, leia, et see ettevõtte on olemas.
K2.2.3	Koolitused on üldistel teemadel	RTK 12: Mul ei tule praegu küll meelde, et oleks olnud. [finantsvaldkonnaspetsiifilised infoturbe koolitused] Aga sellest on räägitud küll, on räägitud arvete kontrollimisest ja ma ütlen, et nende välisarvetega me juba SAP-i toega ju kogu aeg tegeleme, kui mingid kahtlused on. Et ei saa tulla arve sisse, kui ta ei ole õige arve. Saab, kui firma on olemas, õigete tunnustega. Kui on tähe muutus, siis ta on uus tarnija ja siis seda hakatakse kohe vaatama. Ja siis kõikides süsteemides vaadatakse, kas on nii või ei ole. RTK 13: Need koolitused on olnud üldkoolitused ja need on kogu majale ühised. Ega ta ju paha ei tee, kui ta oleks, aga samas jälle otsest puudust ka ei ole tundnud. Lõpuks see kindlasti ju taandub ka selle taha, et me oleme väga hõivatud ja ei saa ju kogu aeg tegeleda ainult koolitusega. RTK 13: Ja peale selle, kui meile tulevad meilid, siis osad kirjad lähevad meililüüsi. Sealt olen mina leidnud õige mitu vajalikku kirja, mis on minu tee pealt ära korjatud, mida ma ei leia. Et mõnikord on see väga agar. Ma arvan, et see on mingi tehniline põhjus. Ma arvan, et see on meie teenusepakkuja. Et kui kirjavahetuse lihtsuses tundub midagi imelikku. Ühesõnaga et ta justkui tundub ohtlik sissetulekul...siis saan teavituse, et ma vaataksin, kas need kirjad on õiged või valed. Ja kui nad on õiged, siis ma saan mingit nupukest vajutada, siis ta tuleb mulle ikkagi meilina sisse. RIT 11: Raamatupidamiskonverentsil rääkis üks naisterahvas ka just nendest ohtudest ja imelikust arvetest. Ja mulle tundus, et meil on võib-olla tõesti natukene see koolitus liiga üldine, et see sobib tervele majale ja meile ka kindlasti. Aga võib-olla rohkem sellistest juhtumitest, et milliseid arveid saadetakse. [Ükski intervjuueeritav ei maininud simuleeritud ründe testimist või valdkonnapõhiste koolituste läbimist] RTK 14: Ei ole mingeid koolitusi. Ma tarbin meediat ja teen järeldused. Niimoodi ma selle teema peale sattusin ja enda ülesandeks võtsin. RTK 14: Meil on väga hea koostöö oma osakonna sees, ja kõik, mis ma jälle mingisuguse omapärase temaatika avastan RTK 14: Mina sain kinni üks kord, ma ei mäleta, kas RIA saatis mõned aastad tagasi ühe... see oli avalikult üleval, meedias läbiv artikkel. Ja sealt hakkasin ma seda uurima, et issand jumal, mis võimalused. Hakkasin mõtlema, et mis kõik võib juhtuda ja sealt võtsingi kätte ja sealt see tuli, et ma sellise kirja iga kord

		asutustele saadan. Et ikka jah, meediast, mina sain meediast, mitte mingeid koolitusi mul olnud ei ole. RTK I4: Ma olen uurinud, et mida teevad näiteks teised riigid. Ma olen aru saanud, et tehakse käsitööd hästi palju. Meil on ju suur osa automatiseeritud, ma ei kujuta ette, et kõike seda massi teha käsitsi, mis meil praegu näiteks Fiteki kaudu käib. Enamus riikides tehakse käsitsi kogu seda massi.
K2.3.1	Kahtlustamine ja topelt-kontroll	RIT I1: Ühesõnaga, meile tuli üks arve, mis oli pool vene keeles, pool eesti keeles. Ma ei mäleta, kas seal arve all oli veel mingit ingliskeelset teksti. Kuna seal ei olnud ühtegi nime, kellele see arve peab kuuluma, siis ma võtsin ühendust. Aga ma otsisin kuskilt, ma ei mäleta, kas äriregistrist või kuskilt otsisin need kontaktid, kirjutasin sinna firmasse, saatsin selle arve pildi, küsisin, kas see on teie poolt saadetud arve? Vist kahe nädala jooksul ma vist tuletasin veel kaks korda neile meelde, ma ei saanud seda vastust. Siis ma kustutasin selle arve lihtsalt ära. RIT I1: Me selliseid üldaadresse üldjuhul ei usaldanud ka varem [Boltist] RIT I1: Ma ei ole alati nendes 100 protsenti kindel... ja vahepeal käime pisteliselt lepingutest neid asju kontrollimas. Eriti suuremate summade puhul, et kas lepingusumma vastab esitatud arve summale. RTK I4: Ma panen tarnija nime ja IBAN-i ning pank ütleb, kas nimi ja IBAN klapiivad RTK I4: Kakskümmend tuhat, mis läbi on käinud nendest meediateadetest ja RIA teadetest, seal on ikkagi kahekümnest tuhandest on need hakanud peale. RTK I4: Pigem võtame ühendust, kui, et on mingid teemad hiljem. RTK I4: Ei, ei ole [kirjalikult dokumenteeritud] RTK I4: Meil on omad inimesed ja nad teavad mu põhimõtteid. RTK I4: Kui on täheerinevused või pisierinevused, ma närin ka nende kallal RTK I4: Kas ma julgen maksta sada tuhat eurot? Mina küll ei julgeks. RTK I4: Ma ei loo SAP-i võimalusi, milles mina ise kindel ei ole. RTK I4: Ma olen ääretult jäik.
K2.3.2	Teadlikkus tuleneb töökogemusest ja erialasest tähelepanelikkusest	RTK I3: Ma arvan, et meil on sellega seoses tunduvalt rohkem sellist puhvrit või bürokraatiat või neid kihte, mis juba on ehitatud siia peale selle jaoks. [võrreldes erasektoriga] RTK I3: See on töö- ja elukogemuse kombinatsioon, mis on toonud sellised teadmised. Üks asi on see, et me oleme väga kaua seda tööd teinud. Me elame silmad lahti ja loeme ja kuuleme, mis maailmas toimub. Mina märkan kogu aeg neid uudiseid. Võib-olla on tõesti see niinimetatud professionaalne kretinism, et sa lihtsalt märkad selle valdkonna uudiseid rohkem, ja selle tõttu ka siis kuidagi oled rohkem kursis juba iseenesest, ilma et sa midagi teeksid lisaks. RTK I3: Selleks ma ei pea ennast teadlikult koolitama, vaid lihtsalt piisab sellest, et ma kuulen, loen ja panen tähele, mis puudutavad selliseid juhtumeid. Omavahel oma osakonnas jagame infot, kui oleme midagi sellist kuulnud või mis info vahendamist väärrib. RTK I4: Ei ole koolitusi läbinud. Ma tarbin meediat ja teen järeldused. Niimoodi ma selle teema peale sattusin ja enda ülesandeks võtsin.
K2.3.3	Makseandmik kui potentsiaalne luurevahend	RTK I3: Makseandmik on olemas Justiitsministeeriumi nõudel. Eesmärk selle loomisel oli korruptsiooniennetus. Ega me poleks seda ise teinud RTK poole pealt ja meie sellel vajadust ei näe. Seal on tõesti väga-väga avalik kõik, et, igaüks võib vaadata kellele, kui palju, millal on makstud. Muidugi sealt jäävad välja eraisikute maksed ja teatud asjad, aga valdavalt on seal olemas, just. RIT I2: Ma ei pea seda infot oluliseks, et seda peaks näitama. Mis kasu sellest keegi saaks? Võib-olla jah, et kui vaatad, kellega me tehinguid teeme, et oma kurjad näpud sinna vahele toppida. Ma arvan lihtsalt, et tänapäeva maailmas selliseid suuremaid tehinguid ja summasid ei peaks pigem kõigile näitama. See kasu on kindlasti seal palju väiksem, kui see, mis kahju seal tõesti võib tekkida.
K2.3.4	Intsidentide käsitlemise protsess	RIT I2: Ma ei tea, kas sellist otsest juhendit vaja on. RIT I2: Ma kindlasti esimesena teavitaksin osakonnajuhatajat, siis ma teavitaksin RTK raamatupidajat, tema saab Riigikassa väljavõtteid võtta. Ja Rahandusministeeriumi kontakti, kes kaardi väljastas. Seda olen mina näinud panga väljavõtte pealt, mida ma kord kuus vaatan, et kas seal on tehinguid. Infoturvet, muidugi.

Summary

PREVENTING BUSINESS EMAIL COMPROMISE THROUGH ORGANIZATIONAL CONTROLS IN THE ESTONIAN PUBLIC SECTOR

Merilyn Haugas

This master's thesis examined invoice fraud as a subtype of business email compromise (BEC), in which the attack is carried out through an organisation's routine invoice-processing workflow by manipulating payment details. The study was motivated by the observation that existing academic literature has primarily focused on technical security measures and psychological manipulation techniques, while considerably less attention has been paid to organisational vulnerabilities and work process-related control mechanisms. The empirical analysis assessed the extent to which the control measures implemented in the analysed public sector organisations correspond to the organisational security measures described in the theoretical framework and identified the stages of the invoice processing process where vulnerabilities may emerge.

The theoretical framework demonstrated that business email compromise attacks are hybrid threats based on social engineering, whose success depends on the interaction between technical, psychological, and organisational factors. The literature review indicated that invoice fraud is particularly likely to succeed in situations where control mechanisms rely on trust, individual experience, or assumptions that another party has already performed the necessary verification. Key risk factors identified in previous research included the absence of segregation of duties, lack of independent verification channels, heuristic decision-making caused by workload and time pressure, organisational pressure to simplify controls, insufficient cybersecurity awareness, and excessive trust in technical systems. Theoretical findings also highlighted that the most effective protection mechanisms are multi-layered and combine technical, organisational, and behavioural controls.

The empirical study confirmed that the analysed organisations had implemented several organisational security measures consistent with the theoretical framework. The invoice processing workflow relied on standardised e-invoicing, integrated information systems, and multi-stage approval procedures. The study showed that the mandatory use of e-invoices in the Estonian public sector significantly reduces the effectiveness of fraud schemes based on forged email addresses or manipulated invoice attachments. In addition, the principle of segregation of duties was systematically applied throughout the process, as invoice processing involved multiple employees and additional approval layers for larger

payments. An important empirical finding was that approval procedures were not bypassed even in urgent payment situations. Instead, additional parties were involved when necessary, even though urgency and time pressure are commonly described in the literature as key manipulation techniques used in business email compromise attacks.

At the same time, the study identified several process-related vulnerabilities that may create conditions for invoice fraud. The most significant vulnerability was the diffusion of responsibility between organisations operating within a shared service model. The service provider relied on the client organisation's substantive verification of invoices, while the client assumed that formal verification controls were performed by the service provider. Although such a trust-based arrangement functioned effectively under normal circumstances, it could fail in situations where invoice content appeared legitimate, but payment details had been manipulated. The findings indicated that the primary risk did not arise solely from technical shortcomings but from assumptions regarding which party was responsible for a specific control activity.

Another significant vulnerability concerned the absence of a mandatory procedure for verifying changes in payment details through an alternative communication channel. Although employees informally used known contacts or contractual information to verify suspicious payment requests, these practices had not been formally standardised. As a result, the effectiveness of the control depended largely on employees' experience, initiative, and attentiveness. The study also revealed that some critical controls relied on the tacit knowledge and personal initiative of individual employees rather than formally documented procedures, particularly during the creation and verification of supplier data. Such dependence on individual expertise creates organisational vulnerability in situations involving workload increases, staff turnover, or temporary replacements.

The research further demonstrated that heavy workloads and routine tasks may reduce employees' attentiveness, especially when large volumes of invoices must be processed within limited timeframes. In addition, interviews revealed that technical systems could create a false sense of security, leading employees to assume that anomalies would be detected by another process participant or automated system. These findings support the theoretical argument that preventing business email compromise is not solely a technical issue but also an organisational and behavioural challenge.

The thesis concludes that effective protection against invoice fraud depends on the overall structure of the invoice processing workflow rather than on individual technical

solutions. The most effective organisational measures identified in the study included multi-stage approval procedures, segregation of duties, independent validation of payment details through alternative communication channels, standardisation of procedures, and role-specific cybersecurity training. The findings also suggest that organisational resilience against invoice fraud depends significantly on whether security measures are institutionalised as formal procedures or rely primarily on employees' individual awareness and experience.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Merilyn Haugas ,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose
Ärikirjapettuste tõkestamine töökorralduslike meetmete abil Eesti avaliku sektori ,
näitel

mille juhendajad on Kristjan Pulk PhD ja Heidi Reinson MSc ,

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada Tartu Ülikooli digitaalarhiivi kuni autoriõiguse kehtivuse lõppemiseni;

2. annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi kaudu Creative Commons litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni;
3. olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile;
4. kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Merilyn Haugas
19.05.2026