

Sisekaitseakadeemia

Finantskolledž

Angela Lõhmus

**RAHAPESU TÕKESTAMISE NÕUETEST TULENEVA  
HOOLSUSKOHUSTUSE TÄITMINE EESTIS  
RAAMATUPIDAMISETTEVÕTJATE NÄITEL**

Lõputöö

Juhendaja:

Maret Güldenkoh, MBA

Tallinn 2021

## SISEKAITSEAKADEEMIA LÕPUTÖÖ ANNOTATSIOON

Finantskolledž	Juuni 2021
<p>Töö pealkiri eesti keeles: Rahapesu tõkestamise nõuetest tuleneva hoolsuskohustuse täitmine Eestis raamatupidamisettevõtjate näitel</p> <p>Töö pealkiri võõrkeeles: Compliance With Anti-Money Laundering Due Diligence Requirements Among Accounting Firms In Estonia</p> <p>Lõputöö on kirjutatud eesti keeles, kasutatud on 61 allikat.</p> <p>Lõputöö eesmärgiks oli välja selgitada hoolsuskohustuse täitmise viisid Eestis raamatupidamisettevõtjate seas. See tähendab, kui põhjalikult kontrollivad raamatupidamisettevõtjad seatud hoolsusmeetmete kohaselt oma tehingupartnerite tausta ning nendega kaasnevaid võimalikke riske.</p> <p>Eesmärgi täitmiseks püstitas autor neli uurimisküsimust, mis hõlmasid rahapesu tõkestamise nõuete uurimist, raamatupidamisettevõtjate võimalust rahapesu tuvastada, hoolsuskohustuse täitmise viiside kindlakstegemist ning nõuete järgimise puudujääkide väljaselgitamist.</p> <p>Uurimisülesandeid seas autor kolm: analüüsida teemakohast kirjandust rahapesu olemuse ja skeemide kohta, analüüsida rahapesu tõkestamisest tulenevaid nõudeid raamatupidamisettevõtjatele ning neile seatud nõuete järgitavust, et vajadusel teha ettepanekuid.</p> <p>Uuringust selgus, et suurimad puudujäägid esinevad riikliku taustaga isikute kindlakstegemisel, tegelike kasusaajate tuvastamisel, rahapesu teadete esitamisel ning võimalike finantssanktsioonide all olevate isikute kindlakstegemisel. Lisaks tunnetati raamatupidamisettevõtjatele seatud nõudeid ebaproportsionaalsena võrreldes raamatupidamisettevõtjate võimekusega riske tuvastada.</p>	
Võtmesõnad: rahapesu, hoolsuskohustus, riskipõhine lähenemine, tunne oma klienti põhimõte	
Võõrkeelsed võtmesõnad: <i>money laundering, customer due dilligence, risk-based approach, KYC</i>	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
Töö autor: Angela Lõhmus	
<p>Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Annan Sisekaitseakadeemia tasuta loa (lihtlitsentsi) minu loodud teose reprodutseerimiseks säilitamise ja elektroonilise avaldamise eesmärgil, sealhulgas Sisekaitseakadeemia raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni. Annan loa teose üldsusele kättesaadavaks tegemiseks Sisekaitseakadeemia veebikeskkonna kaudu sealhulgas Sisekaitseakadeemia raamatukogu digikogu kaudu ja paber kandjal Sisekaitseakadeemia raamatukogus kuni autoriõiguse kehtivuse tähtaja lõppemiseni. Olen teadlik, et nimetatud õigused jäävad alles ka autorile. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.</p> <p>(allkirjastatud digitaalselt)</p>	
Vastab lõputöö nõuetele	
Juhendaja: Maret Guldenkoh	(allkirjastatud digitaalselt)
Kaitsmisele lubatud	
Kolledži direktor: Kerly Randlane	(allkirjastatud digitaalselt)

# SISUKORD

SISSEJUHATUS .....	5
1. RAHAPESU NING SELLE TÕKESTAMINE .....	8
1.1 Rahapesu olemus.....	8
1.2 Rahapesu tõkestamine ja tuvastamine.....	12
1.3 Riskipõhine lähenemine .....	15
1.3.1 Tunne oma klienti põhimõte .....	19
1.3.2 Tegelike kasusaajate tuvastamine .....	22
2. RAAMATUPIDAMISETTEVÕTJATE HOOLSUSMEETMED .....	25
2.1 Uurimismeetodi ja uurimisandmete kirjeldus .....	25
2.2 Raamatupidamisettevõtjate hoolsuskohustuse täitmine .....	28
2.3 Järeldused ja ettepanekud .....	38
KOKKUVÕTE .....	42
SUMMARY .....	45
VIIDATUD ALLIKATE LOETELU .....	46
Lisa 1. Küsimustik raamatupidamisettevõtjatele .....	52
Lisa 2. Raamatupidamisettevõtete arv Äriregistris.....	58
Lisa 3. Tehingupartneri taustakontrolli võimalused .....	59
Lisa 4. Vastused maakondade lõikes .....	61

## TERMINITE JA LÜHENDITE LOETELU

RahaPTS- Rahapesu ja terrorismi rahastamise tõkestamise seadus

EMTAK- Eesti majanduse tegevusalade klassifikaator

CDD- kliendi suhtes läbiviidav hoolsuskohustus (*customer due diligence*)

FATF- Rahapesu tõkestamise toimikond

KYC- tunne oma klienti põhimõte (*know your customer*)

*Offshore* piirkond- madala maksumääraga piirkond või piirkond, kus välismaa äriühingutel puudub maksukohustus

## SISSEJUHATUS

Autori teemavalik tulenes sellest, et viimastel aastatel on avastatud laiaulatuslikke rahapesuga seotud juhtumeid. Mitmete pankade seas on algatatud rahapesuga seotud kriminaalmenetlusi (Rahapesu Andmebüroo, 2020, lk 13). Lisaks on 2019. aastal Finantsinspeksioon teinud pankade seas rahapesu kontrole (Finantsinspeksioon, 2019a). Seega on oluline pöörata rahapesu tõkestamisele tähelepanu. Autoril tekkis huvi, mil määral panustavad rahapesu tõkestamise peale pankade eraettevõtjad. Rahapesu on oluline tõkestada, et takistada illegaalsel teel saadud raha majandusse integreerumist ja seeläbi raha tegelikku päritolu ja sellega seotud tegevust tuvastada.

Lõputöö aktuaalsus seisneb selles, et Rahandusministeeriumi 2018–2021 arengukava üheks eesmärgiks on finantskeskkonna usaldusväarsuse suurendamine (Rahandusministeerium, 2017, lk 4). Lisaks keskendub rahapesu tõkestamisele ka Finantsinspeksiooni 2019–2021. aasta strateegia (Finantsinspeksioon, 2019b, lk 12). Selle täitmiseks moodustati Finantsinspeksioonis juurde eraldi töörühm, et rahapesu tõkestamist tõhustada (Finantsinspeksioon, 2019a).

Rahapesu tõkestamine on oluline finantskeskkonna usaldusväärseks muutmisel ning raamatupidamisettevõtjatel on autori hinnangul selle tagamisel suur roll. Autori arvates on raamatupidamisettevõtjatel võrreldes teiste eraettevõtjatega eelis tuvastada kahtlase sisuga tehinguid, sest nad saavad aru tehingute kajastamisest ning nad on teadlikud veel laekumata tehingutest, kui raha pole ettevõttesse laekunud ning ülekannet pole toimunud. Rahapesu- ja terrorismi rahastamise tõkestamise seadus § 49 järgi on raamatupidamise ja maksustamise valdkonnas nõustamisteenuse pakkujatel, kui kohustatud isikutel, kohustus esitada Rahapesu Andmebüroole teade, kui nad tuvastavad asjaolusid, mis viitavad rahapesule (Rahapesu- ja terrorismi rahastamise tõkestamise seadus, 2017).

Lõputöö uudsus seisneb selles, et autorile teadaolevalt pole raamatupidamisettevõtjalt uuritud, mis ressursse kasutades nad täidavad hoolsusmeetmeid riskipõhisel lähenemisel, kui nad kliendi riskiprofiili tuvastavad. Näiteks, mis meetodeid kasutades teevad kindlaks isikusamasuse ning tegelikud kasusaajad. Varasemalt on uuritud üldisemalt, kas raamatupidamisteenust pakuvad ettevõtjad täidavad hoolsuskohustust. 2014. aastal on

kirjutatud Tallinna Tehnikaülikoolis magistritöö teemal „Audiitorid ja raamatupidamisteenuse pakkujad rahapesu tõkestamise süsteemis Eesti näitel“ (Pärnpuu, 2014). Selles töös uuriti raamatupidamisteenust pakkuvate ettevõtete teadlikkust rakenduvatest nõuetest, kuid ei käsitletud hoolsusmeetmete täitmise viise. Viiside valik näitab, kuidas rahapesu tõkestamise ettevõtjad panustavad. Hoolsuskohustuse rakendamist on käsitletud veel magistritöös „Rahapesu tõkestamise õiguslikud alused ja meetmed krediidi- ja finantseerimisasutustes“ (Tkatsova, 2014). Riskipõhisest lähenemisest on kirjutatud töö peakirjaga „Euroopa parlamendi ja nõukogu 20.05.2015 direktiivist (EL) 2015/849 tuleneva riskipõhise lähenemise ja Eesti kohtupraktikas väljatöötatud majandusliku põhjendatuse kriteerium“ (Šesterikov, 2016). Siiski ei analüüsitud selles töös riskipõhist lähenemist teaduslikel allikatel. Lisaks on 2018. aastal rahapesu tõkestamise direktiivi muudetud ning seeläbi soovib autor teada, kui põhjalikult täidavad raamatupidamisettevõtjad hoolsusmeetmeid.

Rahapesu Andmebüroo 2019. aastaraamatust selgus, et raamatupidamisettevõtjad olid 2019. aastal esitanud kokku 20 teadet. Võrreldes enamike kohustatud isikute teadete saatmise arvuga on raamatupidamisettevõtjate esitatud teadete arv väiksem. (Rahapesu Andmebüroo, 2020, lk 9). Lisaks selgus Pärnpuu (2014, lk 42) magistritööst, et 82% raamatupidamisteenuse pakkujatest puudus sisekontrollieeskiri, millega on hoolsuskohustuse täitmine reguleeritud. Kui sisekontrollieeskiri puudub, saab järeldada, et rahapesu tõkestamise eeskirjade täitmisel esineb puudujääke. Eelnevast püstitub probleemküsimus, kuidas raamatupidamisettevõtjad täidavad rahapesu nõuetest tulenevalt oma hoolsuskohustust?

Mida põhjalikumalt täidetakse hoolsusmeetmeid, seda efektiivsemalt toimib rahapesu tõkestamine. Seega on oluline, et raamatupidajatele kui kohustatud isikutele, kes näevad rahade liikumist ja võrreldes enamike kohustatud isikutega ka ettevõtlustegevuse tervikpilti, et nad kõiki hoolsuskohustuse meetmeid rakendaksid. Seega annab tulemus teada, mis meetmete rakendamisel on puudujääke. Autor on püstitanud uurimisprobleemist tulenevad uurimisküsimused:

1. Milliseid kriteeriume tuleb raamatupidamisettevõtjatel rahapesu tõkestamise nõuete alusel täita?
2. Mis ressursse kasutades saavad raamatupidamisettevõtjad hoolsuskohustust täita?
3. Kuidas raamatupidamisettevõtjad saaksid rahapesu tuvastada?

4. Milliste hoolsusmeetmete rakendamise osas võib raamatupidamisettevõtjatel esineda puudujääke?

Lõputöö eesmärgiks on välja selgitada hoolsuskohustuse täitmise viisid Eestis rahapesu tõkestamise nõuetest tulenevalt raamatupidamisettevõtjate näitel. See tähendab, mis võimalusi on hoolsuskohustust täita ning milliste hoolsusmeetmete täitmisel esineb puudujääke.

Eesmärgist tulenevalt püstitas autor järgnevad uurimisülesanded:

1. Analüüsida teemakohast kirjandust rahapesu olemuse ja skeemide kohta ning selle tõkestamise kohta riskipõhisel lähenemisel.
2. Analüüsida rahapesu tõkestamisest tulenevaid nõudeid raamatupidamisettevõtjatele.
3. Sünteesida uuringu tulemusi ja analüüsida raamatupidamisettevõtjatele seatud nõuete järgitavust ning vajadusel teha ettepanekuid.

Eesmärgi täitmiseks kasutab autor kombineeritud uurimismeetodit. Kvantitatiivse analüüsi puhul kasutab autor kirjeldavat statistikat ehk kogutud andmed esitatakse visuaalselt diagramme esitades (Õunapuu, 2014, lk 184; Bryman, 2012, p. 337). Andmekogumismeetodina kasutatakse ankeetküsitlust, kus esitatakse avatud kui ka suletud küsimusi. Avatud küsimuste puhul kasutatakse kvalitatiivset sisuanalüüsi ehk sarnase mõttega tekst kodeeritakse ning koondatakse kategooriatesse (Laherand, 2008, lk 290; Saldana, 2009, pp. 8–11).

Lõputöö esimene peatükk koosneb kolmest alapeatükist. Esimeses alapeatükis antakse ülevaade rahapesu olemusest ja skeemidest. Teises alapeatükis analüüsitakse rahapesu tõkestamist ning kuidas raamatupidajad saaksid rahapesu tõkestamisele kaasa aidata ning kahtlaseid tehinguid tuvastada. Kolmandas alapeatükis antakse ülevaade, mis võimalusi on hoolsuskohustust täita riskipõhise lähenemise järgi. Seejärel keskendutakse tunne oma klienti põhimõttele ning tegelike kasusaajate tuvastamisele. Teine peatükk koosneb kolmest alapeatükist. Esimeses alapeatükis kirjeldatakse uurimismeetodit ning kirjeldatakse uurimisandmeid, teises alapeatükis analüüsitakse raamatupidamisettevõtjate seas läbiviidud küsitlust. Kolmandas alapeatükis tehakse küsitluse põhjal järeldused ning vajadusel antakse soovitusi. Töös kasutatakse 15.02.2021 seisuga kehtivaid õigusakte.

# 1. RAHAPESU NING SELLE TÕKESTAMINE

Käesolevas peatükis antakse ülevaade rahapesu faasidest ning rahapesu olemusest. Tuuakse välja, missuguseid võimalusi leiavad rahapesijad raha päritolu varjamiseks ning kuidas raamatupidajad saaksid rahapesu tuvastada ja tõkestada. Lisaks antakse ülevaade riskipõhisest lähenemisest ning tuuakse välja, mis nõuded rakenduvad rahapesu tõkestamise nõuetest raamatupidamisettevõtjatele ning analüüsitakse kliendi riskiprofiili tuvastamist.

## 1.1 Rahapesu olemus

Rahapesu on protsess, mille käigus varjatakse kriminaalsel teel saadud tulu ning suunatakse see legaalsesse majandusse. Rahapesu koosneb kolmest etapist. Esimeses etapis suunatakse kriminaalsel teel saadud tulu majandusse. Teises etapis varjatakse saadud tulu, et poleks võimalik avastada saadud tulu päritolu. Kolmandaks jõuab kriminaalsete tunnusteta raha tagasi rahapesijateni. (Anitei & Gardikiotis, 2015, p. 14)

Seega jagatakse rahapesu protsess kolme faasi (Gilmour, N., 2020, p. 515; vt joonis 1, lk 11):

- Paigutamine: suunatakse ebaseaduslikul teel saadud vahendid legaalsesse majandusse;
- Ladestamine: saadud tulu varjamine;
- Integreerimine: raha investeerimine ning uue vara soetamine.

Michael Levi (2002, p. 182) sõnul on rahapesu kriminaalsel teel saadud tulu varjamine, viies sularaha seaduslikku finantsvääringsusse. Rahapesuks peetakse ka asjaolu, kui vara on illegaalsel teel saadud ning varjatakse selle päritolu. Rahapesuna on käsitletav ka rahapesija abistamine ning vara varjamine, omamine ja kasutamine, kui teatakse, et see raha on kuritegelikku päritolu. (Kärner, 2019, lk 519-520) Seega peetakse rahapesuks nii varjamis- kui ka muundamistegevusi. Varjamistegevuste all mõeldakse kuritegelikust tegevusest saadud vara päritolu ja omamise varjamist. Lisaks on selleks ka varaga seotud õiguste varjamine. Muundamistegevusena käsitletakse vara varjamist selle muundamisel, omandamisel, valdamisel või ülekandmisel, mille eesmärk on peita vara päritolu ning abistada kuriteos osalenud isikut. Selle tegevuse eesmärgiks on vältida, et rahapesijat võetaks õiguslikult vastutusele. (Evestus, 2015, lk 360)



Organiseeritud kuritegevus on andnud aluse hakata rahapesu tõkestama. Rahapesu eelkuriteod nagu näiteks narkokaubandus või alkoholiga kauplemine on rahapesijate vara suurendanud ning seetõttu on nad pidanud hakkama mõtlema viise, kuidas oma varast märkamatuks kasu saada. Kui algselt tegeleti narkoäri vastase võitlusega, siis aja jooksul on lisandunud mitmeid teisi eelkuriteoliike. (Tibar, 2007, lk 578) Rahapesu eelkuriteoks peetakse kõiki karistusseadustiku eriosas märgitud kuriteoliike, mille tulemusel on saadud rahapesu varjamis- või moondamistegevustes kasutatav vara (Evestus, 2015, lk 363). Eelkuritegu on oluline rahapesu koosseisu hindamiseks ehk see on üks eeldustest rahapesu toimepanekuks (Evestus, 2015, lk 361). Eelkuriteona käsitletakse ka mitmed majanduskuritegusid, sealhulgas illegaalne majandustegevus, kui puudub tegevusluba, maksukuriteod ning pankrotikuriteod (Evestus, 2015, lk 362). Seega on eelkuriteoliike palju ning ühtlasi rahapesu tõkestamisega aidatakse takistada mitmesuguseid kuritegusid. Sellest järeldub, et rahapesu tõkestamise nõudeid on oluline järgida, kuna see aitab üldist kuritegevust takistada.

Indrek Tibar (2007, lk 581) nendib, et rahapesu esimest etappi (*placement*) peetakse kõige keerulisemaks, kuna see etapp on rahapesijate jaoks kõige suurema riskiga. Üheks võimaluseks on sularaha paigutamine kontole, kasutades isikuid, kes raha erinevatele kontodele kannavad või kui sularaha viiakse teise vääringusse, näiteks füüsiliseks varaks (Raza, *et.al.*, 2020, pp. 912–929). Füüsiliseks varaks võib olla näiteks kuld, juveelid või antiikesemed. Rahapesijad kasutavad neid, kuna nende esemete päritolu on keeruline kindlaks teha. Rahapesijad võivad öelda, et tegemist on päritud varaga või see on soetatud kolleksionäridelt. (Teichmann, 2017, pp. 132–134)

Kulda kasutatakse nii paigutamise kui integreerimise etapis, kuna raha eest on kerge soetada kulda ning hiljem saadud kulla päritolu on keeruline tuvastada. Kulla kasutamise põhjuseks on ka asjaolu, et selle väärtuse kasvades saavad rahapesijad kulda võõrandada ja tulu teenida. (Teichmann, 2017, p. 132) Siiski kõike sularaha ei suunata kontodele, rahapesijatel on tarvis, et oleks reserv, millest saaks illegaalseid toiminguid edasi rahastada. Lisaks kasutatakse osa raha igapäevaste kulude katteks, näiteks tasutakse restoraniarveid või tehakse kulutusi riitele. (Soudijn, 2016, p. 302) Sellest järeldub, et proovitakse teha mõõdukalt niivõrd palju kulutusi olemasoleva rahaga, et seda vähem finantssüsteemi peaks suunama. Eelpool toodust lähtuvalt on rahapesijatel väiksem risk vahele jääda.

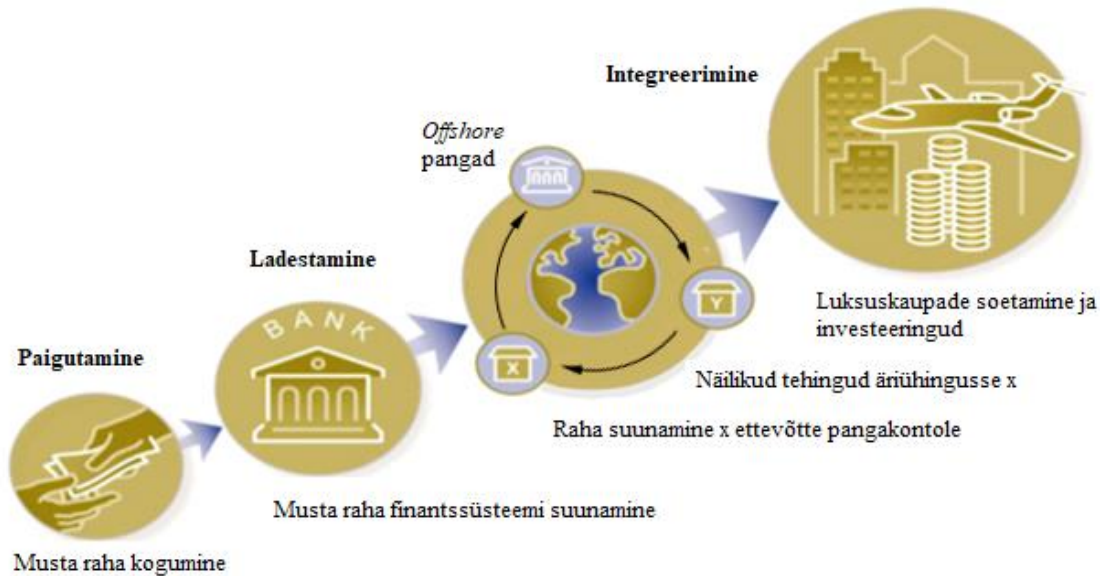
Indrek Tibari (2007, lk 581) sõnul kasutatakse raha paigutamise etapis tihti variisikuid. Variisik on inimene, kes vahendab pangakontode vahelt raha, et seda puhtaks pesta ning poleks võimalik tegelikku isikut tuvastada. Enamasti on variisikuteks iniviidid, kes internetist tööd otsivad ning usuvad, et see on hea võimalus raha teenida. Rahapesijad kasutavad nende pangakaartide andmeid, et tehinguid teha ja seeläbi enda identiteeti varjata. Variisikute kontodele viiakse sularaha ning hakatakse seda erinevate kontode vahel liigutama ja hoiustele kandma. Tihtipeale käib raha paigutamise protsess erinevate riikide vahel, et jälgi segada kuniks see jõuab ringiga rahapesijate kontodeni. (Raza, *et.al.*, 2020, pp. 913– 919)

Juveelide korral võib juhtuda, et rahapesija registreerib juveelipoe, et seal teha näilikke tehinguid eesmärgiga illegaalne raha legaalseks muuta. Rahapesija ostab kollektsoonäärilt legaalselt juveele, seejärel teeb näilikke tehinguid, et illegaalse päritoluga raha ärisse suunata ning saadud raha näidata müügist saadud tuluna. Peale seda ostab ta n-ö klientidelt saadud raha eest uued juveelid, tegelikult ostab ta juveele endalt ning maksab kriminaalsel teel saadud raha eest. (Teichmann, 2017, p. 133) Kui tehakse tehinguid alla kehtestatud rahalise piirmäära, pole kohustust esitada sularahateadet ning rahapesija vahelejäämise oht on väike. Sularaha teate esitamise kohustus tuleneb Rahapesu ja terrorismi rahastamise tõkestamise seaduse § 49 lg 3 järgi alates 32 000 eurost, kui see tehing tehakse sularahas, sealhulgas aasta jooksul mitme maksena (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017).

Ladestamise (*layering*) etapis varjatakse raha päritolu ning tehakse tehinguid, et raha päritolu tuvastamist keerulisemaks muuta. Selleks kasutatakse varifirmasid ning fiktiivseid arveid. (Soudijn, 2016, p. 299) Ladestamise etapis võivad olla tehingud ka füüsiliste isikutega. Näiteks annab rahapesija kriminaalsest tegevusest saadud tulu teisele isikule, kes selle laenuna rahapesijale tagasi annab. Sel meetodil näib see kui tavalise laenu andmisena. (Soudijn, 2016, p. 301)

Integreerimise (*integration*) faasis püütakse näidata enda rahaga seotud tegevusi legaalsena. Selleks luuakse ettevõtte, kuid tegelikkuses tegeletakse ettevõtlusega vaid eesmärgil, et raha seaduslikule kujule viia. Selleks registreerib rahapesija ettevõtlustegevuse, teeb näilikke tehinguid ning kahtluse hajutamiseks teeb osa tehinguid ka päriselt. Enamasti kasutatakse nõustamissettevõtteid, kuna tehingute tegelikkust on keeruline hinnata. (Teichmann, 2017, p. 134) Integreerimise faasis soetatakse luksukaupu nagu autod, kinnisvara ning alustatakse

ettevõtlustegevusega (Soudijn, 2016, p. 299). Rahapesust saadud tulu võidakse näidata ka kui legaalse tuluna. Selleks ühildatakse kriminaalne tulu legaalse tuluga, seejuures tasutakse kogu tulult maksud. (Soudijn, 2016, p. 301) Seega on integreerimise faasi eesmärk näidata oma tegevust täiesti legaalsena, et rahapesu algetappi poleks võimalik tuvastada.



Joonis 1. Rahapesu faasid (Moustafa, *et al.*, 2015, p. 305)

Varifirmasid (*shell entities*) moodustatakse, et varjata oma tegevust ning anda illegaalsele tegevusele seaduslik varjund. Usaldusväarsuse suurendamiseks soetatakse interneti vahendusel varifirma, mis on juba tegutsenud ja seeläbi oma jätkusuutlikkust ja usaldusväarsust tõestanud. Ettevõtte juhatusse valitakse tankist ehk isik, kes teeb formaalselt ettevõtte eest tehinguid. Tankistiks võib olla tegeliku kasusaaja sõber, tuttav või sugulane. Seega on tankistiks isik, kellega saab rahapesija hästi informatsiooni vahendada. Tankisti kaasamise eesmärgiks on varjata tegeliku kasusaaja andmeid. (Pacini, *et al.*, 2019, p. 252) Tegelik kasusaaja on isik, kes ettevõttevõtet tegelikult kontrollib ning tegevusest kasu saab (Pacini, *et al.*, 2019, p. 262).

Varifirmad on rahapesijatele hea võimalus peita tegelike kasusaajate andmeid. Üheks varifirmade ära kasutamise põhjuseks on asjaolu, et paljudes jurisdiktsioonides on keeruline tuvastada tegelikke kasusaajaid või vastavat nõuet puudutavad sätted puuduvad. Lisaks muudab mitmete varifirmade omamine eri riikides rahapesu tuvastamise keeruliseks, kuna

tegelikke kasusaajaid on keerulisem kindlaks teha. (Pacini, *et al.*, 2019, p. 263) Rahapesu tõkestamise toimkonna (edaspidi FATF) 24. soovitus järgi peab olema iga äriühingu kohta teada selle tegelik kasusaaja ning andmed peavad olema uuendatud (FATF, 2014, p. 16).

Seega on rahapesijate eesmärk varjata kriminaalsel teel saadud tulu kaasates variisikuid ning luues varifirmasid, et näidata ettevõtlustegevust ning seeläbi suunata raha äritegevusse ja seda seaduslikuna näidata. Seeläbi saavad rahapesijad varjata enda identiteeti ning tegutseda edasi, integreerides musta raha legaalsesse majandusse ning kasvatades enda tulu veelgi.

## **1.2 Rahapesu tõkestamine ja tuvastamine**

Rahapesu on oluline tõkestada rahvusvaheliselt. Ainuüksi riiklikul tasemel pole võimalik seda tõkestada. Euroopa Liit on rahapesu tõkestamise nõudeid seades võtnud arvesse Rahapesu tõkestamise toimkonna (edaspidi FATF) soovitusi. FATFi soovitusi on laiendatud alates 2012. aastast. (Anitei & Gardikiotis, 2015, p. 21) FATF loodi 1989. aastal G-7 riikide poolt ning selle moodustamisega loodi reeglid finantskuritegude ennetamiseks, tuntud kui FATFi 40 soovitust. Neid reegleid jälgivad kõik FATFi liikmesriigid. Esimene FATFi soovitus verisoon avaldati 1990. aastal, et võidelda narkokuritegude vastu, mis viisid rahapesuni. FATFi soovitusi on tunnustanud Rahvusvaheline Valuutafond ning Maailma Keskpank. (Meral, 2020, pp. 40-41)

Rahapesijad kasutavad rahapesuks mitmeid asutusi. Enim kaasatakse rahapesusse selliseid asutusi, kes tegelevad sularahaga: finantsasutusi. Kuna finantsasutuste järelevalve rahapesu osas on aja jooksul suurenenud, üritatakse kaasata mittefinantsasutusi. Sellisteks näideteks on ka valuutavahetuskohad ning kasiinod. (Ulst, 2003, lk 502) Põhjuseid, miks raamatupidajaid ning teisi professionaale rahapesus ära püütakse kasutada on mitmeid. Rahapesu on keeruline varjata ning seetõttu on vaja rahapesijatel kedagi, kes aitaks neil raha päritolu varjata. Teiseks on raamatupidajad just need, kes tegelevad finantstehingutega, näiteks on nad seotud tehingutega, mille käigus võõrandatakse vara või äriühinguid. Lisaks tuleneb eetikanõudest raamatupidajatele kohustus oma klientide majandustehingud õigesti kirjendada. Seega on raske teha kindlaks, et raamatupidaja pole oma kohustusi õigesti täitnud. Kuna raamatupidajatel on nõue hoida ärisaladust, siis saab rahapesijaks olev klient olla kindel, et tema tehtud tehinguid ei avalikustata. (He, 2006, p. 64)

Lisaks on raamatupidajatel finantsinstitutsioonide ees eelis, et nad näevad kõiki oma kliendi tehinguid. Finantsinstitutsioonid näevad aga osasid tehinguid, kuna rahapesijad varjavad tegelikku tehingut, tehes need väiksemateks ning suunates erinevatesse finantsinstitutsioonidesse. Seetõttu on finantsinstitutsioonidel keerulisem rahapesu tuvastada. (He, 2006, p. 65) Eeltoodust saab järeldada, et raamatupidajatel oleks hea võimalus tuvastada rahapesu teises ehk ladestamise etapis.

Siiski võib rahapesu tõkestamise nõuete järgimine raamatupidajate ja nende klientide vahel tekitada lahkkelisid. Kahtlase tehingu teate korral rikuks raamatupidaja oma kliendiga usaldussuhet. (He, 2006, p. 66) Rahapesu tõkestamiseks on seatud järgnevad hoolsuskohustuse meetmed (Tibar, 2018, lk 43; Rahapesu ja terrorismi rahastamise ja tõkestamise seadus, 2017, § 20):

1. Identifitseerimiskohustus (nii juriidilise kui füüsilise isiku samasuse tuvastamine, sealhulgas esindaja esindusõiguse tuvastamine, riikliku taustaga isiku kindlakstegemine).
2. Tegelik kasusaajate tuvastamine.
3. Ärisuhte mõistmine (tehingud, toimingud).
4. Ärisuhte seire.

Mittefinantsteenust pakkuvatele ettevõtjatele, sealhulgas raamatupidamisettevõtjatele tuleneb nõue teha kindlaks kliendi isikusamasus ning säilitada kogutud andmeid. Oluline on jälgida tehinguid sularaha, kinnisvara ostu-müügi ning aktsiate kohta. Lisaks tuleb raamatupidajatel tähelepanu pöörata ettevõttega seotud üldistele toimingutele, näiteks osakapitali sissemaksele ning toimingutele ettevõtte rahaga või üldistele asjaoludele, mis hõlmavad ettevõtete soetust või müüki. (Mugarura, 2014, p. 81)

Kuna eelpool käsitletud rahapesuskeemidest selgus, et rahapesijad soetavad variettevõtteid, on oluline jälgida, kas soetatud ettevõttega tehtud tehingud võivad kujutada riski, näiteks kas tegemist võib olla näilike tehingutega. Kuna rahapesijad ei tee rahapesutoiminguid ise, vaid kasutavad variisikuid, on oluline teha kindlaks isikusamasus ning need andmed koguda. Seega saab eelnevast tuletada, et põhjalik identifitseerimise protsess on vajalik, et maandada riski, et tegelik kasusaaja kasutab variisiku dokumente. Ettevõtete soetuse puhul tuleks tähelepanu pöörata, kas see on tegelikult eksisteeriv ettevõtte või on tegemist variettevõttega. Sularahaga

tehingute korral tuleks vaadata, millele kulutusi tehakse ning kas need kuluartiklid võivad kujutada riski. Kuna raamatupidajatele on hoolsuskohustuse meetmed seatud, tuleb neil seda rakendada ning ärisuhet ja tehinguid mõista.

Raamatupidamisteenust pakkuvatele ettevõtetele on seatud rahapesu tõkestamise nõuded, kuna neil on suutlikkus näha ettevõtete esmaseid tehinguid ning eristada kahtlase sisuga tehinguid paremini kui finantsinstitutsioonidel. Lisaks puudub raamatupidajatel kontrollorgan, nad on iseseisvad professionaalid. Seega on suurem tõenäosus, et raamatupidajaid kui professionaale püütakse rohkem rahapesusse kaasata. (He, 2006, p. 68) Seega peaksid raamatupidamisettevõtjad olema rahapesu tõkestamise kriteeriumitest hästi teadlikud ning tõdema, et raamatupidamisteenuse osutamisega võivad kaasneda ka riskid.

Üheks rahapesu toimeviimise viisiks on ka *offshore* firmade kasutamine. Need kujutavad välismaal asutatud ettevõtteid, mille eesmärgiks on ära kasutada välismaa seadusi, et makse vähem või üldse mitte maksta. Seega loovad rahapesijad tihtipeale madala maksumääraga piirkonda tütarettevõtte. Emaettevõtte teeb *offshore* piirkonnas asuva tütarettevõttega madala hinnaga tehinguid. Seejärel teeb tütarettevõtte need tehingud *offshore* piirkonnas kõrgema hinnaga ning tulu suureneb, kuid makse makstakse vähem. Hiljem suunatakse osa tütarettevõtte kasumist tagasi investeringuna enda riiki, näiteks laenuna. (George-Dorel, 2013, p. 277) Seega saab järeldada, et madala maksumääraga territooriumitel on tehingute üle väiksem kontroll ning seesuguseid ettevõtteid kasutatakse, et oma tulu suurendada ning saadud tulu kasumlikumalt edasi investeerida. Eelnevast tulenedes peaksid raamatupidamisettevõtjad jälgima, kas *offshore* piirkonda tehtud tehingud on õiglasel väärtuses ning kas need tehingud on seotud ettevõtlustegevusega. Siiski peaks selliseid tehinguid vaatama kooskõlas teiste asjaoludega, kuna *offshore* firma loomine pole keelatud (George-Dorel, 2013, p. 277).

Vastavalt Tulumaksuseadus § 22 lg 1 järgi maksustatakse madala maksumääraga territooriumil oleva juriidilise isiku tulu, kui see äriühing on Eesti residendi kontrolli all. Tulumaksuseadus § 22 lg 2 järgi on juriidiline isik residendist juriidilise kontrolli all, kui juriidilisel isikul on sellest äriühingust vähemalt 50% osalust. Tulumaksuseadus § 22 lg 3 järgi on residendi maksustatav tulu, kui § 22 lg 2 on täidetud ning kui isikul on vähemalt 10% otsene osalus või seotud isikute kaudu. (Tulumaksuseadus, 1991) Seega tuleks nõustamisteenust pakkuvatel raamatupidamisettevõtjatel jälgida, kas isik tulu deklareerib.

FATFi seatud nõuded on aluseks rahapesu tõkestamisele ning see on üle viidud riiklikku seadusesse. Seatud hoolsusmeetmed on oluline osa rahapesu tuvastamisest ja tõkestamisest. Kuna raamatupidamisettevõtjad näevad ettevõtte tehinguid ning kliendi üldiselt äritegevust, on autori hinnangul neil kui kohustatud isikutel üks olulisim roll kõikide kohustatud isikutes seas rahapesu tõkestamise nõudeid järgida. Kuna raamatupidajad vahendavad tehinguid ja haldavad ettevõtete pangakontot, näevad nad autori arvates kõiki tehinguid kogumis ning mõistavad ettevõtlastegevust paremini kui teised kohustatud isikud. Raamatupidajatel on seega teiste kohustatud isikute ees eelis tuvastada kahtlase sisuga tehinguid. Teisest küljest on sarnased võimalused ka audiitorettevõtjatel, kuid nemad ei näe kõiki ettevõtluses toimuvaid tehinguid, vaid kontrollides osa tehinguid. Lisaks on audiitorkontrolli ajal tehingud juba toimunud ja rahad liikunud ehk rahapesuteadet on hilja esitada ning selle aja jooksul on rahapesijad oma tegevusega jõudnud palju kaugemale.

### **1.3 Riskipõhine lähenemine**

Riskijuhtimisel ja riskihindamisel on rahapesu tõkestamisel oluline roll. Riskide juhtimisele on omane, et ei teata kõiki riskikomponente. Riskipõhiseks lähenemiseks on oluline, et oleks mudel, millest lähtuda. Mudel peab näitama, mis tõenäosus on vastavalt mingile tunnusele sattuda rahapesusse. Riskipõhise otsuse tegemiseks tuleb mõista, kuidas mingi tunnus mõjutaks riski realiseerumist. (Ross & Hannan, 2007, p. 110) Seega pole võimalik kõiki riske ette näha ning tuleb vastavalt mudelile jõuda järeldusele, millele tunnus viitab.

Rahapesu riskidest saab eristada kolme riski. Esimene neist on riski tõenäosus ehk vaadeldakse, kui suur sõltuvus on tunnuse ja vaadeldava sündmuse vahel, mida tuvastada soovitakse. Näiteks kui on teada, et rahapesu üheks tunnuseks on alati olnud identiteedivargus ning kui vaadeldav tunnus ehk identiteedivargus on toimunud, saab öelda, et on risk. Riskiks on ka olukord, kus rahapesust pole teada antud ning seetõttu on rahapesu edasi rahastatud, et aidata kaasa kuriteole. Kolmandaks riskiks saab pidada reguloorset riski. Selleks peetakse olukordi, kus ettevõttel on keeruline rahapesu riski tunnuseid hinnata. (Ross & Hannan, 2007, p. 110) Seega rahapesukahtluse korral ning sellest mitte teada andes riskitakse ka ise karistada saada.

Riskipõhine lähenemine keskendub rohkem suuremate riskide tuvastamisele, kui väiksemate riskide kindlakstegemisele. Selleks, et tõhusalt rahapesu vastu võidelda, on oluline riske õigesti hinnata ning riskide tuvastamiseks on vaja teada rahapesu riske. (de Koker, 2009, pp. 336-337) Sellest saab järeldada, et rahapesuskeeme on oluline ära tunda, et teada, mis meetmeid selle tõkestamiseks kasutusele võtta.

Esimene riskipõhine lähenemine tuleneb Euroopa Liidu kolmandast direktiivist põhimõtte tunne oma klienti järgi (CDD). Riskipõhise lähenemise järgi tuleb määrata kas risk on madal, keskmine või kõrgendatud. (van den Broek, 2011, p. 175) Riskianalüüsiks on vaja andmeid otsida ja analüüsida. Selleks tuleb kohaldada hoolsuskohustust ning tuleb hinnata tehingutega seotud riske. CDD järgi tuleb klient identifitseerida ning kindlaks teha tegelik kasusaaja. Lisaks tuleb arvestada tehingute olemust ja sagedust ning arvesse tuleb võtta geograafilisi riske. (Ai & Tang, 2011, p. 271) Riskid saab FATFI soovitude järgi jagada geograafiliseks riskiks, klientidega seonduvaks riskiks ning tehingutega seonduvateks riskideks (FATF, 2019, p. 22).

Geograafilise riski puhul tuleb jälgida tehinguid klientidega, kes on pärit rahvusvaheliste sanktsioonide all olevatest riikidest (Ai & Tang, 2011, p. 271). Kuna seesuguseid tehinguid tuleb jälgida, saab järeldada, et risk on kõrge ning seetõttu peaks rakendama kõrgendatud hoolsusmeetmeid. Klientidega seonduvate riskide puhul tuleb tähelepanu pöörata, kellega on tegu. Näiteks tuleb riikliku taustaga isikute suhtes rakendada kõrgendatud hoolsusmeetmeid, kuna riski peetakse kõrgemaks (Mitsilegas & Vavoula, 2016, pp. 278-279). Tehingutega seotud riskid võivad olla seotud raha kontodel liigutamise ja vahetamisega. Näiteks on ettevõtetel mitu pangakontot ning raha kantakse nende kontode vahelt, et hajutada rahapesuga seotud tegevusi. Üheks ohutunnuseks on ka asjaolu, kui tehinguid hakatakse tegema üle kehtestatud piirmäärade või kui neid tehinguid jaotatakse tahtlikult väiksemateks osadeks, et täissummat varjata. Ka liigne pangakontode vahetus on risk. (Ai & Tang, 2011, p. 273)

Tähelepanu tuleb pöörata ettevõtlustegevusele: kas see on harilik või ebaharilik. Ebahariliku tegevuse korral korduvad asjaolud pikema aja jooksul. Kui tekib põhjendatud rahapesu kahtlus, tuleb tehing peatada ja Rahapesu Andmebürood teavitada. Ebahariliku tegevuse korral võib isik olla avanud suurel hulgal kontosid ning limiite on hakatud suurendama või vahendeid paigutatakse erinevatele kontodele ja seejärel koondatakse ühele ning edastatakse välisriiki.



Lisaks on isiku äritegevus ebaharilik: isik vahetab tihti raamatupidamisteenuse pakkujat, algdokumentidelt nähtub väärkajastusi, soetatakse isikliku tarbimise objekte, mis pole seotud äritegevusega. (Politsei- ja Piirivalveamet, 2019, lk 15–18) Seega tuleb raamatupidajatel raha liikumisi jälgida ning kontrollida algdokumente.

Raamatupidamisettevõtjatel on kohustus täita hoolsuskohustust oma kliendi osas. See tähendab, et tuleb kindlaks teha tegelikud kasusaajad, hinnata tehinguid ning kõrgemate riskide korral peab rakendama tugevdatud hoolsuskohustuse meetmeid. (Gichuki, 2020) Hoolsuskohustuse täitmine on oluline, et riskipõhine lähenemine oleks edukas, ning et rahapesu ennetada (Šesterikov, 2016, lk 14). Hoolsuskohustusena peetakse CDD-d (*Customer due diligence*) ehk tunne oma klienti põhimõtet ning see seisneb oma tehingupartneri taustakontrollis (Nygen, 2018, p. 48). Kõrgendatud hoolsuskohustuse meetmed peavad olema rakendatud kõrge riskiga riikidest pärit klientidele, näiteks riikide suhtes, kus on leebed rahapesu tõkestamise nõuded (Nygen, 2018, p. 51). Seega mõeldakse hoolsuskohustusena rahapesu tõkestamise mõttes oma kliendiga seotud võimalike riskide kindakstegemist: kliendi ja tema ettevõtlustegevuse taustakontrolli.

Hoolsuskohutust kui üldist mõistet on käsitletud erinevalt. Tsiviilseadustiku üldosa seadus § 35 järgi tuleb juhtorgani liikmetele nõue seadusi järgida oodatava hoolega (Tsiviilseadustiku üldosa seadus, 2002). Äriseadustik § 187 järgi peab juhatuse liige ettevõtte ees oma kohustusi täitma korraliku ettevõtja hoolsusega (Äriseadustik, 1995). Seega tuleb ettevõtjatel täita kõiki seadusest tulenevaid nõudeid, sealhulgas Rahapesu ja terrorismi rahastamise tõkestamise seadust.

Raamatupidamisettevõtjatel on RahaPTS § 49 järgi nõue esitada rahapesu kahtluse korral Rahapesu Andmebüroole teade. Seda tuleb teha kahe ööpäeva jooksul alates rahapesu kahtluse tekkimisest. (Rahapesu- ja terrorismi rahastamise tõkestamise seadus, 2017) Kuna kohustatud isikutel on teate esitamise kohustus, tuleb neil tehinguid jälgida ning neid põhjalikult analüüsida (Nygen, 2018, p. 52). Rahapesu teateid on võimalik liigitada kahtlus- ja reegli põhiseks. Kahtluspõhise teate korral peab olema subjektiivne kahtlus, reegli põhine teatamise all mõeldakse sularaha teadet ehk on ette nähtud kindel summa, millest alates tuleb rahapesu teade esitada. (Tibar, 2018, lk 40)

Hoolsuskohustuse järgimiseks tuleneb rahapesu ja terrorismi rahastamise tõkestamise seaduse § 13 lg 1 järgi kohustatud isikutele nõue koostada riskide juhtimiseks riskihinnang. Riskihinnangu alusel tuleb välja selgitada riskid, mis kaasnevad klientide, geograafiliste piirkondade, toodete, teenuste või tehingutega. Lisaks rakendub nõue teha kindlaks klientidega suhtlemise kanalite riskid või toodete, teenuste või tehingute edastamiskanali risk. Vastavalt RahaPTS § 13 lg 5 järgi ei ole riskihinnangu koostamine kohustuslik, kui riiklikult on kohustatud isiku majandustegevuse riskid välja selgitatud ning kui kohustatud isik on esitanud järelevalveasutusele riskihinnangu koostamise vabastuse kohta taotluse, järgib riiklikku riskihinnangut ning teab oma valdkonna võimalikke riske. (Rahapesu- ja terrorismi rahastamise tõkestamise seadus, 2017) Seega on jäetud raamatupidamisettevõtjatele valikuvõimalus, kas riskihinnangut koostada. Teisest küljest võib valikuvõimalus kujutada riski, et ettevõtte siseselt ei olda kursis kõikide riskidega ning seetõttu ei pöörata riskidele niivõrd tähelepanu kui peaks.

RahaPTS § 17 lg 1 alusel tuleb kohustatud isiku juhatuse liikmel vastutada rahapesu tõkestamise nõuete järgitavuse eest. Juhul, kui kohustatud isikul on üle ühe juhatuse liikme, tuleb valida, kes neist vastutab. (Rahapesu- ja terrorismi rahastamise tõkestamise seadus, 2017) RahaPTS § 14 lg 1 alusel peab kohustatud isikutel olema koostatud protseduurireedid. Selleks tuleneb nõue koostada sisekontrollieeskiri, mis seab töötajate kontrollimise korra ning siseauditi korraldamise korra. Sisekontrollieeskirjaga on ära määratud, milline on protseduuri rakendamise kord. RahaPTS § 14 lg 5 järgi kaasneb siseauditikohustuslastel nõue kontrollida siseprotseduuri kinnipidamist. (Rahapesu- ja terrorismi rahastamise tõkestamise seadus, 2017) Efektiveks riskide hindamiseks on oluline, et siseaudit oleks põhjalik ning et töötajaid oleks rahapesu valdkonnas koolitatud (Nguyen, 2018, p. 51).

Lisaks riskipõhisele lähenemisele tuleb kaaluda ka täiendavate meetmete rakendamist, kuna ainuüksi sellest rahapesu tõkestamiseks ei piisa. Täiendavad meetmed võivad olla lisameetmed, mida kasutada, et teha kindlaks isiku raha päritolu või kasutatav vara. Näiteks on seesugused täiendavad meetmed seatud riikliku taustaga isikutele, kes on liikmesriigist või kolmandast riigis. (Šesterikov, 2016, lk 18-19) RahaPTS § 38 lg 1 järgi on täiendavad meetmed mõeldud, et kõrgema rahapesu riski korral riske maandada. Näiteks kontrollitakse täiendavaid dokumente, et välistada tehingute näilisus. (Rahapesu- ja terrorismi rahastamise tõkestamise

seadus, 2017) Seega on kohustatud isikutele ette nähtud pidev kliendi profiili jälgimine ning vajadusel tugevdatud meetmete kasutuselevõtt.

Riskipõhisel lähenemisel esineb ka probleeme. Näiteks on kohustatud isikutel suur otsustusõigus, missuguseid hoolsuskohustuse meetmeid rakendada (Šesterikov, 2016, lk 48). Sellest saab järeldada, et rahapesu tõkestamise meetmeid võib ettevõtjatel olla raske hinnata ja selle tõttu võib rahapesu tõkestamise efektiivsus langeda.

### **1.3.1 Tunne oma klienti põhimõte**

Tunne oma klienti põhimõte (KYC/CDD) on rahapesu tõkestamises ettenähtud protsess, et finantstehingutes tehingupoolt identifitseerida ja selle tõesust kinnitada. Kliendi tundmise protsess on ajamahukas ning tihtipeale tehakse seda käsitsi. (Marsh, 2018, p. 338) CDD eesmärgiks on teha kindlaks, kas klient on see, kes väidab end olevat (Demetriades, 2016, p. 80). See on üks hoolsuskohustuse meetmeid ning eelnevalt tulenedes oluline osa rahapesu riski tuvastamisel.

On raske tõestada, kas tegu on rahapesijaga, kuna rahapesijaid aitavad suure tõenäosusega professionaalid, kel on kogemused ja teadmised raha varjamise valdkonnas. Piisava tasu eest ollakse valmis rahapesijaid aitama. (Demetriades, 2016, p. 82) Kuna rahapesijaid ei ole kerge tuvastada, saab järeldada, et seda põhjalikumad hoolsusmeetmed peaksid rakenduma.

RahaPTS § 20 lg 1 p 1 järgi tuleb tehingupartneri isikusamasus tuvastada kasutades ka e-identimise vahendeid (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017). Seega on ettevõtjatel oluline leida sobiv identimisviis. Üheks kliendi identifitseerimise meetodiks on kasutada automatiseeritud võimalusi. See meetod võimaldab kokku hoida aega ning kliendi riskiprofiili lihtsamalt määrata. Näiteks on üha enam panku hakanud kasutama oma klientide identifitseerimisel tehisintellekti. (Marsh, 2018, p. 342) Kuna üha enam tehinguid tehakse elektrooniliselt, füüsiliselt teise poolega kohtumata, on vaja kindlustada, et tehingupartnerit saaks kontrollida. Distsantsilt on seda teha keeruline ning kliendi riskiprofiili on tarvis tuvastada arvuti vahendusel. (Angell & Demetis, 2006, p. 158) Seega on tehisintellektil kliendi

riskiprofiili tuvastamisel oluline roll, kuna kliente pole suurte vahemaade korral võimalik otsekontaktis tuvastada.

Aja jooksul on suurenenud ettevõtete arv, kes on hakanud pakkuma vastavat tarkvara, et kliendi riskiprofiili tuvastada (Angell & Demetis, 2006, p. 161). Seega on üks võimalus kliendi tausta kontrollida, kui teenust sisse osta. Tehisintellekti kasutamine ei anna kindlust, et rahapesu tuvastatakse. Rahapesu tuvastamiseks tehisintellekti abil peavad panuse andma ka inimesed. Rahapesu tuvastamine on süsteem, mis koosneb mitmetest etappidest ning tehisintellekti peab juhtima. Tehisintellekt suudab küll analüüsida seoseid, kuid ei suuda ette ennustada inimeste käitumist. (Angell & Demetis, 2006, p. 161) Seega on vaja inimesi, kes näevad tervikpilti ning teevad vastavaid järeldusi, milline on rahapesu riski. Teisest küljest on inimestel keeruline panna kokku tehisintellekti andmeid ning endale teadaolevaid andmeid ehk tõlgendada kõiki andmeid kogumis, kuna tehisintellekti kogutuid andmeid on palju (Angell ja Demetis, 2006, p. 161).

Rahapesu ja terrorismi rahastamise tõkestamise seaduse § 22 lg 1 järgi tuleb kohustatud isikul kindaks teha ning säilitada juriidilise isiku andmed: ärinimi, registrikood, juhatuse liikmete nimed ning volitused juriidilise isiku esindamiseks. Lisaks tuleb välja selgitada ka andmed juriidilise isiku sidevahendite kohta. Juriidiline isik peab olema kindel, et esitatud andmed on tõesed. Andmeid juriidilise isiku tuvastamiseks saab äriregistrist. Kui tegemist on välisriigi juriidilise isikuga, tuleb volitusi tõendada notariaalse tõendiga või sellega võrdsustatud dokumendiga (apostilliga). (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017)

Üheks võimaluseks klienti identifitseerida on kasutada IVC mudelit (*identification-verification-confirmation*). Identifitseerimine hõlmab isiku nime, sünnikuupäeva ning aadressi kindlakstegemist. Vastava informatsiooni kogumine sõltub sellest, kuidas isikuga suhelda: otsekontaktis või virtuaalselt. Seejuures on oluline tagada andmekaitse. (Shust & Dostov, 2020, pp. 875-876). Rahapesu ja terrorismi rahastamise tõkestamise seadus § 21 lg 1 järgi tuleb füüsilise isiku isikusamasuseks tuvastada tema nimi, isikukood (selle puudumisel elu- või asukoht ning sünniaeg), teave esindusõiguse kohta (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017). Kuna IVC meetod on füüsilise isiku kohta, saab järeldada, et seda meetodit on võimalik kasutada juhatuse liikme andmete kindlakstegemiseks.

Kontrollimise faasis kontrollitakse usaldusväärsest allikast, kas isiku esitatud andmed on tõesed. Kontrollimise vahenditeks sobivad ID-kaart või välismaalaste puhul pass. Interneti vahendusel isiku kindlakstegemisel saab kasutada avalikke, eraandmebaase või spetsiaalselt selleks mõeldud andmebaase. (Shust & Dostov, 2020, p. 876) Kinnitamise faasis maandatakse riske, et saada kinnitust, et isik on see, kes ta väidab end olevat. Võrreldes kontrollimise faasiga, mis tõendab, et isik on küll olemas, ei tõendata veel, et andmed isikule kuuluvad. Seega on kinnitamise etapi eesmärgiks kontrollida, et esitatud andmed kuuluvad tuvastatavale isikule. (Shust & Dostov, 2020, p. 876-877)

Kuna klientide identifitseerimise protsess on kulukas, ei saa see kindlustada, et kõiki kliente identifitseeritakse (de Koker, 2014, p. 292). Seega on see regulatoorne risk ehk kliendi tuvastamise protsess on keeruline ning tuvastamata jätmine kujutab omakorda riski. Sellega võidakse rikkuda hoolsuskohustuse meetmeid ning seetõttu ei tuvastata võimalikke riske. Hoolsusmeetmete kulukuse on oma magistritöös välja toonud ka Alina Sviridenko (Sviridenko, 2020, lk 50). Tema uuringust mitte finantsteenuse pakkujate seas selgus, et kallimad hoolsuskohustuse täitmise ressursiallikad on järgmised: ajakulu hoolsusmeetmete täitmisele, ajakulu seaduste jälgimisele, dokumentide koopiategemise ning säilitamise kulu, taustauuringute tegemisele kuluv andmebaaside tasu (Sviridenko, 2020, lk 50).

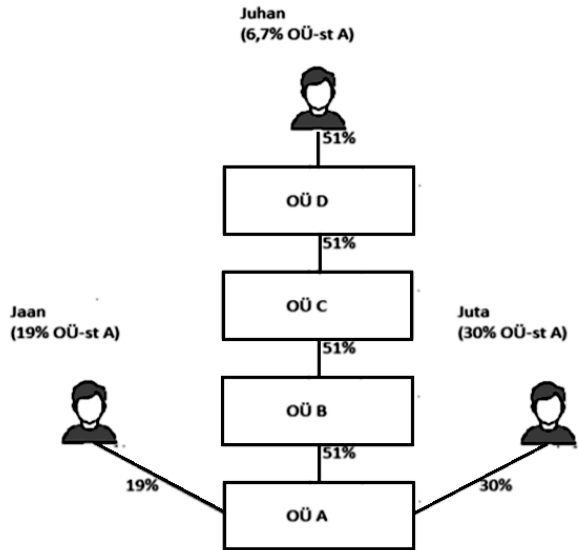
Tunne oma klienti põhimõtte tagamiseks on võimalus kasutada ka biomeetrilisi vahendeid. Selle meetodi kasutamine kinnitab, et isik on see, kes ta väidab end olevat. Biomeetriliseks vahendiks võib olla sõrmejäljetuvastus, digitaalfoto või hääletuvastus. (Shust & Dostov, 2020, p. 880) Üheks IVC uuemaks vahendiks on ka digitaalallkiri, kuid see nõuab kalleid ressursse (Shust & Dostov, 2020, pp. 880-881). Sellest järeldub, et vähem digitaalselt arenenud riikidest tehingupartnerid ei saaks lasta end tuvastada ning see muudaks kohustatud isikule tehingupartneri identifitseerimise keerulisemaks ja aeganõudvamaks.

Kuna rahapesu tõkestamisest tuleneb kohustatud isikutele nõue identifitseerida klient, tuleb valida selleks sobiv viis. Kliente saab tuvastada nii tehisintellekti kasutades kui ka käsitsi otsingumootorite abil. Võimalus on osta ka vastavat teenust sisse. Seega sõltub rahapesu tõkestamise tõhusus ka kohustatud isikute valitud meetodist.

### 1.3.2 Tegelik kasusaajate tuvastamine

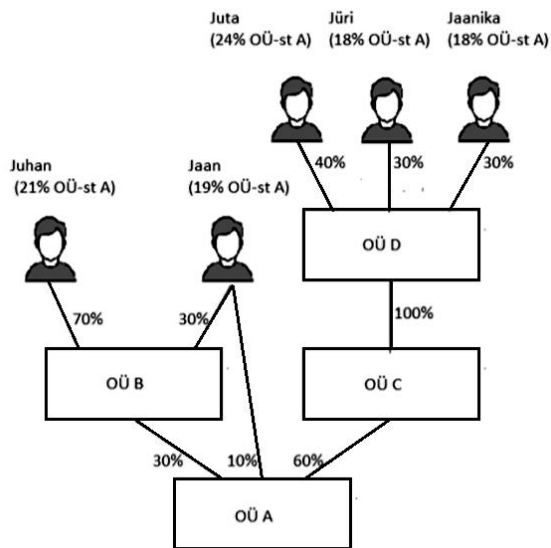
Rahapesu tõkestamise nõuetest tuleneb kohustus teha kindlaks tegelikud kasusaajad ning säilitada vastavaid andmeid. Lisaks peab olema veendunud, et ettevõtte on asutatud ning kindlaks tuleb teha ka ettevõtte aadress ning ettevõtte omanik. Tegelik kasusaaja on isik, kes äriühingut tegelikult kontrollib või selle äriühingu eest tehinguid teeb. (Mitsilegas & Vavoula, 2016, p. 278) Füüsilisest isikust kasusaajana käsitletakse isikut, kes kontrollib teise isiku toiminguid või tehinguid. Juriidilisest isikust kasusaajana käsitletakse isikut, kes omab ettevõtte üle kontrolli osaluse kaudu. Seaduse järgi peetakse konsolideerimisgrupis valitsetava mõjuna olukorda, kui osanikul on ettevõttest vähemalt 50 % osalust. Siiski ei tähenda valitsev mõju ainult juriidilises mõttes vara omamist, vaid valitseva mõjuna saab käsitleda ka väljapressimist või muud kuriteo vormi. (Tibar, 2018, lk 44)

Juriidilisi isikuid kasutatakse tihtipeale, et omandisuhet varjata (Tibar, 2018, lk 43). Äriühingu omamine võib olla otsene või kaudne (Tibar, 2018, lk 44) (vt joonis 2, lk 23). Rahapesu ja terrorismi rahastamise tõkestamise seadus § 9 lg 2 järgi on tegelikuks kasusaajaks isik, kes omab äriühingust vähemalt 25% osalust otseselt või kaudselt või kui need osalused kokku moodustavad vähemalt 25% (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017). RahaPTS § 9 lg 3 järgi on otsene osalus juhul, kui isikul on äriühingus osalus isiklikult. Kui isikul on osalus teise isiku või isikute ahela kaudu, on tegemist kaudse osalusega. (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017). Kui füüsilisest isikust kasusaajat pole võimalik kindlaks teha, peetakse kasusaajaks ettevõtte juhtorgani kõrgeimat liiget (Tibar, 2018, lk 45; Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017) (vt joonis 3, lk 23). Seega, kui tegelikul kasusaajal õnnestub varjata enda seost äriühinguga, peetakse tegelikuks kasusaajaks juhtorgani liiget (Tibar, 2018, lk 45). Sellest järeldub, et tegelikke kasusaajaid on keeruline tuvastada ning rahapesijate hea planeerimise korral võidakse vastutusele võtta tankist ehk isik, kes on ettevõtte etteotsa formaalselt seatud, et ise vastutusest pääseda.



Joonis 2. Otsene ja kaudne osalus (Rahandusministeerium, 2020)

Selles näites on otseseks tegelikuks kasusaajaks Juta, kuna tema osalus on üle 25% ettevõttest OÜ A. Tegelikuks kasusaajaks on lisaks Jutale ka Juhan, kuna ta kontrollib Äriühingut A ettevõtete D, C ning B kaudu ehk tal on neis ettevõtetes enamusosalus. (Rahandusministeerium, 2020, lk 2)



Joonis 3. Tegelik kasusaaja kui juhtorgani liige (Rahandusministeerium, 2020)

Sel joonisel on OÜ A tegelikeks kasusaajateks OÜ D juhtorgani liikmed, sest OÜ A-d kontrollib 60% osalusega OÜ C, mida omakorda juhib OÜ D. Kuna OÜ-l D puudub vähemalt

25% osalusega osanik, loetakse tegelikeks kasusaajateks kõik juhtorgani liikmed. (Rahandusministeerium, 2020, lk 2) Eelnevatest joonistest nähtub, et tegeliku kasusaaja tuvastamiseks tuleb teada ettevõtte omandijaotuse struktuuri. Üheks rahapesu tõkestamise tõhustamise meetodiks on ka avalik tegelike kasusaajate registri nõue (Gilmour, P. M., 2020, p. 719). RahaPTS § 76 lg 1 järgi tuleb eraõiguslikel juriidilistel isikutel esitada Äriregistrisse tegelike kasusaajate andmed (Rahapesu- ja terrorismi rahastamise ja tõkestamise seadus, 2017). Kuna teiste riikide avalikele andmebaasidele on keeruline ligi pääseda, võib osutada mitteresidentidest ettevõtete tegelike kasusaajate tuvastamine keeruliseks (Subashi, 2014). Sellest järeldub, et kõiki kasusaajaid pole võimalik efektiivselt tuvastada ning see on ajamahukas ning kulukas.

Tegelikke kasusaajaid on keeruline tuvastada ka *offshore* firmade korral, kui on välja antud esitajaaktsiad (*bearer shares*). Nende järgi pole võimalik teha kindlaks, kes on aktsia omanik, mis tähendab, et ettevõtte omanike kohta puudub info. Seega kasutatakse esitajaaktsiad, et tegelikke kasusaajaid varjata. (Subashi, 2014) Esitajaaktsiad annavad osanikele õiguse ettevõtet omada tegelikke omanikke registreerimata. Selliseid ettevõtteid võib osades riikides, näiteks USAs registreerida, kuid paljudes riikides on nende kasutamine keelatud. (Pacini, *et al.*, 2019, p. 251) Seega takistab varifirmade tegelike kasusaajate andmete puudumine tegelike kasusaajate tuvastamist (Pacini, *et al.*, 2019, p. 252). Tegelikke kasusaajaid on keeruline tuvastada, kuna raha kantakse erinevate ettevõtete vahelt ning alguslülil on keeruline kindlaks teha. Moodustatakse pikki tehingute ahelaid kasutades variisikuid. (Pacini, *et al.*, 2019, pp. 259-260) Seega on tegelike kasusaajate tuvastamisel oluline jälgida, mis piirkonnast on isik pärit ning oluline on hinnata, kellega on tegu. Riikliku taustaga isikute korral rakenduvad kõrgendatud hooldusmeetmed. Riiklike taustaga isikute kohta saab andmeid otsida erinevatest andmebaasidest, näiteks Worldcheckist või Factivast. Siiski on need andmebaasid kallid ning neid kasutavad peamiselt pangad. (Subashi, 2014) Sellest järeldub, et väiksematele ettevõtetele on see kulukas ning neil oleks tarvis täiendavaid ressursse, et andmebaaside kasutusõigust osta. Tegeliku kasusaaja tuvastamise hooldusmeetme kindlakstegemiseks on võimalik kasutada nii siseriiklikke kui välismaised registreid. Kuna välismaistele registritele on keerulisem ligi pääseda, võib selle hoolduskohustuse täitmise viisi olla raskem täita. Lisaks ei kindlusta ametlikult registreeritud tegelik kasusaaja, et isik on just see, kes ettevõtlusest tegelikult kasu saab ja seda kontrollib.



## **2. RAAMATUPIDAMISETTEVÕTJATE HOOLSUSMEETMED**

### **2.1 Uurimismeetodi ja uurimisandmete kirjeldus**

Lõputöö eesmärk on välja selgitada, mis viise kasutades täidavad raamatupidamisettevõtjad rahapesu tõkestamise nõuetest tulenevalt hoolsuskohustust. See tähendab, kuidas raamatupidamisettevõtjad täidavad rahapesu tõkestamise nõudeid hoolsusmeetmete järgi riskipõhisel lähenemisel ning mis meetmete rakendamisel on suurimad puudujäägid ehk milliste meetmete täitmata jätmise osas võivad esineda riskid. Eesmärgi täitmiseks kasutab autor kombineeritud uurimismeetodit.

Kvantitatiivse analüüsi puhul kasutab autor kirjeldavat statistikat ehk kogutud andmed esitatakse visuaalselt diagrammidena (Õunapuu, 2014, lk 184; Bryman, 2012, p. 337). Andmekogumismeetodina kasutatakse ankeetküsitlust, kus esitatakse avatud kui ka suletud küsimusi. Avatud küsimuste puhul kasutatakse andmeanalüüsimeetodina kvalitatiivset sisuanalüüsi ehk sarnase mõttega tekst koondatakse kategooriatesse (Laherand, 2008, lk 290; Saldana, 2009, pp. 8–11). Suletud küsimuste puhul antakse ette valikuvariandid, kuid avatud küsimuste korral valikuvariante ette pole nähtud, mis annab küsitletavatele võimaluse ise vastata, ilma et teda suunataks. Autor koostas küsimustiku ise ning küsimustikule vastamine oli anonüümne. Suletud küsimustikus kasutatakse nominaal- ja binaarskaalat, reitingu- ja järjestusskaalat. Sellise küsimustiku plussiks on võimalus anda vastajale ette kindlad valikuvõimalused (Õunapuu, 2014, lk 162). Tänu sellele on vastajal mugavam küsimustikule ka vastata. Andmeid analüüsitakse sagedusdiagrammide põhjal. See tähendab, et leitakse proportsioon vastavalt grupi vastanute arvule kogu grupi vastajatest (Õunapuu, 2014, lk 186 – 188).

Teisest küljest peab suletud küsimustiku koostamisel mõtlema kõik valikuvariandid läbi. Avatud küsimuste analüüsimine võtab kauem aega ning tekst tuleb süstematiseerida (Õunapuu, 2014, lk 162). Siiski annavad avatud küsimused edasi rohkem infot ja selgitavad suletud küsimusi. Seega on võimalik küsida vastajate arvamust ja saada teada valitud vastuste põhjuseid: sellest lähtuvalt saab infot paremini analüüsida.

Küsitluse valimiks valis autor raamatupidamisettevõtjad. Kuna raamatupidamisettevõtjatel on esmane võimalus märgata rahapesu, on oluline teada, mil määral panustavad nad rahapesu tõkestamise ning mis hoolsusmeetmete täitmisel esinevad suurimad puudujäägid. Küsimustik toob välja hoolsusmeetmete rakendamise viisid ja annab ülevaate, kuidas raamatupidamisettevõtjad hoolsuskohustust täidavad. See on vajalik selgitamiseks välja, kuidas panustavad rahapesu tõkestamise raamatupidamisettevõtjad ning missuguseid meetmeid täidetakse vähim. Kuna kasumit teenivaid ettevõtjaid on Äriregistris palju, valis autor osaiühingute ja füüsilisest isikust ettevõtjate seast igast maakonnast esimesed 70% nimekirjast. Autor otsis kehtivaid andmeid registrisse kantud ettevõtete kohta vastavalt äriühingu vormile ning maakonnale. Seega kasutab autor süstemaatilist juhuslikku kihtvalimit. Kihtvalimi korral jaotatakse üldkogum tunnuste järgi alampopulatsioonideks (Õunapuu, 2014, lk 141). Alampopulatsiooni tunnusteks määras autor äriühingu vormi ning maakonnad. Andmete saamiseks kogus autor Äriregistrist meiliaadressid perioodil 10.02.2021-02.03.2021.

Autor esitas raamatupidamisettevõtjatele 27 küsimust (vt lisa 1) ning küsimustik väljastati adreessaatidele perioodil 08.02.2021-11.02.2021. Küsitlusele oli võimalik vastata perioodil 08.03.2021-26.03.2021. Küsimustik hõlmab hoolsusmeetmete täitmise viiside kohta küsimusi. Selle eesmärgiks on teha järeldusi, mis meetmete täitmine on efektiivne ning mida täidetakse vähim, ühtlasi on jäetud vastajatele ka probleemkohtade juurde avatud küsimus. Järjestusskaalal on võimalik hinnata meetmete täitmise keerukust ja sellest saab teha vastuste kohta vastavaid järeldusi. Küsimusi esitati füüsilise ja juriidilise isiku andmete kindlakstegemise kohta, tehingupartneri taustakontrolli, tegelike kasusaajate tuvastamise kohta, riikliku taustaga isikute kindlakstegemise kohta ning tehingute jälgimise kohta, riskide kindlakstegemise kohta. Sellest lähtuvalt analüüsib autor hoolsusmeetmete järgimist ja vastavalt teoreetilisele osale leiab vajadusel põhjused meetmete mittetäitmise kohta, et välja pakkuda lahendusi.

Raamatupidamisettevõtjad kuuluvad EMTAK koodi number 69202 alla. Vastava koodi all on nimetatud „Raamatupidamine, maksualane nõustamine“, mis jaguneb järgmiselt (Registrite ja Infosüsteemide Keskus, 2008):

- „Raamatupidamine;
- Era- ja juriidiliste isikute tuludeklaratsiooni koostamine;

- Maksualane nõustamine ja klientide esindamine maksuorganites;
- Maksujõuetuse ning pankrotivara haldamise teenus.“

Äriregistris on 10.02.2021 seisuga kokku 7711 ettevõtet. Neist 7668 on aktsiaseltsid, täisühingud, füüsilisest isikust ettevõtjad, usaldusühingud, osäühingud, tulundusühistud (vt lisa 2). Kuna osäühingud ja füüsilisest isikust ettevõtjad on esindatud kõigis 15. maakonnas, valis autor just need äriühingud. Äriregistrist on võimalik saada vaid 1000 ettevõtte andmed, seega otsustas autor koguda andmed Äriregistrist ise. Nimekirjad on Äriregistris esitatud tähestikulises järjekorras. Kokku saadeti küsimustik ligikaudu 5249 ettevõttele Google Forms keskkonna kaudu. Autor kogus meiliaadresse 4 h kuupäeval 10.02.2021, 7 h kuupäeval 19.02, 5 h kuupäeval 20.02, 5 h kuupäeval 02.03. Lisas 2 on esitatud maakondade lõikes ettevõtete arv äriühingute järgi, kes tegelevad raamatupidamise ja maksunõustamisega (vt lisa 2). Küsimustik saadeti esimesele 70 protsendile osäühingu ja füüsilisest isikust ettevõtjate nimekirjadest (vt tabel 1).

Tabel 1. Moodustatud valim (autori koostatud)

Maakond	OÜ	FIE	Kokku
Harju	2976	122	3098
Hiiu	34	4	38
Ida-Viru	165	32	197
Jõgeva	53	15	68
Järva	70	11	81
Lääne	78	9	87
Lääne-Viru	157	23	180
Põlva	55	9	64
Pärnu	281	34	315
Rapla	127	19	146
Saare	111	16	127
Tartu	554	37	591
Valga	57	8	65
Viljandi	100	18	118
Võru	64	11	75
<b>Kokku</b>	<b>4882</b>	<b>367</b>	<b>5250</b>

Eelnevalt saadeti küsimustik testimiseks kaheksale raamatupidamisettevõtjale, kellest 50% vastas. Tänu sellele sai autor tagasisidet ning küsimustikku täiendada enne selle täielikku väljasaatmist.

## **2.2 Raamatupidamisettevõtjate hoolsuskohustuse täitmine**

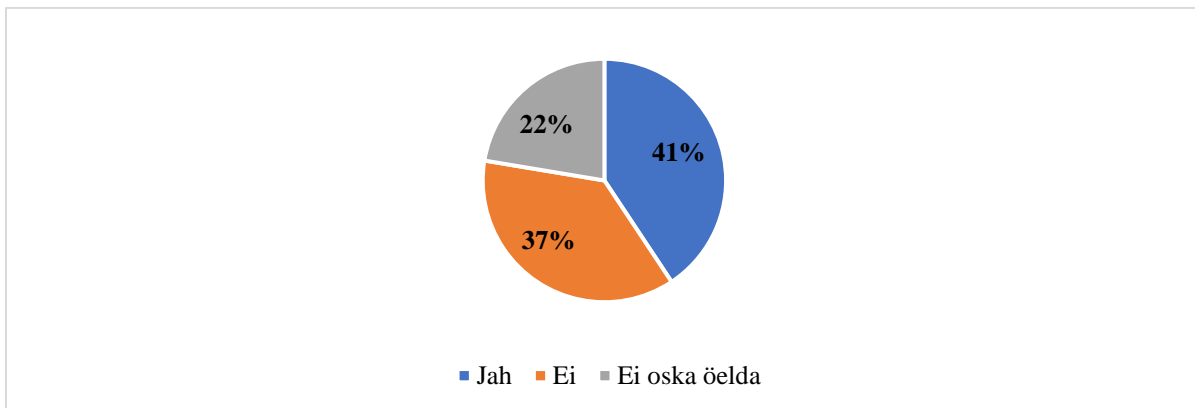
Vastavalt teoreetilisele käsitlusele on võimalikud taustakontrolli allikad toodud lisasse 3. Järgnevalt teostatakse küsitluse analüüs. Küsitlusele vastas kokku 295 ettevõtjat, neist 271 olid osäühingud ning 24 füüsilisest isikust ettevõtjad. Küsitluse tulemused on usaldusväärsed, sest, usaldusnivool 95% veapiiriga 6% on vajalik valim 254. Autorile vastas küsimustikule 295 ettevõtjat, millest tulenevalt on see tõlgendatav valitud grupi kohta. Esimene küsimus oli ettevõtjate tegutsemisaastate kohta. Enim ehk 37% vastas raamatupidamisettevõtjaid tegutsemisaastatega üle 15 aasta, seejärel 24% tegutsemisaastaga 6-10, 21% tegutsemisaastaga 0-5 ning vähim (18%) vastas ettevõtteid tegutsemisaastatega 11-15.

Teine küsimus oli ettevõtlusvormi kohta. 92% vastajatest olid osäühingud, 8% füüsilisest isikust ettevõtjad. Kuna kokku saadeti küsitlus 4882 osäühingule, siis vastanute osakaal oli osäühingutest 5,6%. 367 füüsilisest isikust ettevõtjatest vastas 6,5%. Kolmas küsimus esitati ettevõtte suuruse kohta. Enim ehk 70% vastustest laekus mikroettevõtjatelt, seejärel 28% väikeettevõtjatelt ning 2% keskmise suurusega ettevõtjatelt. Üks vastus laekus suurettevõtjalt. Seega olid esindatud kõik ettevõtjate liigid. Neljas küsimus esitati selle kohta, kas raamatupidamine on põhi- või kõrvaltegevusalaks. Enamik ehk 77% vastajaid tegeleb raamatupidamisega põhitegevusalana. Seega peaksid nad seatud hoolsusmeetmeid järgima põhjalikult. 23% jaoks on raamatupidamine lisategevusala, mis tähendab, et esmaseks tegevusalaks on muu ettevõtlusvorm.

Viienda küsimusena tuli ettevõtjatel valida, mis maakonnas nad registreeritud on. Enim vastanutest olid Harjumaalt (49%), seejärel Tartumaalt (12%), Pärnumaalt (5%), Ida-Virumaalt, Lääne-Virumaalt, Võrumaalt, Viljandimaalt ning Põlvamaalt igast maakonnast 4%, Järvamaalt 3%, Raplamaalt ning Jõgevamaalt kummastki 2%. Saaremaalt ja Läänemaalt vastas mõlemast maakonnast 2%. Vähim vastuseid laekus Hiiumaalt (2%) ning Valgamaalt (1%).

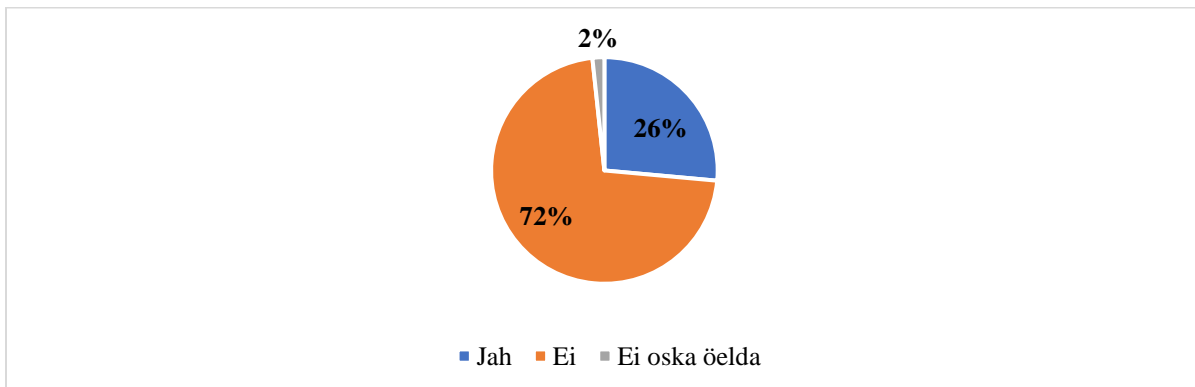
Kuuenda küsimusena soovis autor teada, kas vastajad peavad end rahapesu ja terrorismi rahastamise tõkestamise seaduse alusel kohustatud isikuks. 41% vastanutest pidas end

kohustatud isikuks, 37% vastajatest ei pidanud ning 22% ei osanud öelda (vt joonis 4). Sellest järeldub, et enamik vastajatest olid ebakindlad, kas nad kuuluvad kohustatud isikute sekka, või arvasid, et ei kuulu.



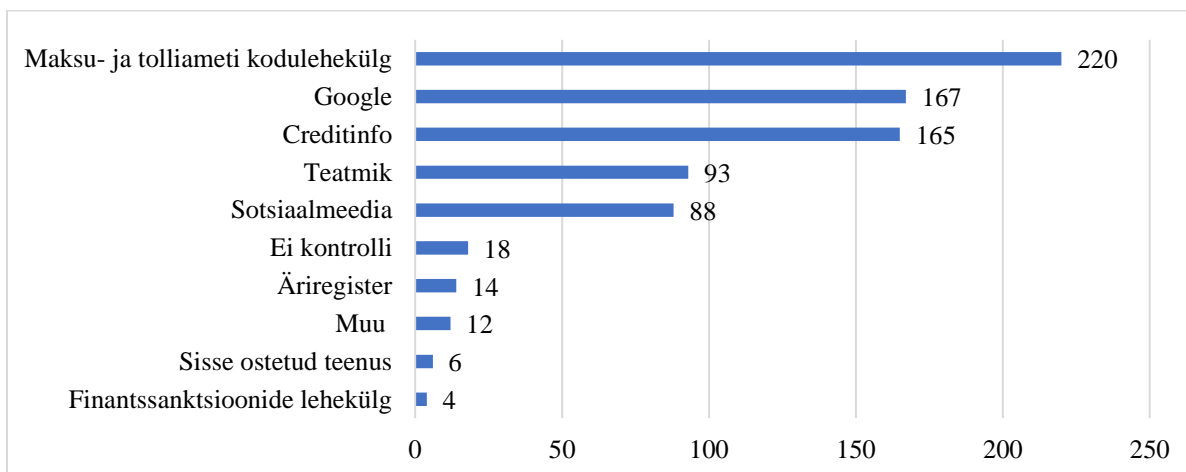
Joonis 4. Kohustatud isikute osakaal (autori koostatud)

Seitsmenda küsimusega küsiti, kas ettevõttes on koostatud sisekontrollieeskiri, millega rahapesu reguleeritud on. 72% vastajatest see puudus. 26% ettevõtjatest oli see ettevõttes koostatud ning 2% ei olnud teadlikud, kas ettevõttes on vastav eeskiri (vt joonis 5). Seega ühtib tulemus varasema lõputööga „Audiitorid ja raamatupidamisteenuse pakkujad rahapesu tõkestamise süsteemis Eesti näitel“, kus leiti, et sisekontrollieeskiri puudub 82% vastajatest (Pärnpuu, 2014). Sellest järeldub, et see puudujääk esineb jätkuvalt, ettevõtjad pole sisekontrollieeskirjaga rahapesu tõkestamise reegleid piisavalt sätestanud. Seega tuleb ettevõtjaid selles valdkonnas nõustada. Kui ettevõtte rahapesu reguleeriv siseprotseduur on vähe reguleeritud, ei tea töötajad, kuidas rahapesu korral peaks toimima ning see vähendab rahapesu tõkestamise efektiivsust.



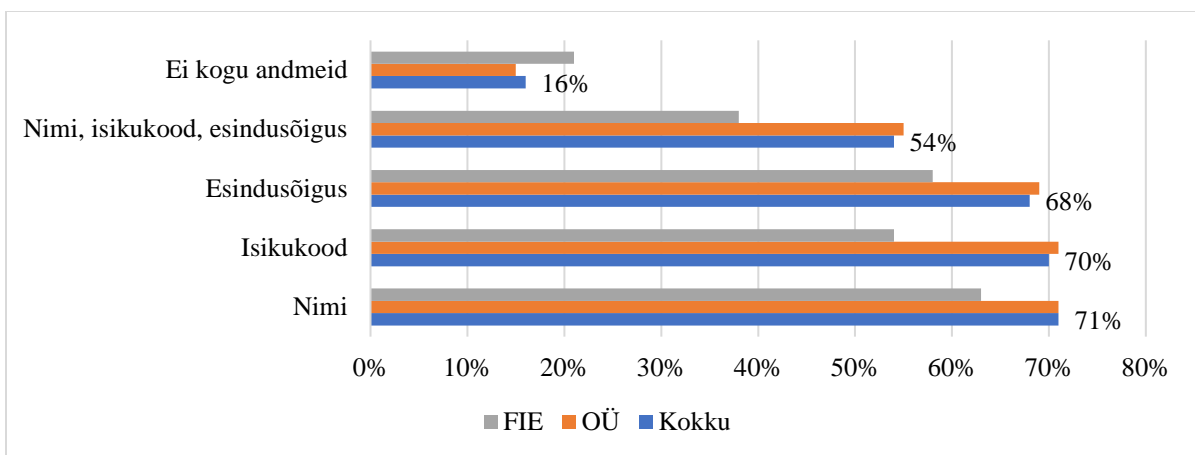
Joonis 5. Sisekontrollieeskirja olemasolu (autori koostatud)

Kaheksanda küsimusena esitati, mis allikaid kasutades kontrollivad kohustatud isikud oma tehingupartneri tausta. Kuna valida sai mitu vastusevarianti, on vastuste koondsumma üle saja. Enim kasutakse tasutakontrolliks Maksu- ja Tolliameti kodulehekülge (75%). Google otsingumootorit (57%), seejärel Krediidinfot (56%) ning Teatmikku (32%). Sotsiaalmeediat kasutab taustakontrolliks 30% (vt joonis 6). 6% vastanutest ei kontrolli oma tehingupartneri tausta. Äriregistrit kasutab tehingupartneri taustakontrolliks 5% vastajatest. Vastusevarianti „Muu“ vastas 4% ning selle hulgas esinesid järgnevad vastsed: „Muud andmebaasid (näiteks Bisnode, Infopank), otsene vestlus kliendiga, Rahapesu Andmebüroo, tuttavad“. Sisse ostetud teenust kasutab vaid 2% vastanutest. Finantssanktsioonide lehekülgi kasutab taustakontrolliks vaid 3% vastanutest (välismaale teenusepakkujate seas). Eelnevast järeldub, et enamjaolt kasutavad ettevõtted tasuta andmebaase.



Joonis 6. Tehingupartneri taustakontrolli allikad (autori koostatud)

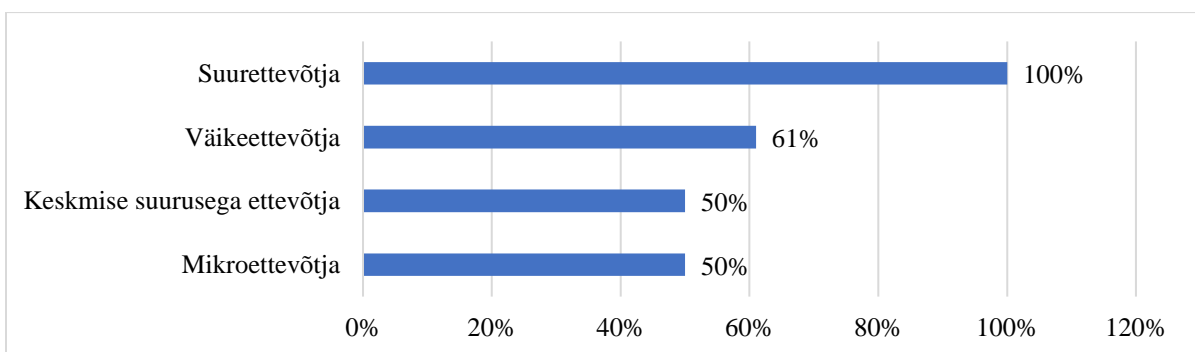
Usaldusväärseteks allikateks peetakse Maksu-ja Tolliameti kodulehekülge (76%), seejärel Krediidinfot (49%), Teatmikku (23%), Google (16%), Ettevõtte kodulehekülge (12%), Sisse ostetud teenust, millel on spetsiaalne tarkvara (12%), Sotsiaalmeediat (8%). Üheteistkümnenda küsimusena uuriti, mis andmeid kogutakse ärisuhet luues füüsilise isiku isikusamasuse tuvastamiseks (vt joonis 7, lk 31). Enim kogutakse füüsilise isiku nime (71%). OÜ-dest kogusid nime 71% vastanutest, FIE-de seas oli vastav näitaja 63%. Isikukoodi koguti kokku 70% juhtudel, sealhulgas kogusid OÜ-dest 71%, FIE-dest aga 54% vastanutest. Esindusõigust kogus kokku 68% vastajatest, sealhulgas OÜ-dest 69% ning FIE-dest 58%. Üldse ei kogunud vastavaid andmeid 16% vastajatest, OÜ-dest 15% ning FIE-dest 21%. Sellest järeldub, et olulisimaks peeti nime ning isikukoodi kogumist.



Joonis 7. Füüsilise isiku isikusamasuse tuvastamisel kogutavad andmed (autori koostatud)

Kui võrrelda osahinguid ja füüsilisest isikust ettevõtjaid, siis osahingud koguvad vastavaid andmeid rohkem. Nii nime, isikukoodi kui ka esindusõigust kogub 54% vastajatest. Kuna nime ja isikukoodi kogutakse ligikaudu 70% vastajatest, siis on selle meetme täitmise pigem hea. Maakondade lõikes selgus, et enim kogutakse nii nime, isikukoodi kui ka esindusõigust Hiiumaal, seejärel Järvemaal ning Raplemaal (vt lisa 4, joonis 1). Vähim kogutakse kõiki neid andmeid Jõgevamaal, Pärnumaal ning Viljandimaal. Üldkokkuvõttes saab öelda, et enim kogutakse neid andmeid Põhja- ning Kagu-Eestis, vähim Kesk-Eestis.

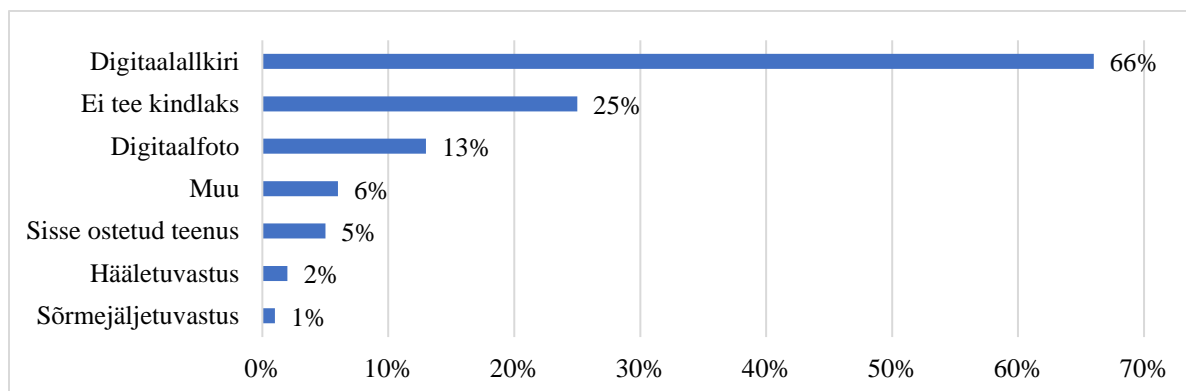
Kui võrrelda andmeid ettevõtete suuruse järgi, siis võrreldes mikroettevõtjatega koguvad väikeettevõtjad ja suurettevõtjad neid andmeid hoolikamalt (vt joonis 8). Sellest saab järeldada, et kuna nendes ettevõtetes on suuremad käibed, on neil ka rohkem ressursse, et vastavaid andmeid koguda.



Joonis 8. Nime, isikukoodi ja esindusõiguse kogumine ettevõtte suuruse järgi (autori koostatud)

Kaheteistkümnenda küsimusena esitati küsimus, mis allikast kontrollitakse füüsilise isiku isikusamase tuvastamiseks esitatud andmeid. Valida sai mitme vastusevariandi vahel ning seetõttu ületab koondsumma 100%. 17% vastajatest ei kontrolli isikusamasuse tuvastamiseks esitatud andmeid. Siiski kontrollib esitatud andmete tõlevastavust isikut tõendava dokumendi järgi 81% vastanutest, välismaal välja antud dokumendi järgi kontrollib 27% (välismaale teenusepakkujate seas). Vastusevariandi „Muu“ all toodi välja, et tehingupartneri esitatud andmeid kontrollitakse Äriregistri abil. Seega järgitakse kontrollimise faasis esitatud andmeid küllaltki põhjalikult. See tähendab, et tehakse kindlaks, kas esitatud andmete järgi isik eksisteerib. Veel oli välja toodud, et paar üksikut isikut küsib ka tehingupartneri pangakonto väljavõtet või sideteenuste arveid. Maakondade lõikes selgus, et enim ei kontrollita isikusamasuse tuvastamiseks esitatud andmete tõlevastavust Läänemaal, Raplemaal ning Valgemaal (vt lisa 4, joonis 2).

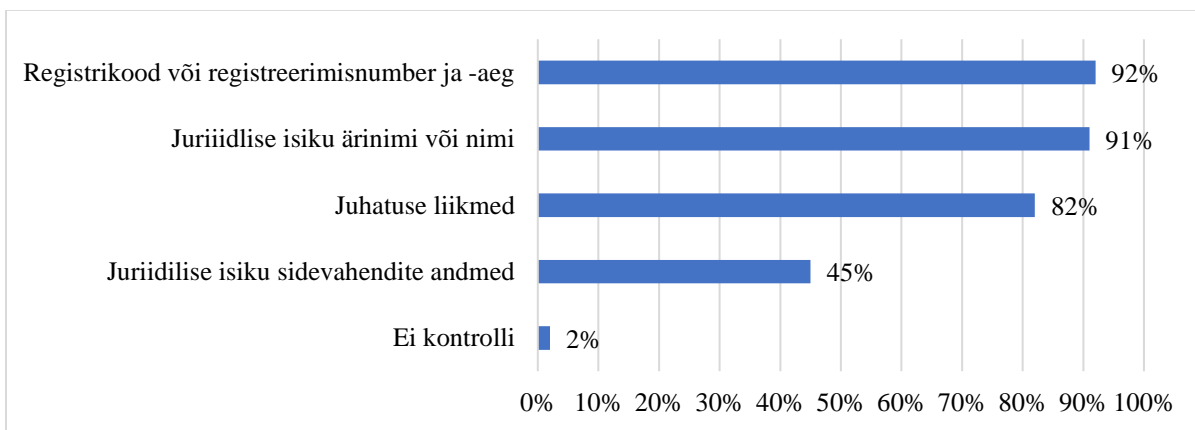
Kolmeteistkümnenda küsimusena esitati, kuidas tehakse kindlaks kas ärisuhet luues on isik, see, kes väidab end olevat. Sellest saab järeldada, kui põhjalikult täidetakse IVC mudeli järgi kinnitamise faasi. Küsimusele oli võimalik vastata mitme valikuna ning seetõttu ületab koondsumma 100%. Enim levinud kliendi kindlakstegemise meetod on digitaalallkiri, seda kasutab 66% vastajatest, seejärel digitaalfotot 13% vastajatest (vt joonis 9). Tehingupartneri taustakontrolli teenust ostab sisse 5% vastajatest. Vähim kasutatakse hääletuvastust (2%) ja sõrmejäljetuvastust (1%). Vastusevariandi „Muu“ all vastati enim otsekontakti või videosilla vahendusel tuvastamist (6%). Siiski ei kontrolli 25% vastajatest, kas nendega suhtlev isik on see, kes väidab end olevat. Sellest järeldub, et sisse ostetakse teenust küllaltki vähe, küll aga kasutatakse e-identimise võimalusi.



Joonis 9. Tegelik isiku kindlakstegemine (autori koostatud)



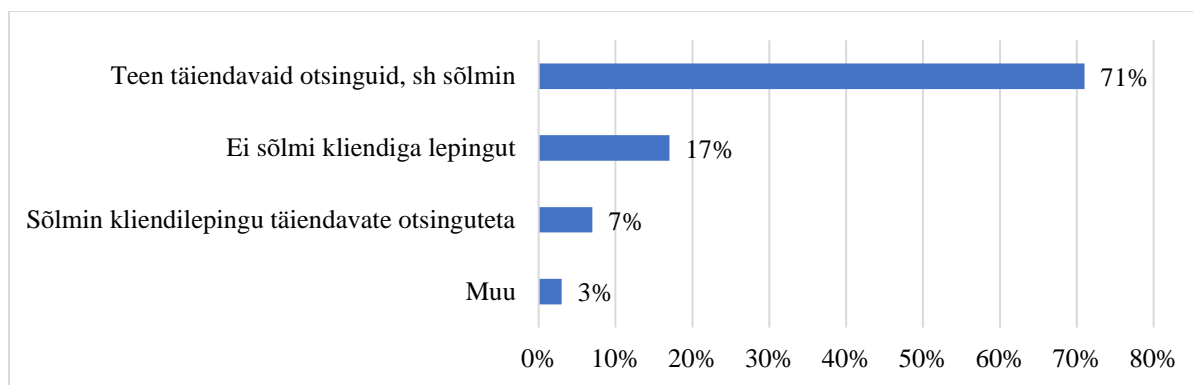
Maakondade lõikes selgus, et enim ei tehta isikut kindlaks Viljandimaal, Läänemaal, Hiiumaal, Ida-Virumaal ning Pärnumaal. Enim tehakse aga kindlaks Harjumaal, Võrumaal, Põlvamaal ning Saaremaal (vt lisa 4, joonis 3). Viieteistkümnenda küsimusena esitati, milliseid juriidilise isiku andmete tõlevastavust kontrollitakse. Selgus, et enim (92%) kontrollitakse registrikoodi ning juriidilise isiku ärinime tõlevastavust (vt joonis 10). Vähim (45%) kontrollitakse juriidilise isiku sidevahendite andmeid. Juhatusel liikmeid ning nende volituste tõlevastavust kontrollitakse 82% juhtudest. Ainult 2% vastajatest ei kontrolli vastavaid andmeid. Seega on suurim puudujääk juriidiliste isikute sidevahendite kontrollimisel.



Joonis 10. Juriidiliste isikute andmete kontrollimine (autori koostatud)

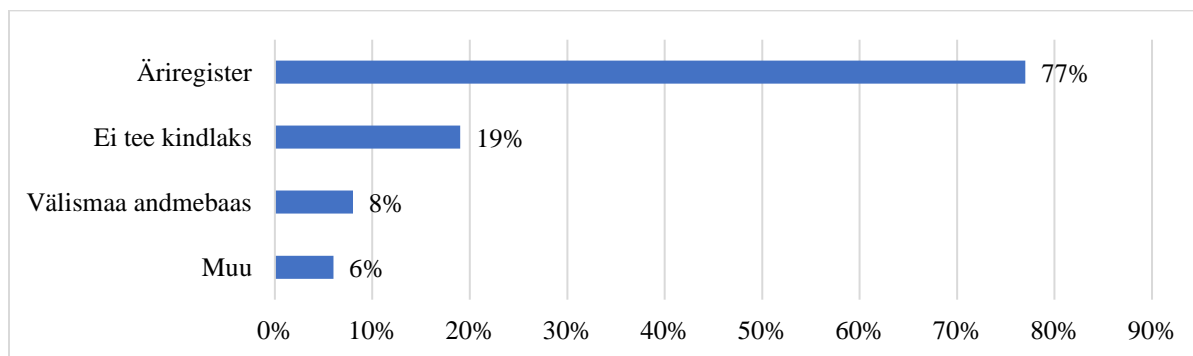
Järgmise küsimusena soovis autor 1-10 pallisüsteemis teada, kui keeruline on eelmises küsimuses esitatud andmete tõlevastavust kontrollida, sealhulgas 1-pole üldse keeruline, 10-väga keeruline. Vastajate keskmine väärtus oli 3,6, millest saab järeldada, et neid andmeid on kerge kontrollida.

Neljateistkümnenda uuriti, kuidas toimitakse, kui kliendi kohta leidub vähe infot. 71% vastajatest teeb täiendavad otsinguid, et kliendilepingut sõlmida, 17% vastajatest aga ei sõlmi kliendilepingut ning 7% vastajatest sõlmivad kliendilepingu hoolimata infopuudusest (vt joonis 11, lk 34). Vastusevariandi „Sõlmin kliendilepingu täiendavate otsinguteta“ all toodi välja, et sõlmitakse tingimuslik leping või leping sõlmitakse ainult ettemakse tingimusel. Vastusevariandi „Muu“ all märgiti, et toimitakse vastavalt tehingu suurusele ja võimalikule riskile või sellist olukorda pole ette tulnud.



Joonis 11. Täiendav kliendi taustakontroll vähese info puudumisel (autori koostatud)

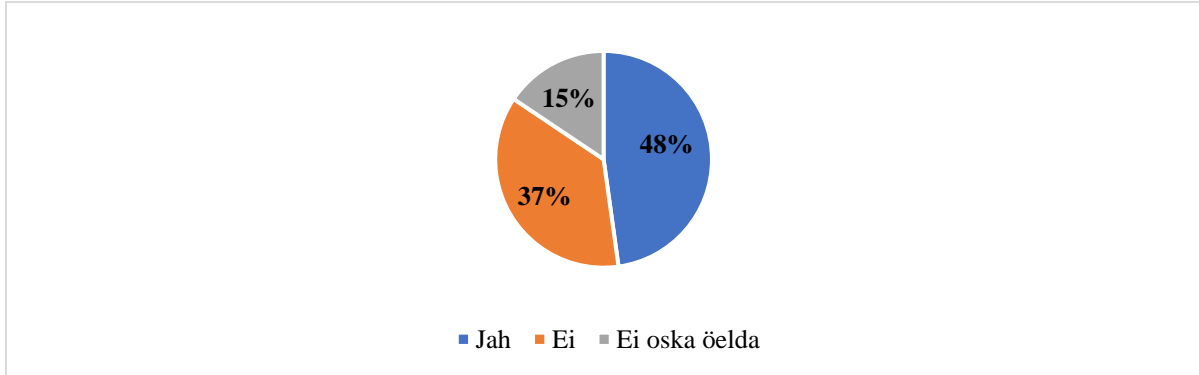
Tegelikke kasusaajaid tuvastatakse enim Äriregistri kaudu (77% vastajatest). Vastusevariandi „Muu“ all kajastus, et küsitakse isikult sellekohast allkirjastatud dokumenti, ettevõtte registriväljavõtet või omandistruktuuri kohta, või uuritakse Krediidinfo (6%). Välismaa andmebaasi kasutab 18% vastajatest (välismaale teenuse osutajate seas) ning tegelikke kasusaajaid ei tee kindlaks 19% vastajatest (vt joonis 12). Seega kasutatakse täiendavaid hoolsusmeetmeid, näiteks kahtluse korral lisadokumentide küsimist küllaltki vähe, usaldatakse Äriregistri andmeid. Siiski oli mõnes üksikus vastuses välja toodud, et Äriregistri andmed ei pruugi olla tõesed. Välismaale teenusepakkujad teevad tegelikke kasusaajaid kindlaks küllaltki vähe, millest saab järeldada, et andmetele võib olla keeruline ligi pääseda.



Joonis 12. Tegelikke kasusaajate tuvastamise allikad (autori koostatud)

Vastajate hinnangul on tegelikke kasusaajaid mõõdukalt keeruline kindlaks teha. Keskmise väärtus oli 5,2. Riikliku taustaga isikute kohta esitas autor küsimuse, kas ärisuht luues tehakse kindlaks, kas tegu võib olla riikliku taustaga isikuga. 48% vastajatest teeb riikliku taustaga isikute tausta kindlaks, 37% aga ei tee, 15% vastajatest ei teadnud, kas seda hoolsusmeetmet ettevõttes rakendatakse (vt joonis 13, lk 35). Sellest järeldub, et sellele hoolsusmeetme

rakendamisele tuleks rohkem tähelepanu pöörata. Kümnepalli skaalal hinnati riikliku taustaga isiku kindlakstegemise keerukust hindega 5,8. Seega on see vastajate jaoks pigem keeruline, kui väga lihtne.



Joonis 13. Riikliku taustaga isiku kindlakstegemine (autori koostatud)

Küsimusele, kas uuritakse, mis piirkonnast on klient pärit, et kontrollida ega klient pole pärit leebemate rahapesu tõkestamise nõuetega riigist vastati, et välismaale teenuse osutajate seas 76% kontrollib seda, 24% ei kontrolli. Seega täidetakse selle meetme osas nõuded küllaltki hästi. Kokku on rahapesu alasel koolitusel osalenud 36% vastajatest, 64% pole osalenud. Seega pole enamik vastajatest koolitusel osalenud. Eelnevast analüüsitust järeldub, et paljusid hoolsusmeetmeid täidetakse juba enda ettevõtluse kindlustamiseks, et tehingupartneri usaldusväärsuses kindel olla. Selgus, et vähim on rahapesu tõkestamise alasel koolitusel vastanutest osalenud Lääne-Virumaalt, Viljandimaalt, Saaremaalt (vt lisa 4, joonis 4).

Järgnevalt analüüsitakse küsitluse avatud küsimusi ning avatud küsimuste ja teooria põhjal tehakse järeldused suletud vastuste tulemuste kohta. Andmeanalüüsi meetodina kasutas autor sisuanalüüsi. Autor esitas küsimustikus 5 avatud küsimust, sellest lähtuvalt moodustas autor 5 kategooriat (vt tabel 2, lk 36). Analüüsi tulemused esitatakse kategooriate ja koodide kaupa.

Tabel 2. Avatud vastuste sisuanalüüsi kategooriad (autori koostatud)

Kategooriad	Koodid
Kategooria 1 Tehingupartneri mittekontrollimise põhjus	Kood 1 Isiklikud tuttavad Kood 2 Väikese käibega ettevõtted
Kategooria 2 Füüsilise isiku andmete kogumata ja kontrollimata jätmise ärisuhet luues	Kood 1 Isiklikud tuttavad Kood 2 Pikaajaline tehingupartnerlus Kood 3 Kulukas kontrollida Kood 4 Ettemaksu alusel usaldus
Kategooria 3 Tegelike kasusaajate kindlaks tegemata jätmise	Kood 1 Kulukas Kood 2 Isiklikud tuttavad Kood 3 Ebavajalik Kood 4 Äriregister ei kajasta õiget infot Kood 5 Aeganõudev
Kategooria 4 Kahtlaste tehingute korral toimimine	Kood 1 Kliendisuhete lõpetamine Kood 2 Tehingu kohta täiendava info küsimine ja vajadusel vastavate organisatsioonide teavitamine Kood 3 Audiitoriga konsulteerimine
Kategooria 5 Probleemkohad rahapesu tõkestamise nõuete järgimisel	Kood 1 Vähene info ja juhendmaterjalide puudumine Kood 2 Tasulised andmebaasid Kood 3 Suur halduskoormus Kood 4 Ebaproportsionaalsed nõudmised Kood 5 Suur ajakulu Kood 6 Tehingute kindlakstegemine Kood 7 Vähene rahvusvaheline koostöö Kood 8 Ebaselged nõuded, seaduse tõlgendamine Kood 9 Tankistide kasutamine Kood 10 Välismaiste tehingupartnerite kontroll

Küsimusele, miks ei nähta vajalikuks oma tehingupartneri tausta kontrollida vastati (**Kategooria 1**), et tegu on isiklike tuttavatega (Kood 1), keda usaldatakse või tehingupartneriks on väikese käibega ettevõtted, mistõttu rahapesu riski ei nähta (Kood 2). Sellest järeldub, et tutvusringkonda usaldatakse ja peetakse ebaoluliseks tema ettevõtlustegevuse tausta üle kontrollida. Teisele avatud küsimusele (**Kategooria 2**), miks ei nähta vajalikuks kontrollida ja koguda ärisuhet luues füüsilise isiku andmeid vastati enim, et tehinguid tehakse tuttavatega või kliendid on juba teada pikaajalise koostöö käigus (Kood 2).

Lisaks selgus, et mikroettevõtjate jaoks on see liiga kulukas, neil puudub selleks ressursse (Kood 3).

Tegelike kasusaajate kindlaks tegemata jätmise põhjusena (**Kategooria 3**) toodi asjaolu, et see on ressursimahukas (Kood 1) ja aeganõudev (Kood 5). Lisaks esines arvamus, et Äriregistri kuvatavad andmed ei ole korrektsed ehk tegelike kasusaajate taga peitub teine isik (Kood 4) ning tegelikku kasusaajat on kerge varjata. Veel toodi välja, et paljud andmed on Äriregistris uuendamata, kajastavad vana infot või andmeid pole kasusaajate kohta esitatud (Kood 4). Osade ettevõtjate jaoks on tegelike kasusaajate tuvastamine ebaoluline, kuna ettevõtjate jaoks pole oluline, kes tegelikult ettevõtlustegevusest kasu saab (Kood 3).

Tehingute jälgimise kohta esitas autor küsimuse, kuidas raamatupidamisettevõtjad toimivad, kui teenust pakkudes märkavad, et klient on eelnevalt vahetanud raamatupidamise teenuse pakkujat, teeb tehinguid *offshore* piirkonda, vahetab tihti pangakonto limiite (**Kategooria 4**). Enamik vastanutest leidsid, et lõpetavad kliendisuhete (Kood 1). Sealhulgas kajastus vastustest, et uuritakse kliendilt täpsemalt, milles tehing seisneb ja tegutsetakse vastavalt vajadusele (Kood 2). Kui kliendiga kontakti tulemusel selgus, et risk esineb, siis oldi valmis teavitama vastavaid institutsioone. Ära märgiti Rahapesu Andmebüroo ning Maksu- ja Tolliamet. Sellest järeldub, et vajadusel rakendatakse kõrgendatud hoolsusmeetmeid, võetakse arvesse ka tehingute suurust ja kliendi põhjendusi. Rahapesu teadet oldi valmis esitama küllaltki vähe, enamjaolt otsustatakse lihtsalt vastav kliendileping lõpetada. Esines ka üksikuid vastuseid audiitoriga konsulteerimise osas: see tähendab, et ollakse valmis küsima lisadokumente, kuid võrreldes enamike vastanutega teeb seda väga väike osa.

Rahapesu tõkestamise reeglite täitmise probleemkohti näeb 52% vastanutest (**Kategooria 5**). Enim nähakse infopuudust ja juhendmaterjalide vähesust (Kood 1). Ettevõtjatel pole piisavalt suuniseid, millest lähtuda. Lisaks on üheks põhjuseks ka ajakulukus (Kood 5) ning liigne halduskoormus (Kood 3). Raamatupidamisettevõtjate meelest on ebaoproportsionaalne seada neile sisuliselt samasid kohustusi, kui pankadele (Kood 4): see on neile liigne halduskoormus. Veel leiti, et mikro- ning väikeettevõtjatel on võrreldes suurettevõtetega vähem ressursse, et kõiki nõudeid täita. Puudujääke märgiti ka tehingute kindlaksmääramisel: keeruline on tuvastada kas tehing on tegelikult toimunud või on see näilik (Kood 6). Lisaks vastati, et kasutatakse tankiste (Kood 9) ning koolitused ei ole olnud piisavalt praktilised, et sealt saadud

teadmisi rakendada (Kood 1): „*Tihtipeale on rahapesijad head manipuleerijad ning on end hästi ette valmistanud ebameeldivatele küsimustele vastamaks*“. Avatud vastustest selgus, et paljud polnud nõuetega kursis, kohustatud isikute mõiste kui selline on raskesti määratletav (Kood 1). Info kättesaadamatuse all mõeldi ka andmebaaside kulukust (Kood 2) ning ühtse andmebaasi puudumist (Kood 7). Välja toodi ka asjaolu, et nõudmised on ebaselged (Kood 8), näiteks polnud osa vastajatest nõuetest teadlikud ning lubasid vastava teema kohta uurida.

### **2.3 Järeldused ja ettepanekud**

Küsimustiku analüüsi tulemustest ja avatud vastuste analüüsist võib järeldada, et puudujäägid on tingitud vähestest koolitustest või nendel osalemisest, mille põhjal saab väita, et ka teadmised kehtivate nõuete kohta on ebapiisavad. Seda kinnitab uuringu tulemus (vt käesolev töö lk 28), et enamik ehk 52% vastajatest ei pidanud end kohustatud isikuks või ei osanud sellele vastata. Lisaks puudub 72% vastanutest rahapesu tõkestamise sisekontrollieeskiri, millega rahapesu tõkestamine reguleeritud on (vt käesolev töö lk 29). Vastavalt teoreetilisele käsitlusele (vt käesolev töö lk 18) peab kohustatud isikutel olema koostatud sisekontrollieeskiri. Sellest järeldub ka see, et ettevõtte siseses kontrollis ja siseauditis esineb puudujääke: kui puudub sisekontrollieeskiri, siis ei saa ka siseauditi korras ettevõtte siseselt töötajate rahapesu tõkestamise nõuete järgimist efektiivselt kontrollida.

Puudujäägid esinevad ka tegelike kasusaajate tuvastamisel. Uuringu kohaselt (vt käesolev töö lk 34) ei tee tegelikke kasusaajaid kindlaks 19% vastajatest. Avatud küsimuste analüüsist selgus (vt käesolev töö lk 37), et selle põhjuseks on asjaolu, et see on ressursimahukas, aeganõudev, samuti on äriregistris andmed uuendamata või kasutatakse tankiste. Enamasti tehakse tegelikke kasusaajaid kindlaks Äriregistrit kasutades (vt käesolev töö lk 34). Eelnevad vastused ühtivad teoreetilise seisukohaga (vt käesolev töö lk 24), et tegelike kasusaajate tuvastamiseks tuleb mõista ettevõtte struktuuri jaotust ning täiendav info kogumine on ressursimahukas. Teoreetilise käsitluse järgi (vt käesolev töö lk 9-10) kasutavad paljud tegelikud kasusaajad variisikute dokumente. Sellest järeldub, et Äriregistris kajastuv info tegelike kasusaajate kohta võib olla väär juhul, kui vastav äriühing on rahapesuga seotud ning kui tegeliku kasusaaja nimi on vaid formaalselt Äriregistris kirjas.

Identifitseerimise faasi (vt käesolev töö lk 20) täidetakse mõõdukalt. See tähendab, et vastajatest ligikaudu 70% kogub füüsilise isikuga ärisuhet luues nende nime ja isikukoodi. Siiski võib selle 30% puudujäägi tõttu olla hilisema rahapesukahtluse korral keeruline teha andmete esitajat kindlaks (näiteks isikukoodi puudumisel). Juriidiliste isikute puhul täidetakse identifitseerimise faasi paremini: 92% vastajatest kogub äriühingu nime, esindusõigust kontrollib 82% vastajatest. Küll aga ei kontrollita ja koguta sidevahendite andmeid piisavalt. Eelnevast järeldub, et juriidiliste isikute andmeid kogutakse hoolikamalt. Kontrollimise faasis (vt käesolev töö lk 21) kontrollitakse kas esitatud andmed on olemas (nimi, isikukood, esindusõigus). Seda teeb isikut tõendava dokumendi abil 81% vastajatest (vt käesolev töö lk 32), lisaks esines vastuseid, mille korral võrreldi esitatud andmeid Äriregistris avaldatud andmetega.

Kinnitamise faasi (vt käesolev töö lk 21) täidetakse enim digitaalallkirja kasutades (66%), üks neljandik aga ei kontrolli kas esitatud andmed kuuluvad sellele isikule, kes väidab end olevat. Seega on see risk ning vajab suuremat tähelepanu. Vastavalt IVC mudelile (vt käesolev töö lk 20) ei kindlusta andmete kogumine ja nende kehtivus veel seda, et tegu on tõepoolest selle isikuga, kes end esitleb olevat (vt käesolev töö lk 21). Seega kui mudeli kolmandat faasi mitte täita, on rahapesijatel kergem kasutada variisikuid ning nende dokumente kasutades toiminguid teha, näiteks allkirju anda. Kuna digitaalallkirjaga ei tuvastata, kes digitaalallkirja annab, siis ainuüksi sellest võib olla vähe. Vastavalt teoreetilisele seisukohale (vt käesolev töö lk 10) kasutavad paljud tegelikud kasusaajad variisikute dokumente. Siiski 5% (vt käesolev töö lk 32) vastanutest ostab vastavat kliendi taustakontrolli teenust sisse, mille abil määratakse kliendi riskiprofiili paremini. Kuna avatud küsimuste analüüsist selgus, et tasutakontroll on kulukas ja aeganõudev ning mikro- ja väikeettevõtjatele liiga koormav, siis see võib olla üks põhjustest, miks kinnitamise faasi täitmisel seesugused puudused esinevad. Teoreetilise käsitlemise järgi (vt käesolev töö lk 21) on kliendi identifitseerimise protsess kulukas. Vastav väide ühtib järeldusega (vt käesolev töö lk 21) ning varasema lõputööga „Mittefinantsteenuseid pakkuvate kohustatud isikute teadlikkus rahapesu tõkestamise süsteemis Eestis“, kus K. Pärnpuu leidis samuti, et hoolsuskohustuse täitmine on kulukas (vt käesolev töö lk 21). Avatud küsimuste järgi peavad vastajad taustakontrolli alternatiiviks teenuse eest ettemaksu küsimist (vt käesolev töö lk 36).

Kliendiga ärisuhet luues kontrollib vaid 48% vastajatest, kas tegu võib olla riikliku taustaga isikuga. Vastajad hindasid riikliku taustaga isiku kindlakstegemise keerukust keskmiselt hindegas 5,8. Sellest järeldub, et seda pole väga keeruline teha kindlaks, pigem võib olla põhjuseks teadmatus, et seda tuleks eelnevalt kontrollida või ressursipuudus (vt käesolev töö lk 47, Kategooria 5, Kood 5). Käesoleva töö lk 24 teoreetilisest seisukohast lähtudes selgus, et riiklike taustaga isikute andmebaasid on kallid ja sellekohane võimekus seda kontrollida on pigem pankadel.

Mis puutub geograafiliste riskide kindlakstegemisse, siis 76% vastajatest kontrollib, mis riigist tehingupartner pärit on. Siiski selgus, et finantssanktsioonide lehekülge kasutab tehingupartneri taustakontrolliks vaid 3% vastajatest. Kuna finantssanktsioonid on ette nähtud ka füüsilistele isikutele (vt lisa 3), tuleks füüsilisest isikust tehingupartnerite korral neid riske põhjalikumalt jälgida.

Vastavalt teostatud analüüsile ja teoreetilistele seisukohtadele teeb autor Rahandusministeeriumile järgnevad ettepanekud:

1. Koostada kohustatud isikutele rahapesu hoolsusmeetmete kohta selgemad juhised/juhendmaterjalid.

Põhjendus: Näiteks luua konkreetne juhised, kuidas vastavas olukorras toimida. See võiks olla interaktiivne lahendus, mille korral suunatakse rahapesu riskide kindlakstegijat eraldi lehtedele, kust infot leida ja kontrollida ning millist infot ja mida kontrollida. Kuna paljude vastajate jaoks on kohustatud isikutele seatud nõuded ebaproportsionaalsed: see tähendab, et arvestatud pole ettevõtte võimekusega, teeb autor ettepaneku kehtivad nõuded üle vaadata või propageerida ettevõtete vahelist koostööd, et vastavaid andmeid tehingupartnerite kohta jagada.

2. Viia läbi rohkem ning praktilisemaid koolitusi.

Põhjendus: Nii teoriast kui ka läbi viidud küsitlusest saab järeldada, et kohustatud isikutele on riskipõhise lähenemise järgi seatud suur riskide hindamise vastutus. Selle põhjal saab järeldada, et kui koolitustel pole osaletud ja juhendmaterjale on vähe, on neil rahapesu riske maandada väga keeruline. Seda kinnitab ka uuringu tulemus, et paljud vastajatest oleksid lihtsalt kliendilepingu lõpetanud, kuid teadet poleks esitanud (vt käesolev töö lk 37).



### 3. Koostada andmebaas.

Põhjendus: See tähendab, et loodud oleks kohustatud isikutele mõeldud andmebaas, kus on rahapesu riskidega isikud kaardistatud, kuhu iga kohustatud isik saab märkida ilmnenud riskid. Nii oleks teistel kohustatud isikutel kergem riske kaardistada ning neid ka hinnata. Kui varasem risk on tuvastatud, siis ollakse selle ettevõttega tehinguid tehes või raamatupidamisteenust osutades ka valvsamad. Lisaks teeb rahapesu riskide maandamise keeruliseks ka informatsiooni laiali hajutatus, kui infot tuleb erinevast kohast otsida ning puudub ühtne koht, kust tehingupartneri tausta kontrollida. Autori arvates aitaks seesugune kohustatud isikutele mõeldud ühtne andmebaas kogutud infot koondada ning kohustatud isikute vahel infot jagada, et kokku hoida aega, mis kulub igal kohustatud isikul eraldi tehingupartneri taustakontrolliks ja riskide kaardistamiseks. Kas aga sellise andmebaasi loomine oleks õiguspärane, tuleks edasistes uurimistöodes uurida.

## KOKKUVÕTE

Kuna rahapesu on olnud viimastel aastatel mitmete pankade seas läbiviidud rahapesu kontrollide tõttu aktuaalne teema, on vajalik selgeks teha, mil määral panustavad rahapesu tõkestamisse raamatupidamisettevõtjad. Sellest tulenevalt püstitus järgnev probleemküsimus: „Kuidas täidavad raamatupidamisettevõtjad rahapesu tõkestamise nõuetest tulenevalt oma hoolsuskohustust?“. Lõputöö eesmärgiks oli välja selgitada hoolsuskohustuse täitmise viisid. Autor selgitas hoolsuskohustuse täitmist hoolsusmeetmete täitmise viisi järgi. See tähendab, et küsitletatavalt uuriti, mis allikaid kasutades nad täidavad hoolsusmeetmed ning mis on mitte täitmise põhjusteks.

Esimeseks uurimisküsimuseks oli: milliseid kriteeriume tuleb raamatupidamisettevõtjatel rahapesu tõkestamise nõuete alusel täita. Raamatupidamisettevõtjad kuuluvad rahapesu ja terrorismi rahastamise tõkestamise seaduse alusel kohustatud isikute sekka ning sellest tulenevalt tuleb neil kindlaks teha tehingute, kliendi ning geograafiliste piirkondadega seotud riskid ning tegelikud kasusaajad. Kliendiga seotud riskide all mõeldakse eelkõige kliendi ning tema ettevõtlustegevuse tasutakontrolli. Sellest lähtuvalt tuleb kohustatud isikutel koguda ärisuht luues füüsiliste isikute andmed ning maandada riske, et välistada olukorda, et klient saaks jääda anonüümseks. Kogutud andmete tõlevastavust tuleb kontrollida ning viimase etapina on vajalik teha kindlaks, et isik on see, kes väidab end olevat. Täiendavate riskide korral tuleb rakendada kõrgendatud hoolsusmeetmeid, näiteks riikliku taustaga isikute korral või kui ilmneb, et kliendi äritegevus on ebaharilik. Seega on riskipõhine lähenemine kohustatud isikutele seatud, et vastavalt ilmnenu asjaoludele rahapesu riski maandada.

Teiseks uurimisküsimuseks oli uurida, mis ressursse kasutades on võimalik hoolsuskohustust täita. Selgus, et selle täitmiseks on võimalik kasutada nii tasuta kui tasulisi siseriiklike andmebaase kui ka välismaa andmebaase. Uuringust selgus, et enim kasutatakse Maksu- ja Tolliameti kodulehekülge, seejärel Google otsingumootorit, Krediidinfot, Teatmikku, sotsiaalmeediat, Äriregistrit. Vähesel määral kasutatakse ka tasulisi tehisintellekti rakendusi, mis kujutab spetsiaalset tarkvara, et teha kindlaks, et isik on see, kes väidab end olevat.

Kolmandaks uurimisküsimuseks oli vastavalt teoreetilisele käsitlusele teha järeldusi, kuidas raamatupidajad saaksid rahapesu tuvastada. Kõige efektiivsem oleks raamatupidajatel

rahapesu tuvastada ladestamise ning integreerimise etapis. Ladestamise etapis üritatakse raha jälgi segada ehk selles osas saaksid raamatupidajad tuvastada pangakontodel ebaharilikku raha liikumist. Integreerumise faasis saaksid nad jälgida ettevõtete kuluartikleid: kas need on kooskõlas ettevõtlustegevusega.

Neljandaks uurimisküsimuseks oli analüüsida, milliste hoolsusmeetmete rakendamise osas võib raamatupidamisettevõtjatel esineda puudujääke. Küsitlusest selgus, et suurimad puudujäägid esinevad tegelike kasusaajate tuvastamisel, riikliku taustaga isikute kindlakstegemisel, rahapesu teate esitamisel ning võimalike finantssanktsioonide all olevate isikute kontrollis. Tegelikke kasusaajaid ei tuvasta 19% vastanutest. Kui vastavalt teoreetilisele seisukohale ja avatud küsimustele võtta arvesse asjaolu, et Äriregister ei pruugi anda tõest infot, siis tegelikkuses ei kontrollita tegelikke kasusaajaid põhjalikult. Vaid paar üksikut vastust esines, kui tehti kindaks ettevõtte omandistruktuur ehk hinnati, kes on ettevõtte tegelik kasusaaja. Riikliku taustaga isikuid tegid kindlaks 48% vastanutest ehk alla poolte. Rahapesu teadet esitasid vastavalt avatud küsimusele vaid väike osa vastajaid, enamasti lõpetati kliendiga leping. Välismaale raamatupidamise teenusepakkujate seas ilmnes, et kliendi võimalikku finantssanktsiooni all olemist kontrollib vaid 3% vastanutest. 25% vastajatest ei tee kindlaks, kas tehingupartnerit esindav isik on see, kes väidab end olevat. Küsitlusest selgus, et 71% vastajatest puudus rahapesu tõkestamist reguleeriv sisekontrollieeskiri. Sellest saab järeldada, et sisekontrollieeskirja puudumisel on ettevõtte töötajatel rahapesu riske keeruline hinnata ja märgata.

Esimeseks uurimisülesandeks oli analüüsida rahapesu olemusest ja selle skeeme, et mõista raamatupidamisettevõtjate rolli rahapesu tõkestamisel. Teiseks uurimisülesandeks oli analüüsida raamatupidamisettevõtjatele seatud nõuded. Selgus, et probleemkohtadena nähakse liiga suurt halduskoormust, mis raamatupidamisetevõtetele on seatud: võrreldes pankadega on raamatupidamisetevõtjatel palju vähem rahalisi ressursse, et kõiki neid nõudeid täita. Kuna tehisintellekti võimalused on kallid, pole raamatupidamisetevõtjatel piisavalt ressursse, et teha kindlaks, kas isik on see, kes väidab end olevat. See kajastus ka küsitluses, ainult 2% vastajatest ostavad vastavat teenust sisse, mis tehisintellekti kasutades pakub laiemat ja täpsemat kliendi taustakontrolli. Kolmandaks uurimisülesandeks oli analüüsida raamatupidamisetevõtjate rahapesu tõkestamise nõuete järgitavust ning teha vajadusel järeldusi.

Analüüsitust saab järeldada, et tehingupartnerite tausta kontrollitakse, vajadusel kasutatakse ka kõrgendatud hoolsuskohustuse meetmeid. Seega sai autor oma uurimisküsimustele vastused ning uurimisülesanded täidetud. Reeglite mitte täitmine on pigem tingitud ressursipuudusest kuid ka vähestest teadmistest ning suunistest, kuidas riske maandada. Raamatupidamisettevõtjad ootavad praktilisemaid koolitusi. Analüüsist tulenevalt teeb autor ettepaneku raamatupidamisettevõtjaid rahapesu tõkestamise hoolsusmeetmete vallas rohkem koolitada ning seada selgemad juhendmaterjalid. Lisaks pakub autor lahendusena suuremat infovahetust kohustatud isikute vahel andmebaasi loomisena, mis on mõeldud kohustatud isikutele rahapesu tõkestamise jaoks vajaliku info jagamiseks, et taustakontrollile ja riskide maandamisele kuluvat aega rohkem kokku hoida.

## SUMMARY

As money laundering has been a relevant topic in recent years, the author was interested in the extent to which accounting firms contribute to the prevention of money laundering. Consequently, the following problem question was posed: "How do accounting firms fulfil their due diligence obligations under anti-money laundering requirements?". The objective of the thesis was to identify the ways in which due diligence is carried out.

The first research question was to find out what criteria accounting firms have to comply with under the anti-money laundering requirements. Accountancy firms are obligated persons under the Anti-Money Laundering Act and, as such, are required to identify the risks associated with their transactions, their customers, their geographic areas and their beneficial owners. Customer-related risks are understood to mean, in particular, payment controls on the customer and his business activities.

The second research question was to investigate what resources are available to fulfil the due diligence obligation. It was found that both free and paid domestic databases and foreign databases could be used to fulfil this obligation. To a lesser extent, paid artificial intelligence applications are also used, which is a special software to verify that a person is who they claim to be. The third research question, in line with the theoretical approach, was to draw conclusions on how accountants could detect money laundering. It would be most effective for accountants to detect money laundering at the storage and integration stage. The fourth research question was to analyse which due diligence measures accountancy firms might be lacking in. The study found that the main shortcomings were in identifying beneficial owners, identifying persons with a national background, reporting money laundering and checking for possible financial sanctions. Only a small proportion of respondents reported money laundering according to the open question, most of them terminated the contract with the client.

Consequently, the author proposes that the requirements for accounting firms should be reviewed and that accounting firms should receive more training on anti-money laundering. As a solution, the author proposes either a greater exchange of information between the parties responsible or the creation of a single database for the collection of information needed to prevent money laundering.

## VIIDATUD ALLIKATE LOETELU

- Ai, L. & Tang, J., 2011. Risk-based approach for designing enterprise-wide AML information system solution. *Journal of Financial Crime*, 18 (3), pp. 268–276.
- Angell, I. O & Demetis, D. S., 2006. AML-related technologies: a systemic risk. *Journal of Money Laundering Control*, 9 (2), pp. 157–172.
- Anitei, N. C. & Gardikiotis, C. A., 2015. Money laundering. National and European regulations. *Jurnalul de Studii Juridice*, 10 (1-2), pp. 13–23.
- Auditortegevuse seadus* (2010) RT I, 21.11.2020, 2.
- Bryman, A., 2012. *Social Research Methods*. Oxford University Press: New York.
- E-krediidiinfo, 2021. *Creditinfo Eesti AS andmebaas ja Ametlik Maksehäireregister*. [Võrgumaterjal] Leitav: <https://www.e-krediidiinfo.ee/> [Kasutatud 30.03.2021].
- de Koker, L., 2009. Identifying and managing low money laundering risk. *Journal of Financial Crime*, 16 (4), pp. 334–352.
- de Koker, L., 2014. The FATF's customer identification framework: fit for purpose? *Journal of Money Laundering Control*, 17 (3), pp. 281–295.
- Demetriades, G., 2016. „Is the person who he claims to be?“ old fashion due diligence may give the correct answer! *Journal of Money Laundering Control*, 19 (1), pp. 79–91.
- Euroopa Ülemkogu, 2021. *Ehtsate isikut tõendavate ja reisidokumentide avalik veebiregister*. [Võrgumaterjal] Leitav: <https://www.consilium.europa.eu/prado/et/prado-start-page.html> [Kasutatud 30.03.2021].
- Evestus, S-H., 2015. Eelkuriteo sisustamine rahapesukuriteo puhul. *Juridica*, V, lk 360–365.
- FATF, 2014. *Transparency and beneficial ownership*. [Võrgumaterjal] Leitav: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf> [Kasutatud 07.12.2020].

FATF, 2019. *Risk-based Approach for the Accounting Profession*. [Võrgumaterjal] Leitav: <https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Accounting-Profession.pdf> [Kasutatud 07.12.2020].

Finantsinspeksioon, 2019a. *Finantsinspeksiooni tegevus 2019. aastal*. [Võrgumaterjal] Leitav: <https://www.fi.ee/et/finantsinspeksioon/rahapesu-tokestamine/finantsinspeksiooni-tegevus-2019-aastal> [Kasutatud 30.11.2020].

Finantsinspeksioon, 2019b. *Finantsinspeksiooni tegevuse strateegia 2019-2021*. [Võrgumaterjal] Leitav: [https://www.fi.ee/sites/default/files/2019-01/finantsinspeksiooni\\_tegevuse\\_strateegia\\_2019-2021.pdf](https://www.fi.ee/sites/default/files/2019-01/finantsinspeksiooni_tegevuse_strateegia_2019-2021.pdf) [Kasutatud 27.10.2020].

George-Dorel, P., 2013. Tax havens and the terrorism. *Constanta Maritime University Annals*, 14 (20) pp. 275–279.

Gichuki, N. E., 2020. The conflict between anti-money laundering reporting obligations and the doctrine of confidentiality for legal practitioners in Kenya. *Journal of Money Laundering Control*.

Gilmour, N., 2020. Illustrating the incentivised steps criminals take to launder cash while avoiding government anti-laundering measures. *Journal of Money Laundering Control*, 23 (2), pp. 515–526.

Gilmour, P. M., 2020. Lifting the veil on beneficial ownership. *Journal of Money Laundering Control*, 23 (4), p. 717–734.

He, P., 2006. Lawyers, notaries, accountants and money laundering. *Journal of Money Laundering Control*, 9 (1), pp. 62–70.

Kärner, M., 2019. Direktiiv (EL) 2018/1673 rahapesu vastu võitlemise kohta kriminaalõiguse abil. *Juridica*, VII, lk 518–532.

Laherand, M-L., 2008. *Kvalitatiivne uurimisviis*. Tallinn: OÜ Infotrükk.

Levi, M., 2002. Money Laundering and Its Regulation. *The ANNALS of the American Academy of Political and Social Science*, 582 (1), pp. 181–194.

Maksu- ja tolliamet, 2021. Maksukäitumise hinnangud. [Võrgumaterjal] Leitav: <https://maasikas.emta.ee/rating/search> [Kasutatud 30.03.2021].

Marsh, B., 2018. How effective data management and automation can improve operational efficiency in onboarding and know your customer. *Journal of Securities Operations & Custody*, 11 (4), pp. 337–344.

Meral, Y., 2020. Strategic Management to Prevent Money Laundering: The Role of Effective Communication. *Journal of Accounting and Finance*, 20 (6), pp. 40-41.

Mitsilegas, V. & Vavoula, N., 2016. The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law. *Maastrich Journal of European and Comparative Law*, 23 (2), pp. 261–293.

Moustafa, T. H., El-Megied, M. Z. A., Sobh, T. S. & Shafea, K. M. 2015. Anti money laundering using a two-phase system. *Journal of Money Laundering Control*, 18 (3), pp. 304–329.

Mugarura, N., 2014. Customer due diligence (CDD) mandate and the propensity of its application as a global AML paradigm. *Journal of Money Laundering Control*, 17 (1), pp. 76–95.

Nguyen, C. L., 2018. Preventing the use of financial institutions for money laundering and the implications for financial privacy. *Journal of Money Laundering Control*, 21 (1), pp. 47–58.

Õunapuu, L., 2014. *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes*. Tartu: Tartu Ülikool.

Pacini, C., Hopwood, W., Yound, G. & Crain, J., 2019. The role of shell entities in fraud and other financial crimes. *Managerial Auditing Journal*, 34 (3), pp. 247–267.



Politsei- ja Piirivalveamet, 2019. *Juhend kahtlaste tehingute tunnuste kohta*. [Võrgumaterjal] Leitav:

<https://www.politsei.ee/files/Rahapesu/juhendkahtlastetehingutetunnustekohta.pdf?222a84e8fa> [Kasutatud 30.12.2020].

Politsei- ja Piirivalveamet, 2021. *Dokumendi kehtivuse kontroll*. [Võrgumaterjal] Leitav:

<https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/> [Kasutatud 30.03.2021].

Pärnpuu, K., 2014. *Audiitorid ja raamatupidamisteenuse pakkujad rahapesu tõkestamise süsteemis Eesti näitel*. Magistritöö, Tallinn: Tallinna Tehnikaülikool.

Rahandusministeerium, 2017. *Rahandusministeeriumi valitsemisala arengukava aastateks 2018-2021*. [Võrgumaterjal] Leitav:

[https://www.rahandusministeerium.ee/et/system/files\\_force/document\\_files/rm\\_valitsemisala\\_arengukava\\_2018-2021\\_kinnitatud.pdf?download=1](https://www.rahandusministeerium.ee/et/system/files_force/document_files/rm_valitsemisala_arengukava_2018-2021_kinnitatud.pdf?download=1) [Kasutatud 27.10.2020].

Rahandusministeerium, 2020. *Juhis tegeliku kasusaaja määratlemiseks, v1.2*.

[Võrgumaterjal] Leitav:

[https://www.rik.ee/sites/www.rik.ee/files/elfinder/article\\_files/tegelike\\_kasusaajate\\_andmete\\_esitamise\\_juhis.pdf](https://www.rik.ee/sites/www.rik.ee/files/elfinder/article_files/tegelike_kasusaajate_andmete_esitamise_juhis.pdf) [Kasutatud 15.01.2021].

Rahandusminister, 2020. *Loetelu Eesti ametikohtadest, mille täitjaid loetakse riikliku taustaga isikuteks. Määrus. RT I, 24.09.2020, 4*.

Rahapesu Andmebüroo, 2020. *Ülevaade rahapesu andmebüroo tegevusest 2019. aastal*.

[Võrgumaterjal] Leitav: [https://www.politsei.ee/files/2020-06/1591869302\\_rab-aastaraamat-2019-est.pdf?718d45e9fb](https://www.politsei.ee/files/2020-06/1591869302_rab-aastaraamat-2019-est.pdf?718d45e9fb) [Kasutatud 27.10.2020].

Rahapesu Andmebüroo, 2021. *Kasulik info*. [Võrgumaterjal] Leitav:

<https://www.fiu.ee/kasulik-info/kasulik-info> [Kasutatud 30.03.2021].

*Rahapesu- ja terrorismi rahastamise tõkestamise seadus* (2017) RT I, 21.11.2020, 13.

Raza, M. S., Zhan, Q. & Rubab, S., 2020. Role of money mules in money laundering and financial crimes a discussion through case studies. *Journal of Financial Crime*, 27 (3), pp. 911–931.

- Registrite ja Infosüsteemide Keskus, 2008. *EMTAK 2008 selgitavad märkused*.  
[Võrgumaterjal] Leitav: [https://www.rik.ee/sites/www.rik.ee/files/elfinder/article\\_files/emtak\\_2008\\_pdf\\_0.pdf](https://www.rik.ee/sites/www.rik.ee/files/elfinder/article_files/emtak_2008_pdf_0.pdf)  
[Kasutatud 27.02.2021].
- Ross, S. & Hannan, M., 2007. Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control*, 10 (1), pp. 106–115.
- Saldana, J., 2009. *The Coding Manual for Qualitative Researchers*. London: Sage.
- Šesterikov, K., 2016. *Euroopa parlamendi ja nõukogu 20.05.2015 direktiivist (EL) 2015/849 tuleneva riskipõhise lähenemise ja Eesti kohtupraktikas väljatöötatud majandusliku põhjendatuse kriteerium*. Magistritöö, Tartu: Tartu Ülikool.
- Shust, P. M. & Dostov, V., 2020. Implementing innovative customer due diligence: proposal for universal model. *Journal of Money Laundering Control*, 23 (4), pp. 871–884.
- Soudijn, M. R. J., 2016. Rethinking money laundering and drug trafficking. *Journal of Money Laundering Control*, 19 (3), pp. 298–310.
- Subashi, R., 2014. The Beneficiary Ownership and Joint Stock Companies. *Journal of Finance, Accounting and Management*, 5 (1).
- Sviridenko, A., 2020. *Mittefinantsteenuseid pakkuvate kohustatud isikute teadlikkus rahapesu tõkestamise süsteemis Eestis*. Magistritöö, Tartu: Eesti Maaülikool
- Teatmik, 2021. *Teatmik.ee*. [Võrgumaterjal] Leitav: <https://www.teatmik.ee/et> [Kasutatud 30.03.2021].
- Teichmann, F. M. J., 2017. Twelve methods of money laundering. *Journal of Money Laundering Control*, 20 (2), pp. 130–137.
- Tibar, I., 2007. Rahapesu kujunemisloost ja olemusest. *Juridica*, VIII, lk 573–583.
- Tibar, I., 2018. Tähelepanekud uue rahapesu ja terrorismi rahastamise tõkestamise seaduse jõustumisega seoses. *Juridica*, I, lk 37–46.
- Tkatsova., O., 2014. *Rahapesu tõkestamise õiguslikud alused ja meetmed krediidi- ja finantseerimisasutustes*. Magistritöö, Tallinn: Tallinna Tehnikaülikool.

*Tulumaksuseadus* (1991) RT I, 28.12.2020, 13.

Ulst, I., 2003. Rahapesu ja terrorismi finantseerimine: regulatiivsed aspektid ja finantssüsteemi kaitsmine. *Juridica*, VII, lk 501–508.

van den Broek, M., 2011. The EU's preventive AML/CFT policy: asymmetrical harmonisation. *Journal of Money Laundering Control*, 14 (2), pp. 170–182.

Veriff, 2021. The AI-powered Identity Verification Platform-Veriff. [Võrgumaterjal] Leitav: <https://www.veriff.com/> [Kasutatud 30.03.2021].

Grant Thornton, 2021. Due diligence. [Võrgumaterjal] Leitav: <https://www.grantthornton.ee/teenused/finantsnoustamine/due-diligence/> [Kasutatud 30.03.2021].

Äriregister, 2021. Äriregistri teabesüsteem. [Võrgumaterjal] Leitav: <https://ariregister.rik.ee/> [Kasutatud 30.03.2021].

## Lisa 1. Küsimustik raamatupidamisettevõtjatele

### 1. Ettevõtte vanus (aastates)

- a) 0-5
- b) 6-10
- c) 11-15
- d) Üle 15

### 2. Äriühingu vorm

- a) OÜ
- b) FIE
- c) Muu

### 3. Raamatupidamine on:

- a) Peategevusala
- b) Lisategevusala
- c) Muu

### 4. Maakond

- a) Harjumaa
- b) Hiiumaa
- c) Ida-Virumaa
- d) Jõgevamaa
- e) Järvamaa
- f) Läänemaa
- g) Lääne-Virumaa
- h) Pärnumaa
- i) Põlvamaa
- j) Raplamaa
- k) Saaremaa
- l) Tartumaa

- m) Valgamaa
- n) Viljandi
- o) Võrumaa

**5. Ettevõtte suurus**

- a) Mikroettevõtja
- b) Väikeettevõtja
- c) Keskmise suurusega ettevõtja
- d) Suurettevõtja
- e) Ei oska öelda

**6. Kas teie ettevõtte on kohustatud isik rahapesu ja terrorismi rahastamise tõkestamise seaduse alusel?**

- a) Jah
- b) Ei
- c) Ei oska öelda

**7. Kas Teie ettevõttel on koostatud sisekontrollieeskiri rahapesu tõkestamiseks?**

- a) Jah
- b) Ei
- c) Ei oska öelda

**8. Milliseid allikaid kasutades kontrollite oma tehingupartneri tausta?**

- a) Google
- b) Teatmik
- c) Creditinfo
- d) Sotsiaalmeedia
- e) Kodulehekülg
- f) Maksu- ja Tolliameti kodulehekülg
- g) Ostan teenust sisse ettevõttelt, kes kasutab spetsiaalseid andmebaase ja tarkvara, et tehingupartneri tausta kontrollida

- h) Ei kontrolli
- i) Muu

**9. Kui vastasite eelmisele küsimusele „ei kontrolli“, siis palun põhjendage, miks te leiate, et see vajalik pole.**

**10. Millist allikat/allikaid peate kliendi taustakontrolliks kõige usaldusväärsemaks?**

- a) Google
- b) Teatmik
- c) Creditinfo
- d) Sotsiaalmeedia
- e) Kodulehekülg
- f) Maksu- ja Tolliameti kodulehekülg
- g) Sisse ostetud teenus (st ettevõttelt, kes teostab taustakontrolli ise, kasutades spetsiaalset tarkvara)
- h) Muu

**11. Mis andmeid kogute ärisuhet luues füüsilise isiku isikusamasuse tuvastamiseks?**

- a) Nimi
- b) Isikukood, elu- või asukoht isikukoodi puudumisel
- c) Esindusõigus
- d) Ei kogu andmeid
- e) Muu

**12. Mis allikast kontrollite füüsilise isiku isikusamasuse tuvastamiseks esitatud andmeid?**

- a) Isikut tõendav dokument
- b) Välismaal välja antud reisidokument
- c) Ei kontrolli
- d) Muu

**13. Mis allikat kasutades teete kindlaks, et isikusamasuse tuvastamiseks esitatud andmed ärisuhte loomiseks on tõesed ehk klient on see, kes väidab end olevat?**

- a) Ostan kliendi taustakontrolliks teenust sisse
- b) Digitaalalkiri
- c) Hääljetuvastus
- d) Digitaalfoto
- e) Sõrmejäljetuvastus
- f) Ei tee kindlaks
- g) Muu

**14. Kui vastasite eelmisele kolmele küsimusele eitavalt, siis palun põhjendage, miks te leiate, et see pole vajalik.**

**15. Milliste kliendi järgmiste andmete tõlevastavust kontrollite?**

- a) Juriidilise isiku ärinimi või nimi
- b) Registrikood või registreerimisnumber ja -aeg
- c) Juhataja nimi või juhatuse liikmete või muu seda asendava organi liikmete nimed ja nende volitused juriidilise isiku esindamisel
- d) Juriidilise isiku sidevahendite andmed
- e) Ei kontrolli

**16. Palun hinnake skaalal 1-10, kui keeruline on kontrollida eelmises punktis nimetatud andmete tõlevastavust? (0-Pole keeruline, 10-Väga keeruline)**

**17. Palun selgitage, kuidas toimite, kui kliendi kohta leidub vähe infot?**

- a) Ei sõlmi kliendiga lepingut
- b) Teen täiendavaid otsinguid
- c) Sõlmin kliendilepingu
- d) Muu

**18. Kuidas teete kindlaks tegelike kasusaajate andmed?**

- a) Ei tee kindlaks

- b) Äriregister
- c) Välismaa andmebaas
- d) Muu

**19. Palun hinnake skaalal 1-10, kui keeruline on tuvastada tegelikke kasusajaid?  
(0-pole keeruline, 10-võimatu)**

**20. Kui te ei tee kindlaks tegelikku kasusajat, siis miks Te leiate, et see on ebavajalik?**

**21. Kui loote ärisuhte uue kliendiga, siis kas uurite, kas isik võib olla riikliku taustaga isik?**

- a) Jah
- b) Ei
- c) Ei oska öelda

**22. Palun hinnake skaalal 1-10, kui keeruline on tuvastada riikliku taustaga isikut?  
(0-pole keeruline, 10-võimatu)**

**23. Kui loote ärisuhte uue kliendiga, kas uurite, mis piirkonnast on klient pärit, et kontrollida ega klient pole pärit leebemate rahapesu tõkestamise nõuetega riigist?**

- a) jah
- b) ei
- c) ei paku teenust välismaale

**24. Kas Te olete osalenud rahapesu tõkestamise koolitusel?**

- a) Jah
- b) Ei

**25. Palun selgitage, kuidas toimiksite, kui avastate teenust pakkudes, et kliendi äritegevus on ebaharilik: algdokumentidelt nähtub väärkajastusi, klient on**



eelnevalt tihti vahetanud raamatupidamisteenuse pakkujat, klient muudab tihti pangakontol limiite ning teeb tehinguid *offshore* piirkonda?

26. Palun hinnake skaalal 1-10, kui keeruline on teha kindlaks rahapesu riske? See tähendab, et peate hindama kliendi, tehingute ja geograafiliste piirkondadega seotud riske ning vajadusel võtma kasutusele kõrgendatud meetmed, et riske maandada? (0- pole keeruline, 10- väga keeruline)

27. Milliseid probleemikohti näete rahapesu tõkestamise reeglite täitmisel?

## Lisa 2. Raamatupidamisettevõtete arv Äriregistris

Tabel. Raamatupidamisettevõtete arv Äriregistris (autori koostatud kuupäeval 20.02.2021)

Maakond	AS	TÜ	FIE	UÜ	OÜ	TÜH	Kokku
Harju	26	26	174	39	4252	4	4521
Hiiu		1	5	1	48		55
Ida-Viru	1	3	45	15	236		300
Jõgeva	1		21		75		97
Järva			15		100		115
Lääne	1		13	2	111		127
Lääne-Viru			33	5	224	1	263
Põlva			13	1	79	1	94
Pärnu			49	2	401	1	453
Rapla		1	27		181		209
Saare	2		23	1	159		185
Tartu	2	2	53	17	792		866
Valga		1	12	1	81		95
Viljandi	1		25	6	143		175
Võru	1	1	16	3	92		113
<b>Kokku:</b>	<b>35</b>	<b>35</b>	<b>524</b>	<b>93</b>	<b>6974</b>	<b>7</b>	<b>7668</b>

### **Lisa 3. Tehingupartneri taustakontrolli võimalused**

Vastavalt uurimiseesmärgile on kohustatud isikutel mitmeid valikuid täita hoolsusmeetmeid. Nagu varasemalt toodud, tuleks juriidiliste isikute tasuta põhjalikult kontrollida, et võimalikke riske maandada. Vastavateks võimalusteks on kasutada nii siseriiklikke kui ka välismaa andmebaase. Äriregistrist saab andmeid ettevõtte juhatuse liikme(te) kontaktide kohta, aadressi, sidevahendite, tegelike kasusaajate kohta, seoseid teiste äriühingutega (Äriregister, 2021). Seega saab äriregistrit kasutada tegelike kasusaajate tuvastamiseks.

Äriühingu üldandmete kohta saab infot Teatmikust. Seal kuvatakse äriühingu võlgnevused, tegevusload, esitatud ja esitamata majandusaasta aruanded, tasutud maksud ning töötajate arv. (Teatmik, 2021) Creditinfost saab teavet äriühingu üldandmete kohta. Lisaandmete saamiseks tuleb soetada vastav pakett. (E-krediidiinfo, 2021) Maksu- ja Tolliameti koduleheküljelt saab valida avalike andmete päringu. Maksukäitumise hinnangutes kuvatakse ettevõtte üldandmed ning kvartalite lõikes tasutud maksud, töötajate arv, ettevõtte ajalugu. Lisaks saab Maksu- ja Tolliameti kodulehelt teha päringut võlainfo kohta. (Maksu- ja Tolliamet, 2021) Käsitsi otsingute alternatiiviks on osta sisse spetsiaalset teenust. Mitmed ettevõtted pakuvad vastavat teenust, et kliendi eest otsinguid teha. Näiteks pakub Grant Thornton hoolsusauditit. Selle käigus hinnatakse ettevõtte majanduslikku, juriidilist ning maksukäitumist (Grant Thornton, 2021).

Geograafiliste riskide korral tuleb tuvastada kõrge riskiga riigid: selle kohta saab infot FATFi koduleheküljelt või komisjoni delegeeritud määrusest (EL) 2016/1675. Suure riskiga kolmandaks riigiks peetakse RahaPTS § 37 lg 4 järgi piirkonda, kus (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017):

- Klient on seotud riigiga, kus on ebatõhus rahapesu tõkestamise süsteem.
- Esineb kõrge kuritegevuse tase.
- Euroopa Liit või ÜRO on kehtestanud sanktsioonid.
- Tegutsevad terroristlikud organisatsioonid.

Euroopa Liidu kehtestatud sanktsioonidega saab tutvuda aadressilt [sanctionsmap.eu](https://sanctionsmap.eu). Seal on välja toodud, mis isikute ja riikide suhtes sanktsioonid kehtivad. (EU Sanctions Map, 2021)

Isikusamasuse tuvastamiseks esitatud andmete kehtivust, näiteks isikut tõendava dokumendi kehtivust saab kontrollida Politsei- ja Piirivalveameti koduleheküljelt, dokumendi kehtivuse kontrollist (Politsei- ja Piirivalveamet, 2021).

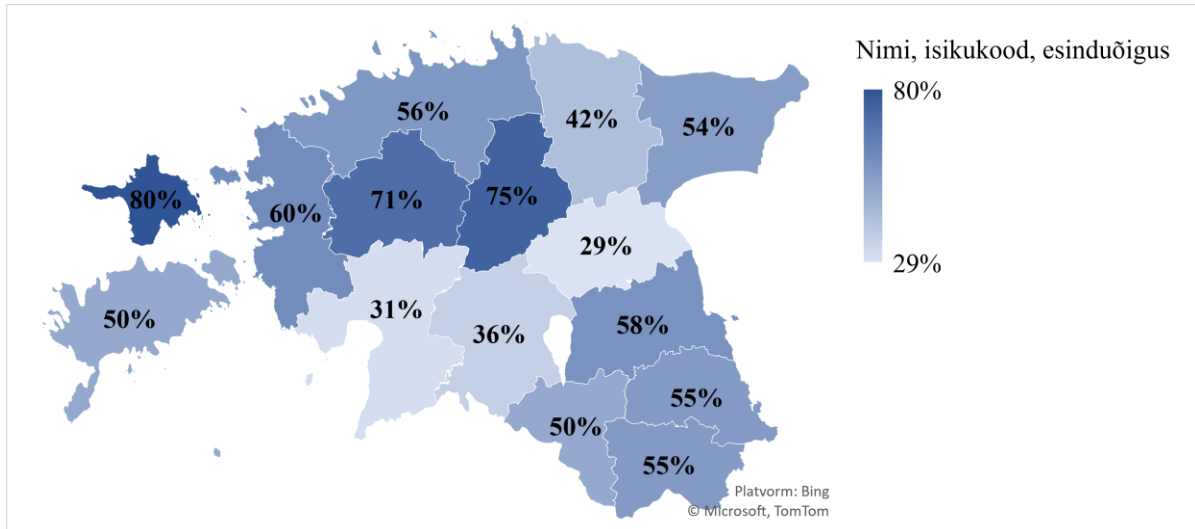
Isikut tõendavate dokumentide ehtsuse kohta saab informatsiooni Ehtsate isikut tõendavata ja reisidokumentide avalikust veebiregistrist (PRADO). Sinna on koondatud erinevate riikide andmebaaside lingid, kust dokumendi kehtivust kontrollida. Siiski ei kajasta see täiesti õigeid andmeid. Lisaks on toodud erinevate riikide dokumentide näidised, sealhulgas võltspasside näidised, kehtetud passid. (Euroopa Ülemkogu, 2021)

Kui äriühing tahab tehingupartneri usaldusväärsuses täiesti veenduda, on võimalus osta teenust sisse. Näiteks pakub Veriff OÜ teenust, et teha kindlaks kas isik on see, kes väidab end olevat. Selleks tuleb tuvastataval isikul saata endast pilt ning isikut tõendav dokument, mille järel tehisintellekt teeb kindlaks kas tegu on õige isikuga. (Veriff, 2021) ShuftiPro teenust kasutades on võimalik teha rahapesu riskid kiirelt kindlaks tuginedes FATFi soovitustele, kuna tehisintellekti abil tehakse otsinguid erinevatest andmebaasidest. Näiteks saab identifitseerida riikliku taustaga isikuid. Veel saab lasta teha tuvastatava isikuga video, et riske maandada (ShuftiPro, 2021). Määruse „Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord“ § 11 lg 1 järgi esitatakse isikule küsimusi vastavalt tema täidetud ankeedile (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017).

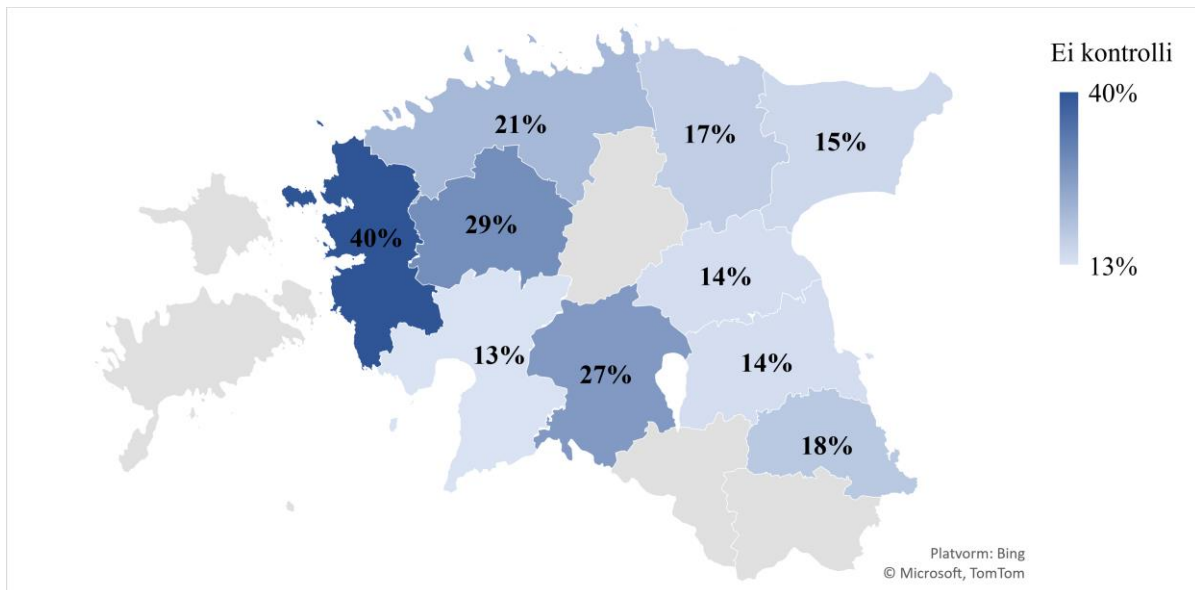
Eelpool nimetatud võimalused pole ammendav loetelu, vaid näited. Kui teenus on liiga kallis, on alternatiiviks teha vastavaid otsinguid ise. Riikliku taustaga isikute nimistuga saab tutvuda määrusest „Loetelu Eesti ametkohtadest, mille täitjaid loetakse riikliku taustaga isikuteks“ (Rahandusminister, 2020). Detailsema informatsiooni leidmiseks saab infot Rahapesu Andmebüroo koduleheküljelt, kus on edasised viited (Rahapesu Andmebüroo, 2021).

## Lisa 4. Vastused maakondade lõikes

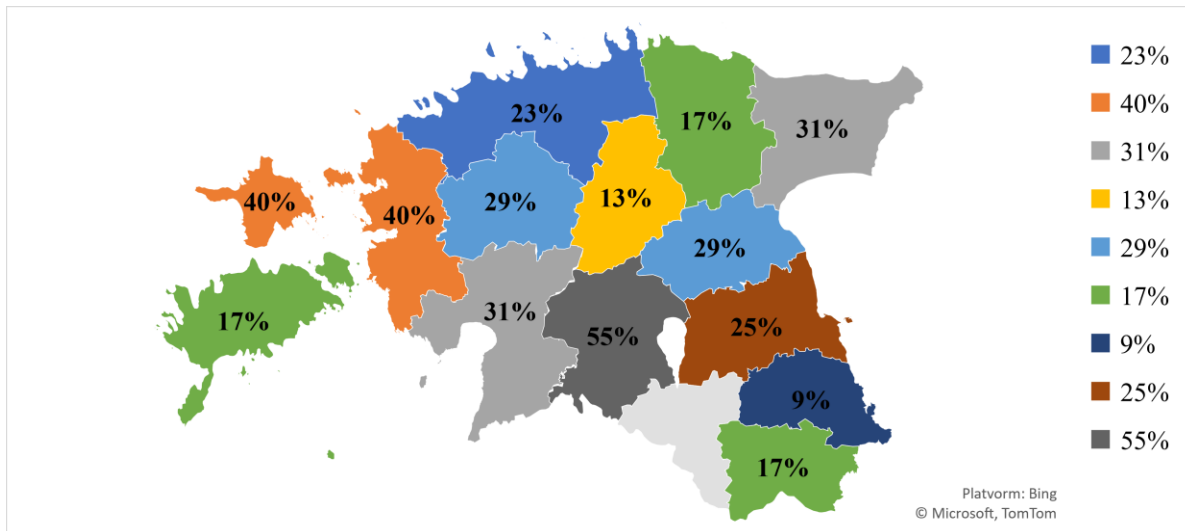
Küsimustiku vastused maakondade lõikes on toodud neljal erineval joonisel.



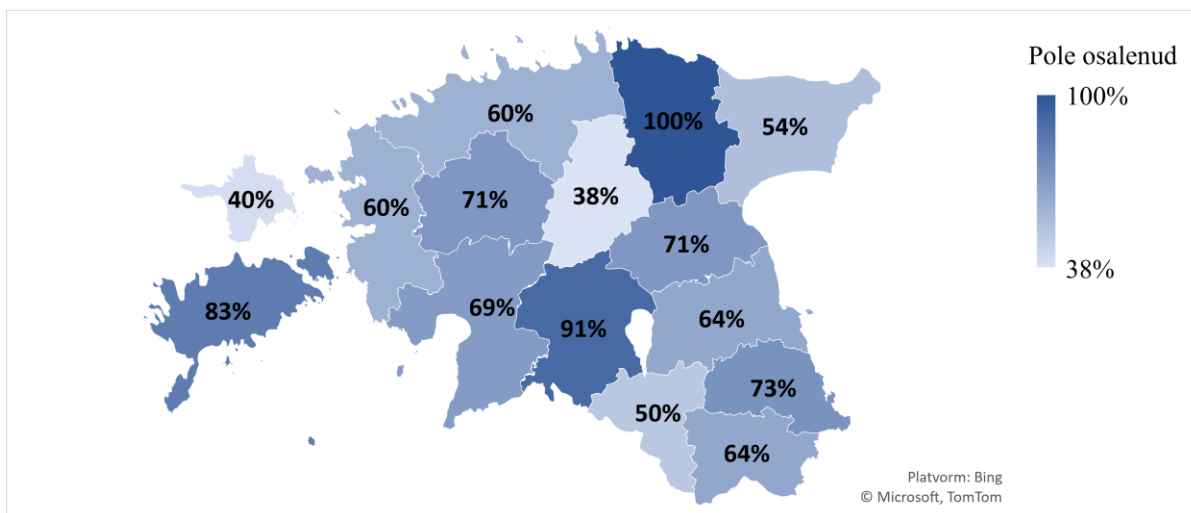
Joonis 1. Nime, isikukoodi ja esindusõiguse kogumine maakondade lõikes (autori koostatud)



Joonis 2. Isikusamasuse tuvastamiseks esitatud andmete kontrollimine (autori koostatud)



Joonis 3. Tegeliku isiku kindlaks tegemata jätmise (autori koostatud)



Joonis 4. Rahapesu tõkestamise koolitusel mitte osalenute osakaal vastajate seas (autori koostatud)