

Sisekaitseakadeemia

Finantskolledž

Liisi Orav

**SULARAHAGA SEOTUD RAHAPESU TÕKESTAMISE
HOOLSUSMEETMETE RAKENDAMINE
PANGANDUSSEKTORI NÄITEL**

Lõputöö

Juhendaja:

Kaide Tammel, PhD

Tallinn 2024

SISEKAITSEAKADEEMIA LÕPUTÖÖ ANNOTATSIOON

Finantskolledž	Juuni 2024
<p>Töö pealkiri eesti keeles: Sularahaga seotud rahapesu tõkestamise hoolsusmeetmete rakendamine pangandussektori näitel</p> <p>Töö pealkiri inglise keeles: Implementation of Due Diligence Measures to Prevent Cash-Related Money Laundering on the Example of the Banking Sector</p> <p>Lõputöö on kirjutatud teemal „Sularahaga seotud rahapesu tõkestamise hoolsusmeetmete rakendamine pangandussektori näitel“. Lõputöö on kirjutatud eesti keeles ning eesti- ja inglisekeelse kokkuvõttega.</p> <p>Lõputöö eesmärk on välja selgitada sularahaga seotud rahapesu tõkestamisel esinevad probleemid pangandussektoris. Eesmärgi täitmiseks on püstitatud neli uurimisülesannet: 1. Anda ülevaade teemakohase kirjanduse põhjal rahapesu õigusaktidest. 2. Anda ülevaade teaduskirjanduse põhjal sularahaga seotud rahapesu riskidest ja riskihinnangust. 3. Analüüsida pangandussektoris rahapesuga seotud finantsametnike hinnanguid sularahaga seotud rahapesu hoolsusmeetmete rakendamise kohta. 4. Analüüsida võimalikke lahendusi ning teha selle põhjal järeldusi.</p> <p>Töö raames viidi läbi kvantitatiivne uuring, mis aitab kõige paremini saada vastused lõputöös püstitatud probleemile, uurimisküsimustele, uurimisülesannetele ja eesmärgile. Andmekogumismeetodiks on uurimistöös ankeetküsitlus. Küsitlus viidi läbi ühes Eesti pangas, mis vastab elutähtsa teenuse osutaja tingimustele ning küsitleti antud panga kolme erineva osakonna töötajaid.</p>	
Võtmesõnad: rahapesu, sularaha, pangandussektor, hoolsusmeetmed	
Võõrkeelsed võtmesõnad: money laundering, cash, banking sector, due diligence	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
<p>Töö autor: Liisi Orav</p> <p>Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjallikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Annan Sisekaitseakadeemiale 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 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>	
Vastab lõputöö nõuetele	
Juhendaja: Kaide Tammel	allkirjastatud digitaalselt
Kaitsmisele lubatud	
Kolledži direktor: Kerly Randlane	allkirjastatud digitaalselt

SISUKORD

SISSEJUHATUS.....	5
1. RAHAPESU TÕKESTAMINE NING SELLEGA SEOTUD NÕUDED JA REGULATSIOONID	8
1.1 Rahapesuvastaste nõuete evolutsioon Ameerika Ühendriikides.....	8
1.2 Rahapesuvastase võitlusega seotud nõuded ja regulatsioonid.....	9
1.2.1 Rahapesu tõkestamine Euroopas	9
1.2.2 Euroopa Liidu direktiivid	10
1.3 Rahapesu tuvastamine ja tõkestamine pankades.....	11
1.3.1 Eestis kehtivad rahapesuvastase võitluse reeglid ja asutuste roll	14
1.3.2 Pankade I ja II kaitseliin	15
1.4 Sularahaga seotud rahapesu hoolsusmeetmete rakendamine pankades.....	16
1.4.1 Sularaha ja rahapesu	16
1.4.2 Sularahatehingute kontroll pankades.....	18
1.4.3 Riskipõhine lähenemine	19
1.4.4 Tunne oma klienti põhimõte.....	22
2. SULARAHATEHINGUTE RAHAPESUVASTASTE HOOLSUSMEETMETE RAKENDAMINE PANGAS	23
2.1 Uurimismeetodi kirjeldus.....	23
2.2 Pangandussektori sularahaga seotud hoolsusmeetmete täitmine	24
2.2.1 Küsimused I kaitseliinile.....	26
2.2.2 Küsimused II kaitseliinile	33
2.3 Järeldused ja ettepanekud.....	37
KOKKUVÕTE	41
SUMMARY	43
VIIDATUD ALLIKATE LOETELU	44
Lisa 1. Küsimustik telleritele	49
Lisa 2. Küsimustik KYC osakonnale	51
Lisa 3. Küsimustik AML osakonnale	54

TERMINITE JA LÜHENDITE LOETELU

RahaPTS – Rahapesu ja terrorismi rahastamise tõkestamise seadus

FATF - Rahapesu tõkestamise toimkond (ingl *The Financial Action Task Force*)

RAB – Rahapesu Andmebüroo

KYC – tunne oma klienti põhimõte (ingl *know your customer*)

SISSEJUHATUS

Hoolimata Eesti riigi tugevast finantssektorist, on rahapesu murettekitav probleem. Rahapesu levikul on mitmeid kohalikke ning ka rahvusvahelisi tagajärgi, rõhutades vajadust tõhusamate meetmete järele selle vastu võitlemiseks. Sularahaga seotud rahapesu tõkestamine on tänapäeva pangandussektoris oluline väljakutse, kuna see nõuab tõhusaid hoolsusmeetmeid kuritegeliku tegevuse ärahoidmiseks ja finantsstabiilsuse tagamiseks.

Elektrooniliste maksevõimaluste arengust hoolimata eelistavad kurjategijad siiski sularaha, et tagada oma täielik anonüümsus. 2023. aasta juunis avaldas Rahapesu Andmebüroo artikli teemal „Sularahaga seotud rahapesuohu Eestis püsib“. (Rahapesu Andmebüroo, 2023b lk 2) Uudises kajastub, et kõige kõrgem rahapesu risk on kinnisvara, valuutavahetuse, investeerimiskulla ja hasartmänguteenuste sektoris. Samas tuleb välja, et Eesti roll kuritegeliku sularaha transiitriigina on vähenenud. (Rahapesu Andmebüroo, 2023a; 2023b, lk 2)

Lõputöö teema on aktuaalne, kuna sularahaintensiivsete teenuste rahapesuohu tase on Eestis tõusnud ning seda sellepärast, et sularahatehingud on sagenenud. Sularahakäibe suurenemisele on kaasa aidanud ka kiire inflatsioon ja majanduslangus. (Rahapesu Andmebüroo, 2023a; 2023b, lk 2) Samuti on sularahatehingud jätkuvalt oluline osa majandusest ning seetõttu on nende kaudu võimalik viia ellu ja varjata ebaseaduslikke rahalisi tegevusi. Antud teema on uudne, sest lõputöö keskendub sularahatehingutega seotud rahapesu tõkestamise hoolsusmeetmete rakendamisele pangandussektoris. Aastal 2023 uuris Rahapesu Andmebüroo sularahaga seotud rahapesu ja terrorismi rahastamise riske Eestis. Töö keskendus probleemidele, millised muutused on toimunud sularaha mahtude ja kasutamise osas, millised on kahtlased tegevusmustrid ja millised on peamised teatamislüngad. (Rahapesu Andmebüroo, 2023b, lk2) Sisekaitseakadeemias on varasemalt kaitstud töö pealkirjaga „Rahapesu tõkestamise hoolsusmeetmete rakendamist pangandussektori näitel“. Lõputöö eesmärk oli välja selgitada rahapesu tõkestamise hoolsusmeetmete rakendamine pangandussektori näitel (Alaküla, 2018, lk 4). Antud lõputöö uudsus seisneb selles, et esmakordselt uuritakse sularahatehingutega seotud rahapesu tõkestamise hoolsusmeetmete rakendamist just Eesti pankades.

Rahapesu tõkestamine toimub efektiivsemalt, kui järgitakse ning täidetakse põhjalikumalt hoolsusmeetmeid. Hoolsusmeetmed aitavad finantsasutusel tuvastada ja ennetada

potentsiaalseid rahapesu riske või juhtumeid. Näitena saab tuua kliendi tuvastamise ning temaga kaasneva riski hindamise. See annab pangale võimaluse mõista kliendi tausta, rahavooge ja äritegevust ning selle põhjal avastada kahtlaseid või ebatavalisi tehinguid. Sellest tulenevalt on oluline, et pangad suudaksid veelgi intensiivsemalt kontrollida sularahaga seotud tehinguid. Kriminaalse päritoluga sularaha liigub siiski läbi Eesti pankade ning enamasti saadakse illegaalne sularaha narkokuritegevusest või salakaubandusest. (Rahapesu Andmebüroo, 2023a) Uurimisprobleemina on püstitatud küsimus: kas praegusel hetkel suudetakse pangas kontrollida nii põhjalikult sularahatehinguid, et vähendada rahapesu ning sellega kaasnevaid riske? Probleemidele võimalike lahenduste välja selgitamiseks on püstitatud uurimisküsimused:

- 1) Milliseid hoolsusmeetmeid rakendatakse sularaha kontrollimisel?
- 2) Millised probleemid ilmnevad pankadel sularaha päritolu kontrollimisel?
- 3) Millised on võimalikud lahendused neile probleemidele?

Lõputöö eesmärk on välja selgitada sularahaga seotud rahapesu tõkestamisel esinevad probleemid pangandussektoris. Eesmärgi saavutamiseks on püstitatud järgmised uurimisülesanded:

1. Anda ülevaade teemakohase kirjanduse põhjal rahapesu õigusaktidest.
2. Anda ülevaade teaduskirjanduse põhjal sularahaga seotud rahapesu riskidest ja riskihinnangust.
3. Analüüsida pangandussektoris rahapesuga seotud finantsametnike hinnanguid sularahaga seotud rahapesu hoolsusmeetmete rakendamise kohta.
4. Analüüsida võimalikke lahendusi ning teha selle põhjal järeldusi.

Lõputöö eesmärgi saavutamiseks kasutatakse kvantitatiivset uurimismetoodikat. Andmete kogumiseks kasutatakse dokumendianalüüsi ning ankeetküsitlust. Küsitluses esitatakse avatud ja suletud küsimusi. Dokumendianalüüsis kasutatakse erialast teaduskirjandust, Euroopa Liidu direktiive, Eesti rahapesu ja terrorismi rahastamise tõkestamise seadust, analüütilisi artikleid, muid õigusakte, varasemalt läbiviidud uurimistöid ja rahvusvaheliste organisatsioonide raporteid. Küsitlus viiakse läbi ühes Eesti pangas, mis vastab elutähtsa teenuse osutaja tingimustele ning küsitletakse antud panga kolme erineva osakonna töötajaid. Andmete analüüsiks kasutatakse kvantitatiivset sisuanalüüsi.

Lõputöö esimene peatükk jaguneb neljaks alapeatükiks, mis omakorda hargnevad mitmeks peatükiks. Esimeses alapeatükis antakse ülevaade rahapesuvastaste nõuete arengust ja

nende algusest. Teises alapeatükis käsitletakse rahapesuvastase võitlusega seotud nõudeid ja regulatsioone. Kolmandas alapeatükis analüüsitakse rahapesu avastamist ja takistamist panganduses ning rõhutatakse I ja II kaitsetaseme tähtsust. Neljas alapeatükk uurib sularahaga seotud rahapesu ennetamise meetmeid pangandussektoris, arutleb sularaha rolli ja olulisust, uurib sularahatehingute järelevalvet ning riskipõhist lähenemist. Teine peatükk koosneb kolmest alapeatükist. Esimeses alapeatükis kirjeldatakse uurimismetoodikat. Teises alapeatükis analüüsitakse pangas läbi viidud küsitlust, mis on jaotatud mitmeks alapeatükiks. Kolmandas alapeatükis tehakse järeldusi küsitluse tulemuste põhjal ning esitatakse soovitusi.

1. RAHAPESU TÕKESTAMINE NING SELLEGA SEOTUD NÕUDED JA REGULATSIOONID

1.1 Rahapesuvastaste nõuete evolutsioon Ameerika Ühendriikides

Aastal 1970. andis USA Kongress välja Pangasaladuse seaduse (ingl *Bank Secrecy Act*), mis võimaldas valitsusasutustel juurdepääsu pangaandmetele eesmärgiga lihtsustada kriminaal-, maksu- ja regulatiivset uurimist. Seadus nõudis pankadelt üksikasjalikku arvestust suuremate valuuta- ja rahvusvaheliste tehingute kohta ning kohustas neid pidama arvestust kontoomanike ja finantsinstrumentide üle. (Mencken, 1998, p. 476) Eesmärk oli tuvastada valuuta ja muude rahaliste vahendite päritolu ja liikumist Ameerika Ühendriikidesse või sealt välja ning nõuda finantsasutustelt aruandlust sularahatehingute kohta, õigeaegset isikutuvastust tehingute tegemisel ning finantstehingute dokumentide säilitamist. (Eldridge, 1986, p. 668)

Aastal 1986 võeti vastu Rahapesu Tõkestamise Seadus (ingl *Money Laundering Control Act*), mille eesmärk oli kuritegelikku finantstegevust kontrolli all hoida, jälgides kuritegevusest saadud vahendeid ning defineerides rahapesu föderaalseks kuriteoks. See suurendas valitsuse võimekust rahapesijaid vastutusele võtta, kehtestades uued tsiviil- ja kriminaalvastutuse meetmed sisuliste kuritegude korral. (Irvine & King, 1987, p. 182)

Rahapesuvastane raamistik laienes taaskord 1992. aastal, kui võeti vastu Annunzio-Wylie rahapesuvastane seadus. Seadus muutis finantsasutuste rolli oluliselt, nõudes neilt kahtlaste tehingute korral kahtlase tegevuse aruande koostamist ning kehtestades miinimumnõuded AML (ingl *Anti Money Laundering*) vastavusprogrammidele. See seadis vastutuse aruannete esitamise otsustamise pankadele ning nõudis neilt ka aruande esitamist FinCENile koos põhjendustega. FinCEN on USA Rahandusministeeriumi allüksus, mis kogub teavet rahapesu ja terrorismivastase võitluse jaoks. See loodi 1990. aastal rahapesukuritegude avastamiseks, uurimiseks ja süüdistamiseks. (Wilkes, 2020, p. 655)

Pangasaladuse seadus muudeti 1994. aastal Kongressi poolt Rahapesu Tõkestamise seaduseks (ingl *Money Laundering Suppression Act*), eesmärgiga tõhustada potentsiaalsete rahapesuoperatsioonide uurimist ja lihtsustada valuutatehingute aruandlust. (Jaarsveld, 2011, p. 398) Mõned aastad hiljem, aastal 2001. kehtestati Rahvusvaheline Rahapesu Tõkestamise ja Välisriikide Korrupsioonivastane Seadus (ingl *International Counter-Money Laundering and Foreign Anti-Corruption Act*), et julgustada riike ja pankasid,

keda Ameerika nägi ohuna rahapesule, muutma oma seniseid tavaid ning välja töötama meetmeid kahtlaste tehingute tuvastamiseks. (Jaarsveld, 2011, p. 399)

1.2 Rahapesuvastase võitlusega seotud nõuded ja regulatsioonid

Rahvusvaheliste rahapesu tõkestavate meetmete väljatöötamiseks loodi 1989. aastal rahapesuvastane töörihm (FATF), et töötada välja meetmed rahapesuvastase poliitika rakendamiseks. (Haq, *et al.*, 2022, pp. 3) FATF kehtestab ülemaailmsed standardid ja kasutab erinevaid vastavusmehhanisme, et tagada rahapesu, terrorismi rahastamise ja sellega seotud ohtude vastu võitlemise õiguslike, regulatiivsete ja operatiivmeetmete tõhus rakendamine. (Goldbarsht, 2018, p. 265)

FATF-i peetakse arenenud riikide organisatsiooniks, mille eesmärk koostöös Majanduskoostöö ja Arengu Organisatsiooniga (ingl *Organization for Economic Cooperation and Development – OECD*) on võidelda rahapesuga. 2000. aastal viidi läbi uurimised, kus külastati riike, mida peeti olevat rahapesu keskusteks ning anti välja “must nimekiri”. Sinna kuulus 15 riiki, milles on ebapiisav või isegi täiesti olematu seadusandlus võitluseks rahapesuga. ÜRO riikidel soovitati pöörata rohkem tähelepanu tehingutele, mis tulevad “musta nimekirja” kuuluvatest riikidest. (Mathers, 2005, p. 30)

1.2.1 Rahapesu tõkestamine Euroopas

Euroopa Nõukogu Rahapesu ja terrorismi rahastamise vastase võitluse hindamise ekspertide komitee ehk MONEYVAL on jälgimisorganisatsioon, mis koosneb 35 liikmesriigist ja territooriumist. MONEYVAL jälgib rahvusvahelisi rahapesu ja terrorismi rahastamise vastase võitluse standardeid, mis on määratletud FATF-i poolt. MONEYVAL on osa Euroopa Nõukogust, mis on 46 liikmesriigiga valitsustevaheline organisatsioon, mille eesmärk on edendada demokraatiat, inimõigusi ja õigusriigi põhimõtteid. MONEYVAL’i koht Euroopa Nõukogu komitees ja FATF-i sarnase organina tagab selle tugeva institutsionaalse ja rahvusvahelise seisundi rahvusvaheliste organisatsioonide seas, mis osalevad rahapesu ja terrorismi rahastamise vastastes võitluses. MONEYVAL keskendub peamiselt Euroopa riikide hindamisele ning toetamisele rahapesu ja terrorismi rahastamise vastu võitlemisel, samal ajal kui FATF kehtestab rahvusvahelised standardid

ning jälgib nende rakendamist kogu maailmas. Mõlemad organisatsioonid võivad omavahel koostööd teha ja teavet jagada, et tugevdada rahvusvahelist koostööd ning parandada rahapesu ja terrorismi rahastamise vastast võitlust (Council of Europe, 2023, lk 1)

Aastal 2023 avaldas MONEYVAL raporti, mis hindas Eesti efektiivsust rahapesu vastases võitluses. Oma raportis tõi MONEYVAL välja 40 omapoolset soovitusi Eestile. Esimeses soovitusel leiab MONEYVAL, et üleriigilise riskihindamise meetodika rakendamisel ja hindamise tulemustel on olulisi puudujääke ning selleks tuleb edasi arendada strateegilisi analüüse, et täita lüngad riskide mõistmises. Hooldusmeetmetes tuvastatud puudusteks olid näiteks, et kohustust rakendada uusi hooldusmeetmeid olemasolevatele klientidele ei ole kõigil juhtudel ette nähtud. Enamik olulisi kriteeriume olid siiski kas täidetud või enamasti täidetud. Mis puutub kahtlaste tehingute teavitamisse, siis olulised puudused püsivad seoses teatamiskohustusega ja terrorismi rahastamise tegevuste hõlmamisega. (Council of Europe, 2023, lk 220-226, 248-254, 271)

1.2.2 Euroopa Liidu direktiivid

Euroopa Liit on üle kolmekümne aasta rahapesu vastu võidelnud ning esimene rahapesuvastane direktiiv võeti vastu juba 1991. aastal. Alates sellest ajast on direktiivi mitmel korral muudetud ja korrigeeritud. (Euroopa Liidu Nõukogu, 2024b) Nõukogu direktiiviga 91/308/EMÜ defineeriti "rahapesu" mõiste uimastikuritegude kaudu ja kehtestati kohustused finantssektorile. Direktiiviga 2001/97/EÜ laiendati eelneva direktiivi reguleerimisala, hõlmates erinevaid kuritegusid, kutsealasid ja tegevusi. FATF vaatas 2003. aastal läbi oma soovitused, et paremini hõlmata terrorismi rahastamist, lisades detailsemaid nõudeid kliendi isikutuvastusele ja kontrollile. Neid muudatusi võeti arvesse Euroopa Parlamendi ja nõukogu direktiivis 2005/60/EÜ ning komisjoni direktiivis 2006/70/EÜ. (Euroopa Parlament ja Euroopa Liidu nõukogu, 2015) Maailm areneb praegu kiiresti ning samuti leitakse kogu aeg ka erinevaid võimalike viise, kuidas direktiividest ja regulatsioonidest kõrvale hoida mis tähendab, et ka neid peab täiendama ja vastavalt oludele arendama.

Praegusel hetkel lähtutakse rahapesu tõkestamisel Euroopa Parlamendi ja nõukogu direktiivist (EL) 2015/849. Tegemist on neljanda rahapesuohu käsitleva direktiiviga.

Antud direktiivi rakendamisel kaasnevad teatavad andmete kogumise, analüüsimise, säilitamise ja jagamise aspektid. Isikuandmete töötlemine peaks olema lubatud ainult juhul, kui austatakse täielikult kodanike põhiõigusi ning seda tehakse üksnes direktiivis sätestatud eesmärkidel, nagu klientidele hoolsusmeetmete kohaldamine, kahtlaste tehingute jälgimine, uurimine ja nendest teatamine, tegeliku kasusaaja tuvastamine, riikliku taustaga isikute identifitseerimine ning teabe jagamine pädevate asutustega ja kohustuslike osapooltega. Isikuandmete kogumine ja töötlemine peaks piirduma ainult selleks vajalikuga direktiivi nõuete täitmiseks ning neid ei tohiks töödelda lisaks sellistele vajadustele mitteärilistel eesmärkidel. (Euroopa Parlament ja Euroopa Liidu nõukogu, 2015)

Euroopa Parlamendi ja nõukogu direktiivis (EL) 2015/849 on sätestatud kliendi suhtes kohaldatavad hoolsusmeetmed, mis hõlmavad meetmeid kliendisuhete loomisel, juhutehingute tegemisel ja rahapesu kahtluse korral. Üheks oluliseks nõudeks on kliendi tuvastamine ja kontrollimine, milleks pangad ja krediitiasutused peavad läbi viima vajalikud meetmed, et tuvastada kliendi isikut tõendavad dokumendid ning tagada nende õigsus ja usaldusväärsus. Pankadel on kohustus teatada kahtlastest ja ebatavalistest tehingutest, mis võivad viidata rahapesule. Finantsteenuseid pakkuvatel ettevõtetel tuleb rakendada riskipõhist lähenemist, mis tähendab, et nad peavad mõistma rahapesu riske ning võtma vastavalt sellele sobivad meetmed. Liikmesriikidel on võimalus kehtestada erinevaid piiranguid sularaha kasutamisele, rakendada üldisi lisapiiranguid ning kehtestada täiendavaid rangemaid eeskirju. (Euroopa Parlament ja Euroopa Liidu nõukogu, 2015) Antud direktiivis on kehtestatud sularahale teatud nõuded, kuid puudujäägiks on piisavalt ranged piirangud sularahatehingutele ja piisavalt põhjalik jälgimine ja aruandlus sularaha kasutamise kohta.

1.3 Rahapesu tuvastamine ja tõkestamine pankades

Pangad võivad sattuda erinevatesse rahapesuskeemidesse, tulenevalt nende tegevuse spetsiifikast. Ükski pank ei ole täielikult kaitstud riski eest saada osaliseks rahapesuprotsessis. Rahapesu tõkestamise nõuete ebapiisav täitmine võib kaasa tuua sanktsioonid, maine kaotuse ja lõpuks isegi krediitiasutuse litsentsi äravõtmise. Rahapesu tõkestamise eripära seisneb suures koguses analüüsitud andmetes ning ainult

kõrgtehnoloogiliste meetodite kasutamine võimaldab pettuste täpse ja efektiivse jälitamise ning peatamise. (Domashova & Mikhailina, 2021, p. 185). Informatsiooni hankimist raskendab mõnevõrra asjaolu, et finantsasutused jagavad üksteisega harva andmeid oma klientide kohta ning seda peamiselt konfidentsiaalsuse ja spetsiifiliste regulatsioonide tõttu.

Pankade tähtsus sularahaga seotud rahapesu protsessis seisneb selles, et pankasid kuritarvitatakse väga sageli kriminaalsete tegevuste sooritamiseks. Kurjategijate ja rahapesijate jaoks on pankadele juurdepääs äärmiselt oluline, kuna see võimaldab neil kiiresti raha üle kanda teistesse finantsasutustesse, valuutat vahetada ja kuritegelik tulu muuta erinevateks finantsinstrumentideks. See ohustab finantsstabiilsust, eriti pangandussektorit. Pankadel pole alati võimalik sularaha päritolu uurida, mis suurendab nende haavatavust ja rahapesuprotsessi kaasamise ohtu. (Georgieva & Buzlevski, 2021, p. 39) Rahapesu riski tuvastamise esimene samm on välja uurida, milliseid rahapesu riske kliendisuhete loomisel või juhutehingu tegemisel võib tekkida. Pangad peavad kliendisuhete või juhutehinguga seotud rahapesu riskide hindamisel arvesse võtma riskitegureid ning teadma, kes on nende klient ja milliseid konkreetseid tehinguid klient sooritab, sealhulgas tema päritolu ja tehingute iseloom. (Finantsinspeksioon, 2018b, lk 6)

Rahapesu tõkestamise raamistik hõlmab finantstehingute kontrolli nii klientide finants- või krediitiasutuste kui ka paljude teiste teenusepakkujate muude kategooriate kontekstis. Sellised toimingud hõlmavad suure hulga klientide isikuandmete tehnilist töötlemist, sealhulgas kogumist, säilitamist ja vajadusel edastamist, mida võivad kasutada õiguskaitseasutused uurimistes. (Mitsilegas & Vavoula, 2016. p. 279)

Kuritegeliku raha sissevoolu kontrolli tugevdatakse õigusaktide ja nende rakendamisega. Pankade kohustus tuleneb seadusest, mis nõuab rahapesu ja muu kuritegevusest saadud tulu ning terrorismi rahastamise tõkestamise seaduse sätete järgimist, eriti kui tegemist on kahtlaste tehingute tuvastamise ja teatamise kohustusega Rahapesu Andmebüroodele. Finantsasutustel on seaduslik kohustus võtta kasutusele järgmised meetmed ja tegevused rahapesu ning terrorismi rahastamise avastamiseks ja ennetamiseks:

- a) Kliendi põhjalik uurimine
- b) Kindlate ja spetsiifiliste tehingute jälgimine ning teavituskohustus
- c) Andmete kogumine, säilitamine ning tehingute ja neid teostavate klientide kohta seotud informatsiooni edastamine

Kui pangad ei saa mingil põhjusel ülaltoodud meetmeid rakendada, on nad kohustatud keelduma kliendisuhetest, mis tähendab lepingust keeldumist või selle lõpetamist. (Nikolosc & Simonovski, 2012. p. 455-456)

Kliendi põhjalik uurimine ja hoolsusmeetmete rakendamine aitavad tagada, et asutused teavad oma klientide tausta. See välistab kliendisuhete loomist tundmatute isikute või ettevõtetega, kelle tegevusest pank täielikult aru ei saa. Kliendi hoolsusmeetmed hõlmavad klientide tuvastamist, nende isikusamasuse kontrollimist, tegeliku kasusaaja tuvastamist ning muu teabe kogumist. Hoolsusprotseduurid tuleb läbi viia nii uute kliendisuhete loomisel, juhutehingute tegemisel kui ka olemasolevate klientide igapäevaste tehingute suhtes. Asutused peavad omal algatusel teatama rahapesu või terrorismi rahastamise kahtlustest pädevale asutusele, näiteks Rahapesu Andmebüroole. Kahtlased asjaolud võivad hõlmata tehinguid, millel pole selget eesmärki, tehinguid, mis ei vasta kliendiprofiilile või mille struktuur on liigselt keeruline. (Unger, 2013, p. 369-371)

Riigid jälgivad sularahatehingute läbiviimist hoolikalt tõsise sularahatehingute väärkasutuse tõttu. Iga riik peab vastu võtma asjakohased seadused, regulatsioonid ja määrused, mis reguleerivad sularaha hoiustamist, vajalikku dokumentatsiooni, sularaha väljavõtmist, rahvusvahelisi sularahatehinguid, tingimusi, mille kohaselt sularahatehingutest teavitatakse pädevaid asutusi nende töötlemise ja analüüsimise jaoks. (Georgieva & Buzlevski, 2021, p. 40)

Pangad seisavad silmitsi mitmete riskidega. Üheks suureks riskiks on mainerisk, mis võib mõjutada pangandussüsteemi likviidsust, mis omakorda toob kaasa panga nõrgema finantstulemuse. Pangad saavad rahapesu tõkestamisel aktiivselt kaasa lüüa, sest peaaegu kõik finantstehingud käivad läbi pankade. Üheks panga edu toetavaks teguriks on panga turvasüsteem. Seega võib öelda, et just nemad on rahapesu tõkestamisel üks olulisemaid lülisid. (Ilma, *et al.*, 2022, pp. 289). Selles valdkonnas on ülioluline, et õigusaktid käiksid sammu finantsteenuste tehnoloogilise innovatsiooniga, et vältida süsteemi lünkade ebaseaduslikku ärakasutamist. (Silva, 2019, p 59)

Sularahatehingute puhul võib tekkida rahapesukahtlus, kui isik, kellega pole kliendisuhet, teeb üle 10 000 euro suuruse sularahasissemakse teise isiku kontole. Samuti tekitavad kahtlusi tehingud, kus kontole laekunud raha võetakse kiiresti sularahas välja, mis pole kooskõlas isiku tavalise tegevusega. (Rahapesu Andmebüroo, 2022, lk 8) Ebaharilik sularahatehing võib olla suurem kui tavaline tehing või hõlmata väiksemate rahakupüüride

vahetamist suuremate vastu. See sõltub riskipõhisest lähenemisest ja tavapärase tehingutega võrdlemisest. (Rahapesu Andmebüroo, 2022, lk 13) Iga riik peaks seadma piirmäära ületavate sularahatehingute kohta, millest tuleb aru anda. See piirmäär võib olla kehtestatud seaduse või muu õigusaktiga ning peaks olema kõrge, et vältida ebaolulistest tehingutest teatamist, kuid samas piisavalt madal, et hõlmata rahapesuga seotud tehinguid. Enamikus Euroopa riikides on see piirmäär 15 000 eurot. (Georgieva & Buzlevski, 2021, p. 40) Eesti on kaetud sularahautomaatide ja kassasüsteemide võrgustikuga, mis tagab suurele osale elanikkonnast mugava juurdepääsu sularahale. Eesti krediidasutused on tugevdanud hoolsusmeetmeid ja loobunud kahtlasi sularahatehinguid tegevatest klientidest. (Rahapesu Andmebüroo, 2023b, lk 3-6)

Pangandussektoris on oluline mõista klientide finantsteenuste kasutamise tavasid. Arvelduskonto puhul on oluline jälgida tehtavate tehingute sagedust, eesmärki, sihtriike, sularahakasutust ja maksete teostamise kanaleid nagu kontor, internetipank ja kaardimaksed. (Finantsinspeksioon, 2018a, lk 48) Tänu Eesti arenenud ja suurele sularahavõrgustikule on sularaha sisse- ja väljamaksed inimestele kergeks ja kättesaadavaks tehtud. Praegusel hetkel on võimalik sularaha lisaks pangakontoritele ja sularahautomaatidele kätte saada ka mõne toidupoe kassast.

Põhjalik klientide uurimine ja hoolsusmeetmete rakendamine tagavad, et pangad on kursis klientide taustaga ning väldivad suhteid tundmatute isikute või ettevõtetega. Riigid jälgivad hoolikalt sularahatehinguid, et välistada nende väärkasutus. Eesti arenenud sularahavõrgustik teeb sularaha hõlpsasti kättesaadavaks kõigile ning seetõttu on oluline, et õigusaktid ja finantsteenuste tehnoloogiline innovatsioon käiksid käsikäes, tagamaks süsteemi turvalisus ja vältides ebaseaduslikku ärakasutamist.

1.3.1 Eestis kehtivad rahapesuvastase võitluse reeglid ja asutuste roll

Eestis reguleerib rahapesu ja terrorismi rahastamist Rahapesu ja terrorismi rahastamise tõkestamise seadus (RahaPTS), mille eesmärk on suurendada ettevõtluskeskkonna usaldusväarsust ja läbipaistvust ning takistada Eesti rahandussüsteemi ja majandusruumi kasutamist rahapesuks ja terrorismi rahastamiseks. Seadus käsitleb rahapesu ja terrorismi rahastamisega seotud riskide juhtimist, hindamist ja maandamist ning määratleb Rahapesu Andmebüroo tegevuse alused. See kehtib krediidasutuste, finantseerimisasutuste,

hasartmängukorraldajate ja kinnisvara vahendajate suhtes. (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2023) Eesti Pank rakendab Rahapesu ja terrorismi rahastamise tõkestamise seaduse § 20 lõike 1 punktides 1-5 määratletud hoolsusmeetmeid, mis nõuavad kohustatud isikutelt klientide isikusamasuse kindlakstegemist ja esitatud teabe kontrollimist, tegeliku kasusaaja tuvastamist ning juhtehingute mõistmist ja täiendava teabe kogumist. Samuti peab olema teada, kas isik või tema pereliige on riikliku taustaga isik. (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017, § 20)

Eestis tegutseb mitmeid organisatsioone, mis võitlevad rahapesuga. Rahapesu Andmebüroo kogub kahtlaste tehingute kohta teavet ja edastab selle uurimisasutustele. Kurjategijate avastamise ja karistamisega tegelevad prokuratuur, Kaitsepolitsei, Maksu- ja Tolliamet ning Eesti kohtud. Finantsinspeksioon tagab Eesti finantssektori läbipaistvuse ja teostab turujärelevalvet, et hoida ära rahapesu ja terrorismi rahastamist. Rahandusministri juhitud rahapesu tõkestamise alane valitsuskomisjon koosneb mitme ministeeriumi, prokuratuuri, Eesti Panga, Maksu- ja Tolliameti, politseiasutuste ja Finantsinspeksiooni esindajatest, ning selle eesmärk on edendada rahapesu ja terrorismivastast võitlust. (Rahandusministeerium, 2023). Rahapesu Andmebüroo asutati 1. juulil 1999 Politseiameti struktuuriüksusena ning alates 1. jaanuarist 2021 kuulub see Rahandusministeeriumi haldusalasse. Rahapesu Andmebüroo peamine eesmärk on tõkestada rahapesu ja terrorismi Eestis, analüüsides ja kontrollides kahtlusi nende kuritegude osas. (Rahapesu Andmebüroo, 2023). Nende ülesanne on vastu võtta, koguda, registreerida, töödelda, analüüsida ja edastada rahapesule või terrorismile viitavat teavet. (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2023)

1.3.2 Pankade I ja II kaitseliin

Pankade I kaitseliin vastutab klientide ja nende tegevuse mõistmise eest ning peab hindama nendega seotud riske. Eesmärgiks on avastada kliendi tegevuses kahtlaseid või ebatavalisi tehinguid või tehinguid, mis ei vasta mõistlikule majanduslikule eesmärgile ning suunata need edasiseks analüüsiks II kaitseliinile. (Rahapesu Andmebüroo, 2022, lk 13) I kaitseliin ei tegele riskide erakorralise juhtimise ega kahtlaste ja ebatavalike tehingute analüüsiga vastavalt funktsioonide lahususe põhimõttele. I kaitseliin edastab kahtlased või ebatavalised asjaolud ja tehingud II kaitseliinile riskide haldamiseks ja edasiste otsuste

tegemiseks. (Finantsinspeksioon, 2018b, lk 14) I kaitseliin koosneb klienditeenindusega seotud üksustest, tavaliselt pangatöötajatest ja spetsialistidest, kes on otseses kontaktis klientidega ja vastutavad esmase suhtluse eest. Nende ülesanded hõlmavad klientide tuvastamist, suhte eesmärgi mõistmist ning riskide hindamist, järgides rahapesu tõkestamise õigusakte ja protseduure. (International Finance Corporation, 2019, p. 11) I kaitseliini kuuluvad näiteks panga tellerid, erinevad kliendihaldurid ja KYC spetsialistid. I kaitseliini töötajatel on protsessis väga suur roll, sest nemad on esimesed, kes kliendiga suhtlevad, identifitseerivad ning kahtlaste tehingute puhul II kaitseliini teavitavad.

Pankade II kaitseliin hõlmab vastavuskontrolli ja riskijuhtimise funktsiooni. Vastavuskontrolli eesmärk on tagada, et pank järgib kehtivaid õigusakte, juhiseid ja dokumentatsiooni ning hinnata nende mõju panga tegevusele. Vastavuskontroll aitab I kaitseliinil tuvastada riskikohad ja nende tõhusat juhtimist. (Finantsinspeksioon, 2018a, lk 14-15) Vastavuskontrolli süsteemi osana töötab tavaliselt pangas Rahapesu Andmebüroo kontaktisik. Tema ülesanne on koguda, analüüsida ja edastada Rahapesu Andmebüroole teavet ebatavaliste tehingute või rahapesukahtluste kohta, mis ilmnevad pangas. (Rahapesu Andmebüroo, 2022, lk 14-15)

1.4 Sularahaga seotud rahapesu hoolsusmeetmete rakendamine pankades

1.4.1 Sularaha ja rahapesu

Kuigi sularahal on mitmeid legitiimseid funktsioone, on selle kasutamisega seotud andmed ja statistika piiratud. Enamik ringluses olevatest pangatähtedest on suure nimiväärtusega. Õiguskaitseorganid on teadlikud kurjategijate sularaha kasutamisest ja on kehtestanud meetmeid selle riskide maandamiseks, eriti suure nimiväärtusega sularaha ja füüsilise sularaha liikumise osas. Ehkki täpset statistikat selle kohta, kui suur osa sularahast on seotud kuritegeliku tegevusega, pole, näitavad uurimused, et kurjategijad kasutavad sageli sularaha rahapesuks. Europolile esitatud teave rõhutab sularaha olulist rolli rahapesu valdkonnas ja sularaha tuvastamise aruanded moodustavad olulise osa rahapesu vastase võitluse jõupingutustest. (Europol, 2015, lk 11-16)

Hädaolukorra seaduse § 36 kohaselt kuulub sularaharinglus elutähtsate teenuste loetelusse. (Hädaolukorra seadus, 2017) Sularahal on tänapäeva digitaalses maailmas endiselt oluline

roll. See tagab majanduse toimimise, kuna inimestel peab olema juurdepääs sularahale. Paberraha ja mündid on ainus maksevahend, mida saab hoida kättesaamatuna kolmandate osapoolte eest. Sularahaga saab tehinguid teha kiirelt ja ilma internetiühenduseta ning see on eelistatud valik sotsiaalselt haavatavatele rühmadele, nagu vanemaealised. Lisaks peetakse sularaha turvalisemaks võrreldes digitaalsete makseviisidega, kuna sellega seostatakse vähem küberkuritegevust ja pettusi. (Euroopa Keskpank) Sularahatehinguteks loetakse sularaha sisse- ja väljamakseid pangakontorites, sularahaautomaatides ja poodides, valuutavahetust ning ostu-müügitehinguid, mis toimuvad käest kätte sularahas.

Sularaha kasutatakse tavaliselt rahapesu paigutamisetapis. Peaaegu kõik kuritegevuse liigid kasutavad sularaha rahapesu hõlbustamiseks. Hoolimata kuritegevuse kiirest arengust ja küberkuritegevuse, veebipettuste ja ebaseaduslike veebiturgude kasvust, on rahapesumeetodid valdavalt traditsioonilised ning sularaha on endiselt üks levinumaid rahapesu soodustavaid tegureid peaaegu kõigis kuritegudes. Sularaha võimaldab varjata vara päritolu ja selle üle puudub kontroll. See kuulub isikule, kes seda parasjagu valdab. (Europol, 2015, lk 9) Sularahatehingud võivad olla anonüümsed, erinevalt elektroonilistest tehingutest, mis raskendab rahapesu ning muu ebaseadusliku tegevuse tuvastamist.

Anonüümsust sularahatehingute puhul aitavad tagada ka rahamuulad ja variisikud. Rahamuulad on isikud, kes on värvatud kuritegelikul teel saadud rahaliste vahendite liigutamiseks kontode vahel. (Euroopa Liidu Nõukogu, 2024) Muulad ei pruugi alati teadvustada, et nad osalevad pettusskeemis. Rahamuul saab kolmandalt isikult raha oma pangakontole ja seejärel kannab selle edasi või võtab sularahas välja, andes selle kellelegi teisele ning saades vastutasuks rahalist tasu. Kuigi rahamuulad ei pruugi olla otseselt seotud raha päritolu kriminaalsete tegevustega, on nad siiski osalised, kuna nad aitavad puhtaks pesta tulu, mis on saadud kriminaalsetest tegevustest. Muulad on rahapesijatele atraktiivne viis jääda anonüümseks. (Europol, 2023) Variisik on eraisik või juriidiline isik, kes tegutseb teise isiku või ettevõtte nimel, varjates tegelikku omanikku ning huve. Tihipeale kasutatakse variisikuid kahtlaste või ebaseaduslike tehingute tegemiseks.

Enamasti tasutakse rahamuuladele 5% summast, mis tähendab seda, et kui nad on nõus 10 000 eurot oma konto kaudu üle kandma ning hiljem sularahas välja võtma, siis on nende tasu tehtud töö eest 500 eurot. Tagamaks, et rahamuul raha ei varastaks, ei teosta paljudel juhtudel sularaha väljamakset muul vaid hoopis kolmas isik. (Custers, *et al.*, 2019, pp. 735-736) Rahamuulade ja variisikute kontod toimivad transiitkontodena. Transiitkonto

tähendab seda, et vahendid laekuvad kontole ning liiguvad sealt kohe edasi. See võib toimida nii rahvusvaheliste kui ka riigisiseste tehingute korral. (Politsei- ja piirivalveamet, 2019, lk 9)

1.4.2 Sularahatehingute kontroll pankades

Finantsasutused peavad hoolikalt uurima kõikide keerukate, ebatavaliste ja suuremahuliste sularahatehingute tausta ja eesmärki. See hõlmab ka ebatavaliste tehinguskeemide tuvastamist, millel võib puududa selge majanduslik või seaduslik alus. Oluline on saada kliendilt täiendavat teavet, näiteks nende amet ja muu avalikustatud teave. Eriti oluline on teabe hankimine kliendi rahaliste vahendite ja vara päritolu kohta. (FATF, 2012, lk 71) Oluline on see sellepärast, et kliendi vara päritolu tundmine, selle tõendamine ning sellest aru saamine annab pangale ülevaate kliendi vara algallikast ning see omakorda laseb välistada kuritegevuslikul teel saadud tulu.

On olemas tugev õiguslik raamistik, mis võimaldab kuritegelikul teel saadud vahendite ja tulu külmutamist, arestimist ja konfiskeerimist, samuti samaväärse väärtuse konfiskeerimist ning laiendatud konfiskeerimist. On mõningaid tehnilisi puudusi sularaha liikumise jälgimisel. (Council of Europe, 2022, lk 9) Tehingute järelanalüüsi nimetatakse monitooringuks. Selles jälgivad pangatöötajad kliendi käitumist ja tehinguid, et avastada olukordi, mis võivad jääda esialgselt reaalses sekkumisest välja, näiteks tehingud sularahaautomaatide kaudu. (Finantsinspeksioon, 2018a, lk 53) Kuigi kaasaegne tehnoloogia kogub hoogu ja uusi rahakandmise tehnikaid turundatakse igapäevaselt, tuginevad mitmed riigid endiselt oma põhilistele rahapesu ennetamise strateegiatele sularahatehingute puhul. (Georgieva & Buzlevski, 2021, p. 39)

Nagu eelnevalt nimetatud, on monitooring protsess, kus pangatöötajad uurivad tehinguid, mida ei olnud võimalik tuvastada ja millesse sekkuda reaalses ehk töötajad teostavad tehingutele hilisemat analüüsi. Monitooringus valitakse tehinguid erinevate parameetrite alusel, näiteks perioodi suurimate tehingute ja sularahaautomaatides tehtud piirmäära ületavate väljavõtmiste ja sissemaksete järgi. (Finantsinspeksioon, 2018a, lk 54) Skriinimine on tehingute jälgimine reaalses vastupidiselt monitooringule. See hõlmab keerukate, suure väärtusega ja ebatavaliste tehingute jälgimist, mis ei ole mõistlikud või ilmsed majandusliku või õiguspärase eesmärgiga või ei ole iseloomulikud konkreetsele

kliendile. Skriinimisel jälgivad pangatöötajad klientide tehinguid reaalsajas, et avastada kahtlased või ebatavalised tehingud, mis võivad ületada piirmäärasid. (Finantsinspektsioon, 2018a, lk 51-52) Eestis kehtib sularahatehingute piirmäär 32 000 eurot. Pank peab esitama sularahateate, kui see summa ületatakse, olenemata tehingu osade arvust või nende vahelistest seostest, ning teavitama sellest Rahapesu Andmebürood. (Rahapesu Andmebüroo, 2022, lk 4-5)

Sularahatehingute kontrollimiseks kasutatavad hoolsusmeetmed on sarnased ülekannete kontrollimisel kasutatavatega. Need hõlmavad kliendi tuvastamist, riskiprofiili määramist ja isikutuvastuse kontrollimist, mis nõuab tavaliselt näost-näkku kohtumist ja identifitseerimisdokumentide esitamist. Pärast kliendi tuvastamist määratakse vajalik hoolsusmeetmete tase vastavalt riskitasemele: madal, keskmine, kõrge või ülikõrge. Kui ilmnevad kahtlased või ebatavalised asjaolud, teeb pank vastava teatise. (Signicat, 2023) Pangad jälgivad ja skriinivad klientide sularahatehinguid suhte kestel ning reageerivad kiiresti kahtluste või ohumärkide ilmnemisel, võttes vastavaid meetmeid. See tõhustab pangasisest järelevalvet ja aitab ennetada rahapesu ning muid ebaseaduslikke tegevusi.

Sularahatehingud võimaldavad anonüümsust, erinevalt elektroonilistest tehingutest, mis raskendab rahapesu ja muu ebaseadusliku tegevuse avastamist. Lisaks esineb sularahatehingute jälgimisel tehnilisi puudusi, kuna paljudesse tehingutesse ei saa reaalsajas sekkuda. Õigusaktid sularahatehingutele muutuvad sageli ja on keerulised, nõudes pangandussektorilt pidevat tähelepanu ja kohanemisvõimet. Seega seisavad pangad silmitsi mitmete väljakutsetega sularahatehingute jälgimisel, mis nõuavad pidevat tähelepanu ning täiustatud süsteeme rahapesu ja muu ebaseadusliku tegevuse tõkestamiseks.

1.4.3 Riskipõhine lähenemine

Riskipõhine lähenemine tähendab, et riigid, pädevad asutused ja pangad tuvastavad, hindavad ja mõistavad rahapesu ja terrorismi rahastamise riske, millega nad kokku puutuvad, ning võtavad vastavalt riskitasemele sobivaid riski maandamise meetmeid. Selline paindlikkus võimaldab ressursse tõhusamalt kasutada, kuna pangad, riigid ja pädevad asutused saavad otsustada, milline on kõige efektiivsem viis nende tuvastatud rahapesu ja terrorismi rahastamise riskide maandamiseks. See võimaldab neil suunata oma ressursse ja rakendada tugevdatud meetmeid olukordades, kus riskid on suuremad, ning

kasutada lihtsustatud meetmeid, kui riskid on väiksemad. Riskianalüüs on pangas riskipõhise lähenemise alus. See peaks võimaldama pangal mõista, millises ulatuses ja kuidas ta on vastuvõtlik rahapesule ja terrorismi rahastamisele. Selle tulemuseks on sageli riskide kategoriseerimine, mis aitab pankadel määrata selle riski maandamiseks vajalike rahapesu ja terrorismi rahastamise ressurside taseme. See tuleks alati korralikult dokumenteerida, hoiustada ja panga vastavatele töötajatele edastada. (FATF, 2014, p 17)

Riskipõhise lähenemise kasutuselevõtt rahapesu tõkestamisel tähendab, et kliente hinnatakse riskitaseme alusel muutujatega nagu näiteks geograafiline risk, kliendirisk ja toote- või teenuse riski, mis võivad suurendada või vähendada konkreetse kliendi või tehinguga kaasnevat tajutavat riski. Rahapesu ja terrorismi rahastamise tõkestamise seaduse § 13 tuleb välja, et kohustatud isikud hindavad, analüüsivad ja tuvastavad rahapesu ja terrorismi rahastamise riske, koostades riskihinnangu, mis hõlmab vähemalt järgmisi riskikategooriaid: (Rahapesu ja terrorismi rahastamise tõkestamise seadus, 2017, § 13)

- 1) Klientidega seonduv risk;
- 2) Riikide või geograafiliste piirkondade või jurisdiktsioonidega seonduv risk;
- 3) Toodete, teenuste või tehingute seonduv risk;
- 4) Kohustatud isiku ja klientide vaheliste suhtlus- või vahenduskanalitega või toodete, teenuste või tehingute edastamiskanalitega seonduv risk.

Kliendiga seotud riskide hindamisel tuleb järgida "tunne oma klienti" põhimõtet. See tähendab, et kliendi riskiprofiili määramisel kasutatakse kogutud informatsiooni. Seadus ei anna konkreetseid juhiseid selle kohta, kuidas kliendid jaotada erinevatesse kategooriatesse või millised tunnused peavad neil kategooriatel olema ning seega on see peamiselt kohustatud isiku enda otsus. Soovituslikult võiks klientide riskitasemed jaotada kolmeks: väikese, tavapärase ja suure riskiga klientideks. (Rahapesu Andmebüroo, 2018, lk 6)

Finantsasutused kasutavad klientide riskihindamise mudeleid rahapesu avastamiseks. Enamik tänapäeva mudelitest põhineb riskitegurite hindamisel, nagu kliendi ametikoht, sissetulek ja pangatooted. Kuigi teave kogutakse konto avamisel, uuendatakse seda harva. Antud sisendeid koos kaaludega kasutatakse riskihinde skoori arvutamiseks. Siiski on hinded tuntud oma ebatäpsuse poolest, kuna mitte ainult ei suuda nad tuvastada mõnda kõrge riskiga klienti, vaid sageli klassifitseeritakse ekslikult tuhandeid madala riskiga klientid kõrge riskiga klientideks. (Mikkelsen, *et al.*, 2019, lk 2) See sunnib asutusi läbi vaatama liiga palju juhtumeid, suurendades nende kulusid ja ärritades madala riskiga

kliehte täiendava järelevalvega. See vähendab rahapesu tõkestamise tõhusust, kuna ressursid suunatakse valele alale. (Rahapesu Andmebüroo, 2022, lk 23-24)

Geograafilised riskid on seotud kliendi, pakutava toote ja teenusega ning hõlmavad erikohustusega isiku asukohariigi riske, samuti selle riigi ja sanktsioonide subjekti geograafilisi, kultuurilisi ja ajaloolisi riske. Tuleb arvestada ka olukordadega, kus tehingud on seotud kõrge sanktsiooniriskiga riikide või piirkondadega ning riikidega, mille kaudu võidakse sanktsioonidest kõrvale hoida. (Finantsinspeksioon, 2021, lk 7) Väike geograafiline risk tähendab, et tegemist on Euroopa Majanduspiirkonna lepinguriigiga või kolmanda riigiga, kus on tõhusad rahapesu ja terrorismi rahastamise tõkestamise süsteemid ning korrupsiooni ja muu kuritegevuse tase on. Suur geograafiline risk viitab piirkondadele, kus on järelevalveasutuste poolt tuvastatud kõrgendatud rahapesu ja terrorismi rahastamise risk. (Rahapesu Andmebüroo, 2018, lk 7-8) Eesti on kurjategijatele atraktiivne tänu geograafilisele asukohale, venekeelsete pangateenuste kättesaadavusele, suurele pangandussektorile ja kiiretele rahaülekannetele. (Eesti pangaliit, lk 2-3)

Pankade jaoks on oluline tagada, et sularaha sissemakseid tehes vastaks klient nende võimekusele ning et vahendite päritolu oleks teada. Riskid tekivad, kui sularaha sissemakse ületab kliendi tavapärasest võimekusest või kui raha päritolu ei ole teada või on ebaharilik. (Finantsinspeksioon, 2018, lk 75) Arvelduskontolt sularaha väljavõtmisel on oluline risk, kui klient võtab raha välja kõrgema rahapesu ja terrorismitasemega riikides või nende naaberriikides. Samuti tuleb arvestada klientide võimekust selliseid tehinguid teha. Risk tekib, kui väljavõetav summa ületab kliendi võimekust või kui tegu on ebahariliku tegevusega. (Finantsinspeksioon, 2018, lk 83)

Oma kliendi vara päritolu mõistmiseks on pankadel õigus küsida selle kohta selgitusi. Pank peab mõistma, kuidas klient on teeninud olemasoleva vara ning vajadusel selgitama, kust on pärit konkreetse tehingu jaoks kasutatavad vahendid. Rahapesu ja terrorismi rahastamise tõkestamise seaduse § 43 lg 1-s on sätestatud, et kohustatud isikul on õigus tehingu tegemine edasi lükata, kuni tehingus või ametitöingus osalev isik, ametiteenust kasutav isik või klient on esitanud hoolsusmeetmete rakendamiseks, sealhulgas tehingu objektiks oleva vara päritolu tõendamiseks või ärisuhte seireks, vajalikud dokumendid ja teabe. Vara päritolu välja selgitamise kohustus kehtib nii sularahatehingute kui ka ülekannete puhul.

1.4.4 Tunne oma klienti põhimõte

"Tunne oma klienti" (inglise keeles "Know Your Customer" ehk lühendatult KYC) on hoolsuskohustus ja pangaregulatsioon, mida finantsasutused ja muud reguleeritud ettevõtted peavad järgima, et tuvastada kliente ja koguda nende finantstehingutega seotud olulist teavet. (Rajput, 2013, p. 1) Rahapesuvastased seadused nõuavad, et ettevõtte, kes töötlevad suuri rahasummasid, teataksid ametiasutustele kõigist kahtlastest tehingutest. Peamine nõue on teha iga uue kliendi kohta KYC kontrollid. Kui spetsialistid avastavad ebatavalist käitumist kliendi konto või rahaliste vahenditega seoses, peavad nad esitama aruande seadusjärgsele asutusele, kes otsustab edasised sammud. Piisav KYC teave ja jälgimine võimaldavad spetsialistidel otsustada, kas tehing on kahtlane, ning täita aruandluskohustusi. (Doughty, 2005, p 249)

Kliendi KYC-protsessi käigus kogutavad andmed võivad erineda sõltuvalt finantsasutusest, kohaldatavatest eeskirjadest ja kliendisuhtlusest tulenevatest riskidest. See hõlmab isikut tõendava dokumendi kasutamist, et kontrollida sanktsioonide või riiklike taustaga isikute (*Politically Exposed Person* ehk PEP) kuulumist ning võib sisaldada ka kliendi tegevuste jälgimist ärisuhte ajal, et tuvastada finantskuritegude riske. (Moreno, *et al.*, 2021, lk 4) Arvestades Eestile omaseid riske, on oluline, et pangandussektoris oleksid selged suunised klientide valikul ning klientide pidev jälgimine ja hoolsusmeetmete rakendamine kogu ärisuhte kestel. (Eesti Pangaliit, lk 2)

2. SULARAHATEHINGUTE RAHAPESUVASTASTE HOOLSUSMEETMETE RAKENDAMINE PANGAS

2.1 Uurimismeetodi kirjeldus

Lõputöö eesmärk on välja selgitada, millised probleemid ilmnevad sularahaga seotud rahapesu tõkestamise hoolsusmeetmete rakendamisel pangandussektoris, mis tähendab rakendatud meetmete kirjendamist pangandussektoris ja puudujääkide tuvastamist. Samuti on oluline aru saada, milliste puuduste või probleemidega seisavad pangad praegu silmitsi ning mis aitaks töötajate arvates antud probleeme lahendada.

Lõputöö eesmärgi saavutamiseks kasutatakse kvantitatiivset uurimismetoodikat. Kvantitatiivne meetod valiti seetõttu, et see meetod võimaldab efektiivselt töödelda suuri andmemahte ning tulemusi väljendatakse numbriliste andmetena. (Hirsjärvi, et al., 2007, lk 130) Autor kasutab andmete analüüsi jaoks kirjeldavat statistikat, et korrastada ja kokku võtta kogutud andmeid, mis seejärel esitatakse visuaalselt diagrammidena. (Holcomb, 2017, p. 2) Andmete kogumiseks kasutatakse ankeetküsitlust. Küsitluses esineb nii avatud kui ka suletud küsimusi, mis tähendab seda, et suletud küsimuste puhul on vastajale ette antud autori koostatud vastusevariandid, aga avatud vastuse puhul saab vastaja oma sõnadega vastata. (Beilmann, 2020) Ankeetküsitluse valikul on oluline kaalutlus, kuna see tagab vastajate anonüümsuse, see on vastajate jaoks mugav ning see on üks kiiremaid andmete kogumise viise. Vastajate aktiivne osalus ja nende antud vastused on äärmiselt olulised, sest nende põhjal viiakse läbi analüüs ning seejärel pakutakse välja võimalikud lahendused. Vastajate mitmekesisus ja ulatuslik kogum andmeid aitavad paremini mõista uuritava teema või probleemi olemust ning toetavad tõhusate lahenduste väljatöötamist.

Küsitlus viiakse läbi ühes Eesti pangas, mis vastab elutähtsa teenuse osutaja tingimustele ning küsitletakse antud panga kolme erineva osakonna töötajaid. Hädaolukorra seaduse järgi on sularaharinglus ja makseteenused elutähtsad teenused. Hetkel pakuvad elutähtsat teenust pankadeks Eestis Swedbank AS, AS SEB Pank, Luminor Bank AS, AS LHV Pank ja Coop Pank AS. (Eesti Pank, 2023.) Küsitlus viiakse läbi ainult ühes pangas ning küsitletakse kolme erinevat osakonda, kellel kõigil on oma osa sularahaga seotud rahapesu tõkestamisel. Küsitluses osales I kaitseliin ehk tellerid ja KYC osakond ning II kaitseliin ehk AML osakond. Autor otsustas uurida panga erinevaid osakondi, sest iga osakond täidab

erinevad eesmärgi ning samuti on töötajatel ka erinev arusaam antud olukorrast ning võimalikest lahendustest. Kuna küsitlus viidi läbi ainult ühe panga erinevates osakondades, siis panga huvides ei kuulu nimi avalikustamisele.

Küsitluse läbiviimiseks koostas autor kolm erinevat veebipõhist küsimustikku Google'i vormid veebikeskkonda. Tegemist on vastajate jaoks kõige mugavama ja lihtsama võimalusega, sest antud keskkond tagab vastaja anonüümsuse, küsimustele on kerge vastata ning vastustest loob keskkond ise ülevaate diagrammidena, mis teeb analüüsi mugavaks ja kiiremaks. Tellerite hulgas said võimaluse küsitluses osaleda kõikide pangakontorite tellerid, kes tegelevad igapäevaselt oma töös sularahaga. Valimist jäid välja tellerid, kes töötavad pangakontorites, kus ei ole võimalik teha sularahatehinguid. Küsitlusankeet saadeti 15 tellerit, kellest vastas 9 töötajat. KYC ja AML osakonna puhul said võimaluse küsitluses osaleda kõik töötajad. KYC tiimist saadeti ankeet viiele töötajale, kellest vastas kolm ning AML tiimist saadeti ankeet kuuele töötajale, kellest vastas neli töötajat. Autor otsustas oma töös kasutada kõikset valimit, kuna osakondade arv on piisavalt väike, võimaldades kõiki neid põhjalikult uurida. (Babbie, 2010, p. 128)

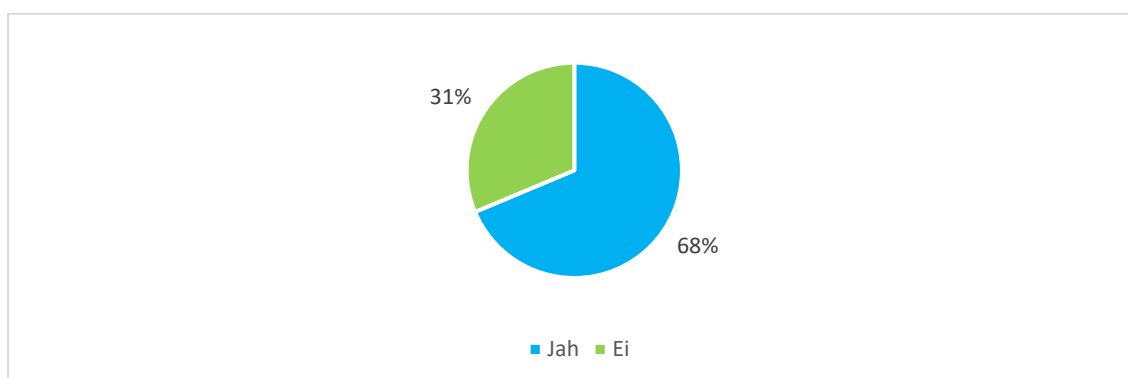
Autor esitas osakondadele kokku erineva arvu küsimusi: telleritele 9 küsimust (vt lisa 1), KYC osakonnale 10 küsimust (vt lisa 2), AML osakonnale 10 küsimust (vt lisa 3). Küsitluses esineb küsimusi, mis on kõikidel osakondadel samad, et hinnata osakondade arvamust kui ka kõikide küsitletavate osakondade arvamust üldiselt. Küsitlused edastati osakondadele 12.03.2024 ning küsitlustele oli võimalik vastata perioodil 12.03.2024-15.03.2024. Küsimustikud hõlmavad küsimusi sularahatehingute kohta: millised on probleemkohad, mis on töötajate jaoks praegu kõige keerulisem, kuidas kliendid koostööd teevad, mida kasutavad töötajad andmete kontrolli ja mida saaks veel praeguses süsteemis parandada. Esmalt saadeti küsimustik testimiseks iga osakonna ühele töötajale. Iga osakonna testija täitis küsitluse ning oli olemas heakskiit, et küsitlus sobib osakonnale saatmiseks.

2.2 Pangandussektori sularahaga seotud hoolsusmeetmete täitmine

Küsitlus viidi läbi ühe panga kolmes erinevas osakonnas, kes kõik tegelevad sularahaga seotud rahapesu tõkestamise hoolsusmeetmete rakendamisega. Tellerid on pangas esimesed, kes puutuvad kliendiga kokku näost-näkku ning seetõttu on nende roll väga

oluline. Tellerid võivad ühtlasi küsida täiendavaid küsimusi suuremate sularahatehingute korral või tuvastada klientide kahtlased või ebatavalised tehingud. KYC osakond vastutab kliendi tausta eest. Osakonna töötajad koguvad klientide kohta käivaid dokumente ning teostavad selle põhjal analüüsi. AML osakond tegeleb omakorda sügavama analüüsi ja uurimistööga seoses kahtlaste tehingute või klientidega. Nende ülesanne on jälgida ja analüüsida suurt hulka andmeid, et tuvastada võimalikke rahapesu juhtumeid ning teha vajadusel teha koostööd vastavate ametiasutustega. Kõik kolm osakonda on ühiselt seotud sularahaga seotud rahapesu tõkestamise meetmete rakendamisega, et tagada pangandussüsteemi terviklikkus ja klientide usaldusväarsus.

Esimene ühine küsimus, mis esitati kõikidele osakondadele ühesugusena, oli töötajate oma arvamus selle kohta, kas nende arvates on Eesti pankadel praegusel hetkel piisav võimekus teostada sularahatehingute kontrolli, et vähendada rahapesu ning sellega kaasnevat risk. Kõikidest vastajatest 68,8% arvas, et pankade võimekus praegu on piisav ning 31,3% arvas, et tegelikult seda võimekust pankadel praegu ei ole.



Joonis 1. Võimekus teostada sularahatehingute kontrolli (autori koostatud)

Võrreldes osakondi eraldi, siis telleritest arvas 88,9%, et hetkel on võimekus piisav ning 11,1% arvas, et võimekus ei ole hetkel piisav. KYC osakonnast arvas 66,7%, et võimekus on piisav ning 33,3% arvas, et võimekus ei ole piisav. AML osakonnas jagunesid arvamused pooleks, 50% arvas, et praegusel hetkel on Eesti pankadel piisav võimekus teostada sularahatehingute kontrolli ning 50% arvas, et piisavat võimekust ei ole.

Teine küsimus oli osakondadel samuti samasugune. Küsimuses paluti eelnevas küsimuses „ei“ vastanutel oma seisukohta põhjendada. Vastustes toodi välja, et tänase päeva seisuga on meie turul palju maksevahendajaid, kes pakuvad võimalust teostada sularaha sissemaksid ning hiljem, kui soovitakse vahendid edasi kanda pankka, siis on vara algse

päritolu kontrollimine raskendatud ning keeruline või aeganõudvam. Veel toodi välja ka erinevad ja uued petuskeemid, mille korral ei jõua pangad piisavalt kiiresti reageerida. Ühe takistusena toodi välja ka regulatsioonid, mis takistavad pankadevahelist infovahetust. Mõned vastanutest arvasid aga, et pangad peaksid oma kliente rohkem monitoorima, et tuleksid välja ka asjad, mis skriiningu käigus välja ei tulnud.

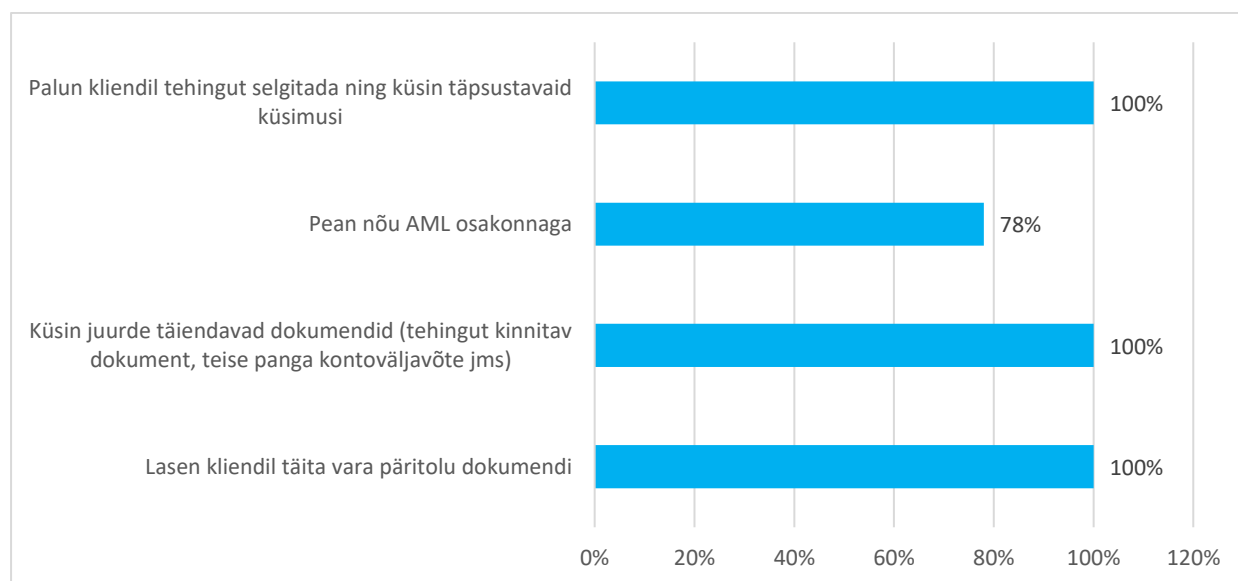
Küsimus, mis oli kõikidele osakondadele veel samasugune, on küsimus variisiku kohta ning kuidas tuvastatakse, et tegemist on variisikuga. Telleritel on antud küsimus järjestuses eelviimane ehk kaheksas, KYC osakonnal oli samuti eelviimane kuid üheksas ning AML osakonnal oli küsimus kaheksas. KYC osakonnal ja AML osakonnal, kes kliendiga näost näkku ei kohtu, oli kõige levinum vastus, et kui klient hakkab tegema tehinguid, mida ta varasemalt sooritanud ei ole. Teine kõige levinum vastus antud osakondade seas oli, et variisiku kahtlus võib tekkida analüüsi ja hoolsusmeetmete rakendamise käigus, kui kliendile esitatakse päringuid, küsimusi, teostatakse ülevaade ja analüüs ning luuakse seosesid teiste isikutega. Vastustest tuli ka välja, et transiitkonto tunnused võivad tekitada variisiku kahtluse. Transiitkonto tähendab seda, et vahendid tulevad kliendi kontole ning liiguvad sealt kohe edasi. Vahendid võivad tulla või minna välisriigi kontole, aga tegemist võib olla ka riigisiseste kontode vahel toimuvate kannetega. (Politsei- ja piirivalveamet, 2019, lk 9) Tellerite vastustes oli põhiliseks kliendi käitumine, kuna nemad näevad ainsana antud osakondadest klienti näost-näkku. Kahtlus tekib tavaliselt, kui klient ei käitu tavapäraselt, mis tähendab, et tekib tunne nagu klienti justkui juhendatakse. See võib tekkida siis, kui klient vestluse ajal telleriga vestleb kellegagi samal ajal telefonis ning kannab vestlusest ette või toimub kirjavahetus telefonis. Veel tekitab kahtlust, kui klient ei oska vara päritolu selgitada, klient on hirmul või segaduses.

2.2.1 Küsimused I kaitseliinile

Tellerid on I kaitseliin. Telleritel on võimalus saada esmane kontakt kliendiga ning enamasti toimub see näost-näkku. Küsimused, mis telleritele esitati, hõlmasid sularaha päritolu selgitamist, dokumentide tõelisuse hindamist, klientide koostöövalmidust, variisiku kahtlust ja koostöö teiste osakondadega.

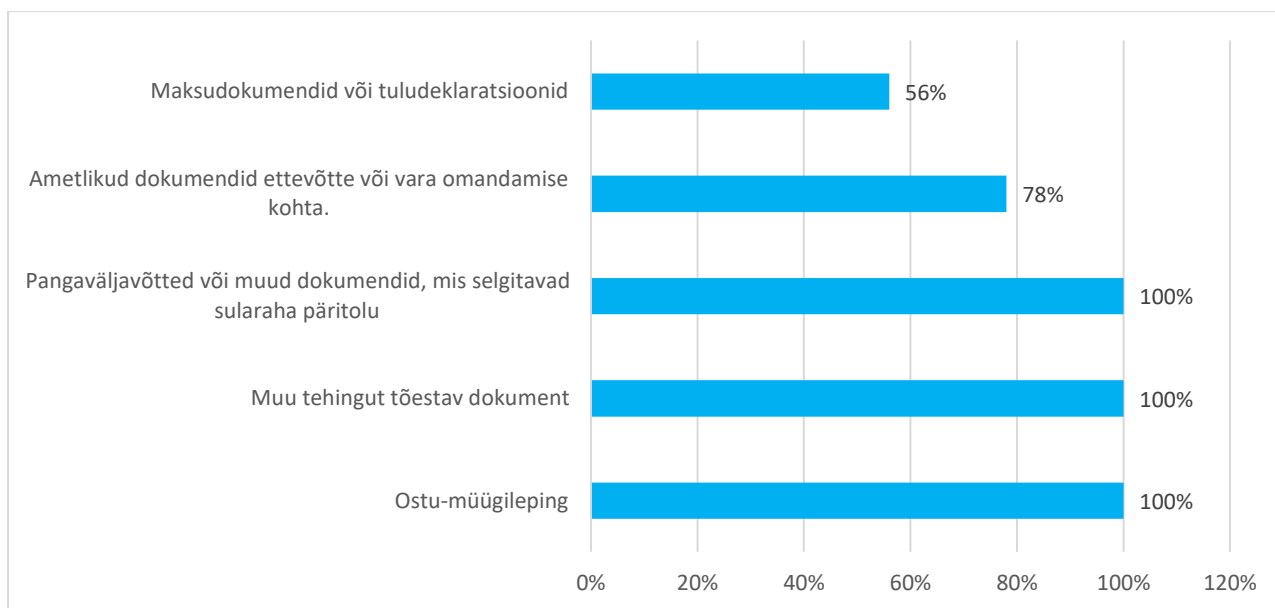
Kolmanda küsimusega, mis telleritele esitati, sooviti kindlaks teha, kuidas tellerid teevad kindlaks sularaha päritolu ning kuidas hinnatakse selle tõelisuses. Kõik vastanud tellerid

lasevad kliendil täita vara päritolu dokumendi, küsivad juurde täiendavad dokumendid ning paluvad kliendil tehingut selgitada küsides täpsustavaid küsimusi. Kõik vastajad valisid eelpool mainitud vastused (100%). Vastajatest 78% peab nõu veel ka AML osakonnaga. Sellest võib järeldada, et tellerid rakendavad mitmeid meetmeid sularaha päritolu kindlakstegemiseks ja selle tõelisuse hindamiseks. Ühtlasi on tellerid valmis kaasama AML osakonna abi ja ekspertiisi vajadusel, et tagada nende tegevuse tõhusus ja vastavus õiguslikele nõuetele.



Joonis 2 . Tellerite sularaha päritolu ning selle tõelisuse hindamine (autori koostatud)

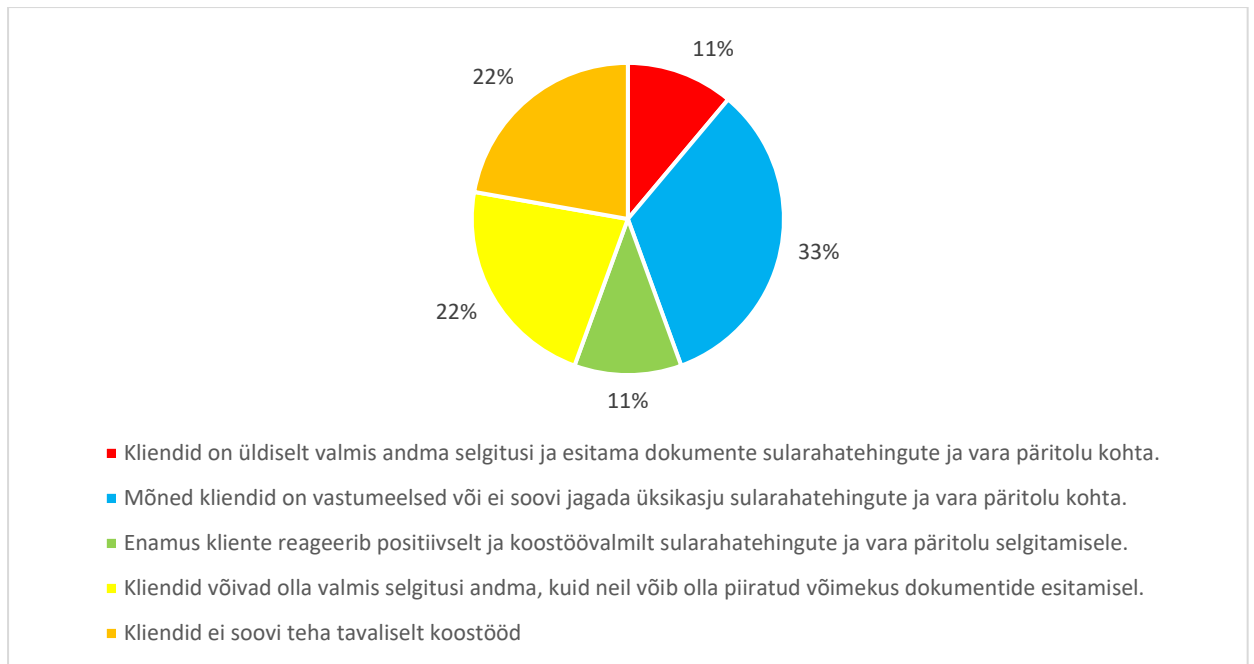
Neljas küsimus, millele paluti telleritel vastata, oli dokumentide kohta, mis palutakse kliendil esitada sularaha päritolu tõendamiseks. Kõik vastanud (100%) küsivad kliendilt juurde ostu-müügilepingut, muud tehingut tõendavat dokumenti ja pangaväljavõtteid või muid dokumente, mis selgitavad sularaha päritolu. Vastanutest 78% küsib kliendilt juurde ka ametlikud dokumendid ettevõtte või vara omandamise kohta ning 56% vastanutest küsib maksudokumente või tuludeklaratsiooni. Tellerid rakendavad mitmekülgseid meetmeid klientide poolt esitatud dokumentide kontrollimiseks sularaha päritolu tõendamiseks ning nad püüavad saada mitmekülgset teavet klientide tehingute ja vara päritolu kohta, et tagada tehingute vastavus seaduslikele nõuetele ja rahapesu tõkestamise standarditele.



Joonis 3. Vara päritolu tõendavad dokumendid (autori koostatud)

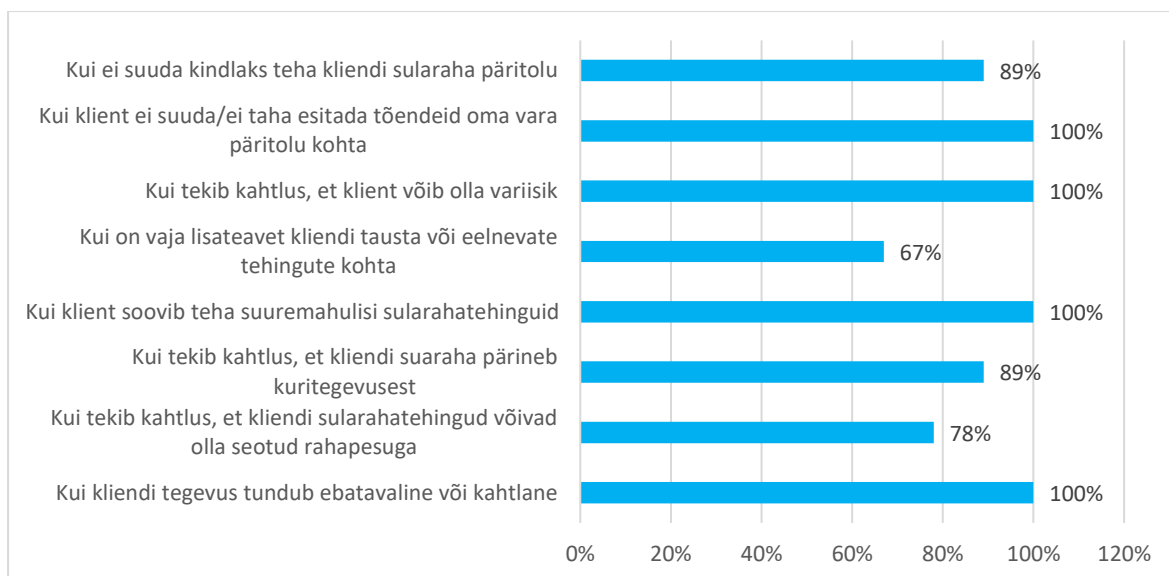
Viienda küsimusega telleritele soovis autor teada klientide valmidust anda selgitusi sularahatehingute ning vara päritolu kohta. Kõige suurema osakaalu (33%) vastustest sai variant, et mõned kliendid on vastumeelsed või ei soovi jagada üksikasju sularahatehingute ja vara päritolu kohta. Võrdselt (22%) osutusid valituks variandid, et kliendid võivad olla valmis selgitusi andma, kuid neil võib olla piiratud võimekus dokumentide esitamisel ning kliendid ei soovi teha tavaliselt koostööd. Võrdselt (11%) osutusid valituks ka variandid, et enamus kliente reageerib positiivselt ja koostöövalmilt sularahatehingute ja vara päritolu selgitamisele ning kliendid on üldiselt valmis andma selgitusi ja edastama dokumente sularahatehingute ja varade päritolu kohta. Vähemuses olid vastused, mis näitasid, et enamus kliente reageerib positiivselt ja koostöövalmilt sularahatehingute ja vara päritolu selgitamisele ning on üldiselt valmis andma selgitusi ja esitama dokumente.

Samasugune küsimus sai esitatud ka KYC osakonnale ning ka nende seas oli kõige suurema protsendiga vastus, et mõned kliendid on vastumeelsed või ei soovi jagada üksikasju sularahatehingute ja vara päritolu kohta. Sellest järeldame, et nii tellerid kui ka KYC osakonna töötajad on kogunud klientide seas vastumeelsust või vastupanu üksikasjaliku teabe jagamisel sularahatehingute ja vara päritolu kohta.



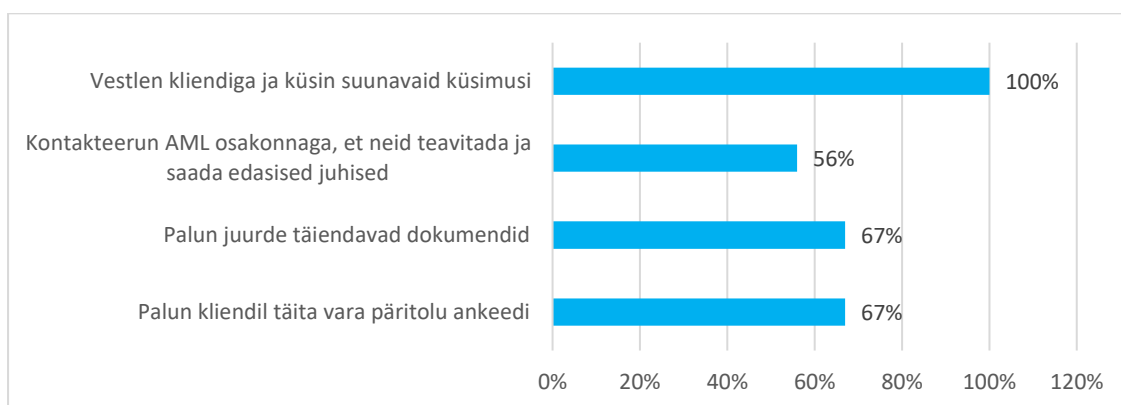
Joonis 4. Klientide valmidus teha koostööd telleritega (autori koostatud)

Kuuenda küsimusega telleritele soovis autor teada saada, millistes olukordades pöörduvad tellerid AML osakonna poole. Võimalik oli valida mitu varianti. Kõik vastanutest (100%) pöörduvad AML osakonna poole, kui kliendi tegevus tundub ebatavaline või kahtlane, kui klient soovib teha suuremahulisi sularahatehinguid, kui tekib kahtlus, et klient võib olla variisik ning kui klient ei suuda või ei taha esitada tõendeid oma vara päritolu kohta. Vastanutest 89% pöörduvad AML osakonna poole ka siis, kui tekib kahtlus, et kliendi sularaha pärineb kuritegevusest ning kui ei suudeta kindlaks teha kliendi sularaha päritolu. Vastanutest 78% pöörduvad AML osakonna poole ka siis, kui tekib kahtlus, et kliendi sularahatehingud võivad olla seotud rahapesuga. Vastanutest 67% pöörduvad siis, kui on vaja lisateavet kliendi tausta või eelnevate tehingute kohta. Sellest järeldame, et tellerid pöörduvad AML osakonna poole mitmesugustes olukordades, mis viitavad võimalikule rahapesule või ebatavalisele käitumisele klientide poolt. Tellerid on teadlikud rahapesuga seotud riskidest ja on valmis tegutsema, kui nad tuvastavad potentsiaalseid märke ebatavalisest käitumisest või võimalikust rahapesust klientide poolt.



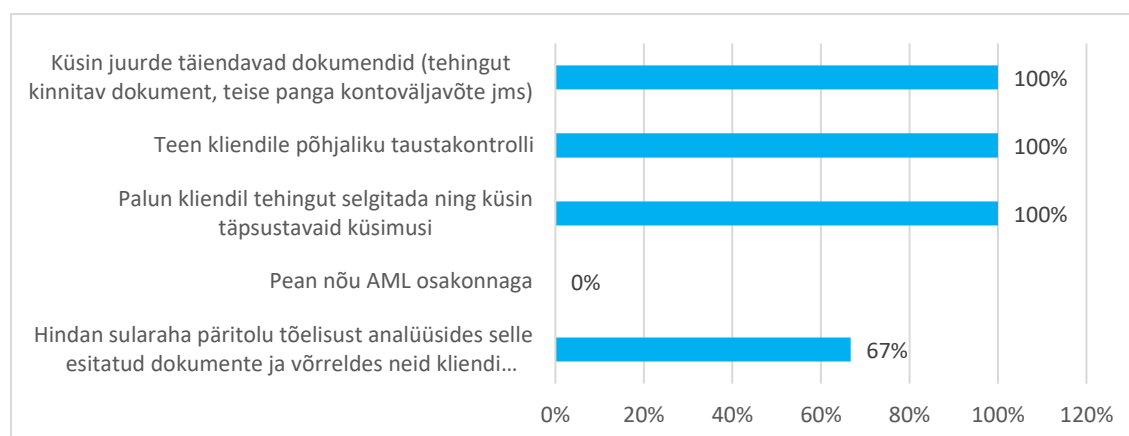
Joonis 5. Olukorrad, kus tellerid pöörduvad AML osakonna poole (autori koostatud)

Seitsmenda küsimusena esitati telleritele küsimus, kuidas toimib teller, kui klient toob panka sularaha, mis jääb alla piirmäära, aga tekib kahtlus vara päritolu osas. Tellerite huvides on ikkagi vara päritolu välja selgitada, sest kõik vastanud (100%) valisid variandi, kus nad suhtlevad kliendiga ja küsivad suunavaid küsimusi. Vastanutest 67% paluvad kliendil täita vara päritolu dokumendi ning samuti paluvad juurde täiendavat dokumentatsiooni. Vastanutest 56% kontakteerub AML osakonnaga, et sealt edasised suunised saada. Sellest järeldame, et telleritel on oluline huvi välja selgitada sularaha päritolu, isegi kui sularahasumma jääb alla piirmäära, kuid tekib kahtlus vara päritolu osas. Tellerid kasutavad mitmeid meetmeid ja ressursse, sealhulgas suhtlemist kliendiga, dokumentide täitmist ja AML osakonnaga konsulteerimist, et tagada tehingute ja varade päritolu õigsus ja seaduslikkus.



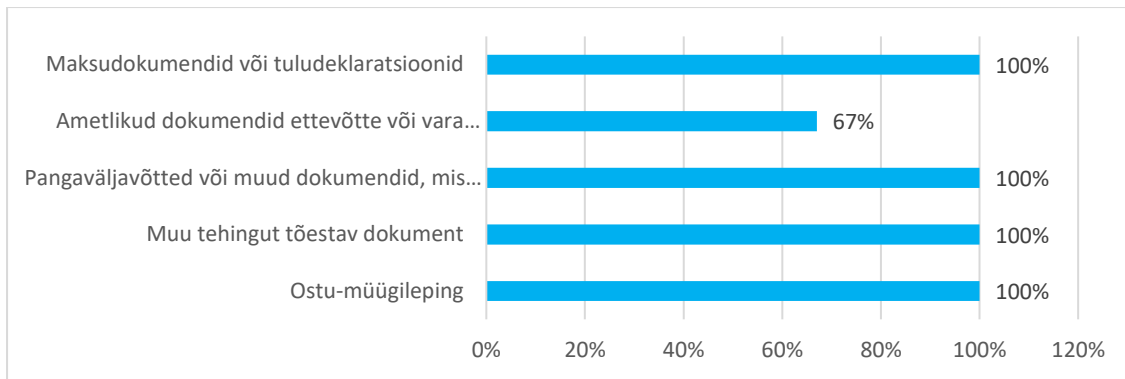
Joonis 6. Toimimine olukorras, kus sularaha jääb alla piirmäära, aga tekib kahtlus (autori koostatud)

KYC osakond kuulub samuti esimesse kaitseliini, mis tähendab seda, et ka nemad suhtlevad klientidega. Küsimused, mis esitati KYC osakonna töötajatele, sisaldavad endas vara päritolu, kliendi tausta, kasutatavate allikate ning klientide koostöövalmiduse küsimusi. Kolmanda küsimusega, mis KYC osakonna töötajatele esitati, sooviti teada, kuidas tehakse kindlaks kliendi sularaha päritolu ning kuidas hinnatakse selle tõelisust. Küsimus oli valikvastustega. Kõik vastanud küsivad juurde täiendavaid dokumente, näiteks tehingut kinnitav dokument või teise panga kontoväljavõtte, kontrollivad põhjalikult kliendi tausta ja paluvad kliendil tehingut selgitada ning küsivad täpsustavaid küsimusi. Antud variandid valisid vastajatest 100%. Vastajatest 67% hindab sularaha päritolu tõelisust analüüsides esitatud dokumente ning võrreldes neid kliendi esitatud informatsiooniga. Sularaha päritolu kindlakstegemisel ning selle tõelisuse hindamisel AML osakonnaga nõu ei peeta.



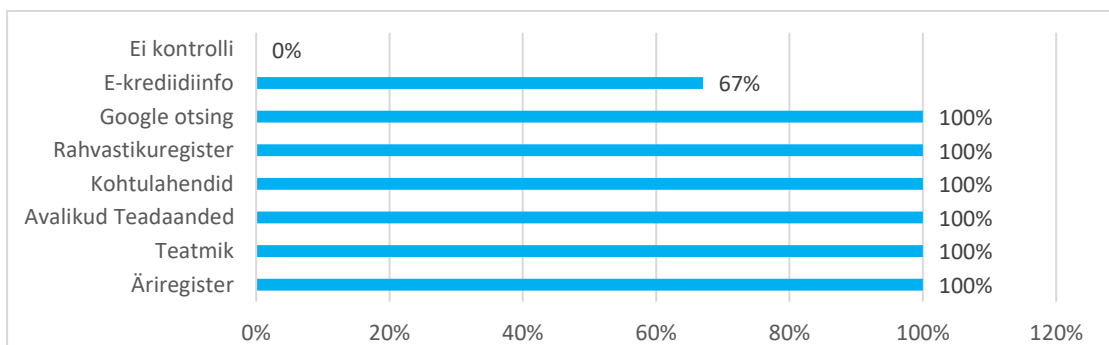
Joonis 7. Sularaha kindlaks tegemine ja tõelisuse hindamine (autori koostatud)

Neljas küsimus KYC osakonna töötajatele oli dokumentide kohta, mis palutakse kliendil esitada sularaha päritolu tõestamiseks. Kõik vastajad paluvad kliendil esitada ostumüügilepingu või muu tehingut tõendava dokumendi, pangaväljavõtted ning maksudokumentid või tuludeklaratsioonid. Antud variandid valisid vastajatest 100%. Ametlike dokumente ettevõtte või vara omandamise kohta küsib klientidelt 67% vastanutest. Vastaja, kes valis variandi „muu“ kirjutas, et otsib avalikest allikatest, mis võiks viidata kliendi tegevusele ja sellest tekkivale sularahale. Sellest saame järeldada, et KYC osakond keskendub eelkõige dokumentidele, mis näitavad konkreetsete tehingute või rahavoogude olemasolu ja päritolu. Samuti teevad töötajad endast kõik oleneva, et ka internetist informatsiooni kliendi sularaha päritolu kohta juurde leida.



Joonis 8. Sularaha päritolu tõendavad dokumendid (autori koostatud)

Viies küsimus, mis KYC osakonna töötajatele esitati, proovis välja selgitada, milliseid allikaid kasutatakse oma klientide tausta kontrolliks. Kõik vastanutest kasutavad oma klientide kontrolliks Äriregistrit, Teatmikku, Avalikke Teadaandeid, Kohtulahendeid, Rahvastikuregistrit ning Google otsingut. Kõik vastajad valisid eelpool mainitud vastused (100%). E-krediidiinfot kasutab vastajatest 67%.



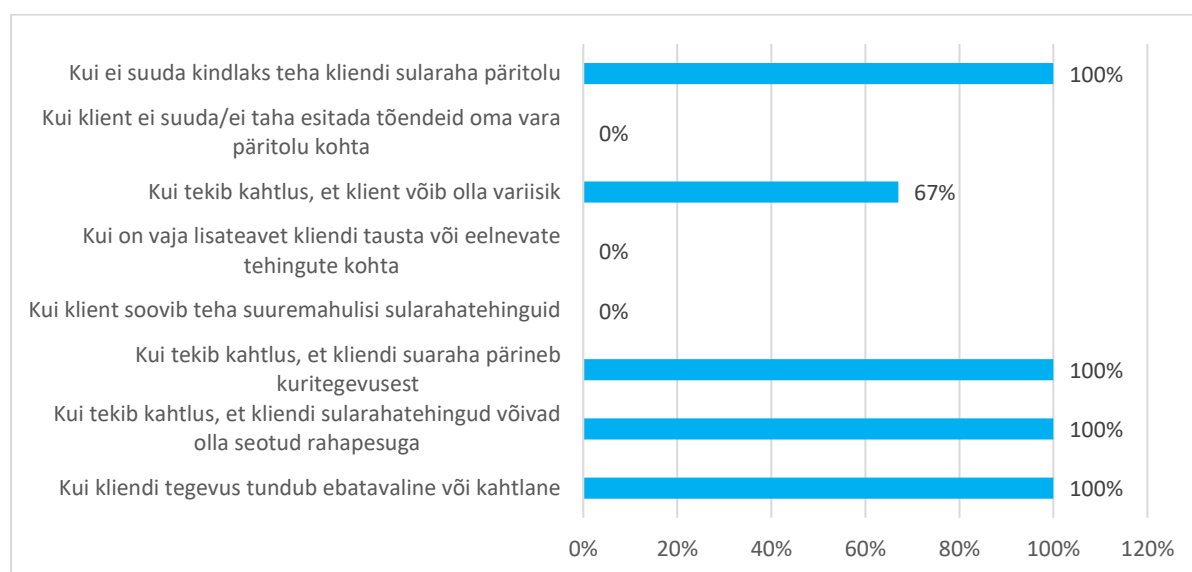
Joonis 9. Kliendi taustakontrolli allikad (autori koostatud)

Kuuenda küsimusena KYC osakonna töötajatele esitati küsimus, mis aitaks paremini aru saada sularahatehingute eesmärgist. Tegemist on avatud küsimusega, mis tähendab, et küsitluses osalenud saavad oma sõnadega vastata. Vastustest tuli välja, et kõige paremini aitab sularahatehingute eesmärgist aru saada kliendi poolt esitatud dokumentatsioon, mis tõestaks sularaha päritolu, kliendi teiste tehingute analüüs ning taustakontroll.

Seitsmes küsimus KYC osakonna töötajatele selgitas välja klientide valmiduse anda selgitusi sularahatehingute ja vara päritolu kohta. Suurem osa vastanutest ehk 67% leiab, et mõned kliendid on vastumeelsed või ei soovi jagada üksikasju sularahatehingute ja vara päritolu kohta. Ülejäänud 33% leiavad, et kliendid on üldiselt valmis andma selgitusi ja esitama dokumente sularahatehingute ja vara päritolu kohta. Oluline on tunnistada klientide erinevaid suhtumisi ja valmisolekut jagada teavet sularahatehingute ja vara päritolu kohta

ning vastavalt kohandada KYC protsessi, et saavutada optimaalne tasakaal klientide privaatsuse ja panganduslike turvameetmete vahel.

Kaheksanda küsimusena KYC osakonna töötajatele esitati küsimus, millistes olukordades pöörduvad nemad AML osakonna poole. AML osakonna poole pöörduakse, kui kliendi tegevus tundub ebatavaline või kahtlane, kui tekib kahtlus, et kliendi sularahatehingud võivad olla seotud rahapesuga, kui tekib kahtlus, et kliendi sularaha pärineb kuritegevusest ning kui ei suuda kindlaks teha kliendi sularaha päritolu. Antud variandid valisid vastajatest 100%. Vastanutest 67% pöördub AML osakonna poole ka variisiku kahtlusega. AML osakonnaga ei võeta ühendust, kui klient soovib teha suuremahulisi sularahatehinguid või kui klient ei suuda või ei taha esitada tõendeid oma vara päritolu kohta. Antud vastused näitavad, millistel juhtudel KYC osakonna töötajad pöörduvad AML osakonna poole ning millistel juhtudel seda ei tehta, mis aitab paremini mõista nende koostööd ja vastutusvaldkondi rahapesu tõkestamisel ja klientide tausta kontrollimisel.

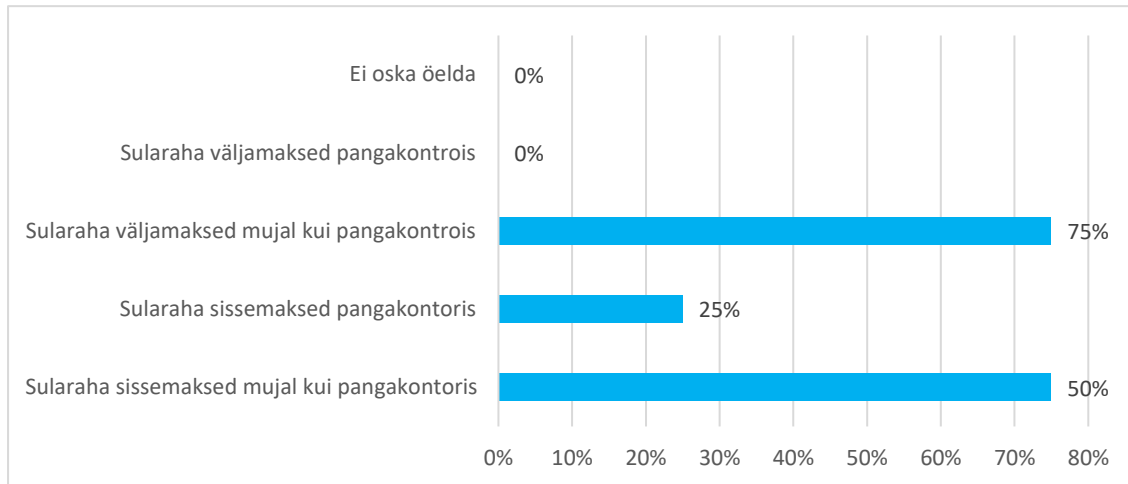


Joonis 10. KYC osakonna ja AML osakonna koostöö (autori koostatud)

2.2.2 Küsimused II kaitseliinile

Rohkem ei esinenud küsimusi, mis olid kõikidel osakondadel sarnased. Kolmanda küsimusega, mis AML osakonna töötajatele esitati, sooviti saada ülevaade sularahatehingute kontrollist, mis on praegusel hetkel kõige keerulisemad ja ressursi nõudvamad. Vastates sai valida rohkem kui ühe variandi. Vastanutest 50% arvas, et kõige

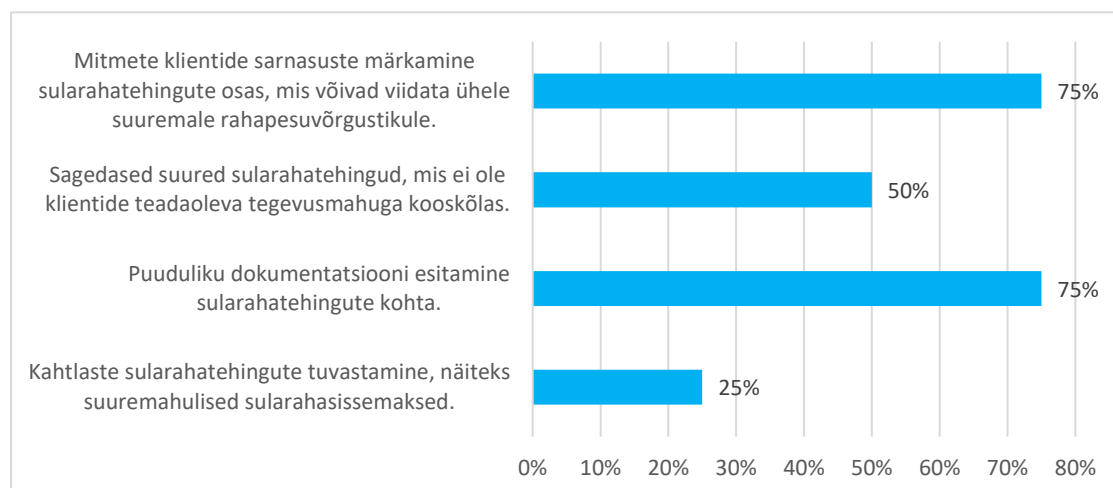
keerulisem ning ressursi nõudvam on sularaha sissemaksed mujal kui pangakontoris, 25% vastanutest valis aga sularaha sissemaksed pangakontoris ning 75% arvas, et sularaha väljamaksed mujal kui pangakontoris. Sularaha väljamaksed pangakontoris ei valinud keegi vastajatest, mis võib tähendada seda, et see võib olla üks turvalisemaid sularahatehinguid.



Joonis 11. Kõige keerulisemad ja ressursi nõudvamad sularahatehingud (autori koostatud)

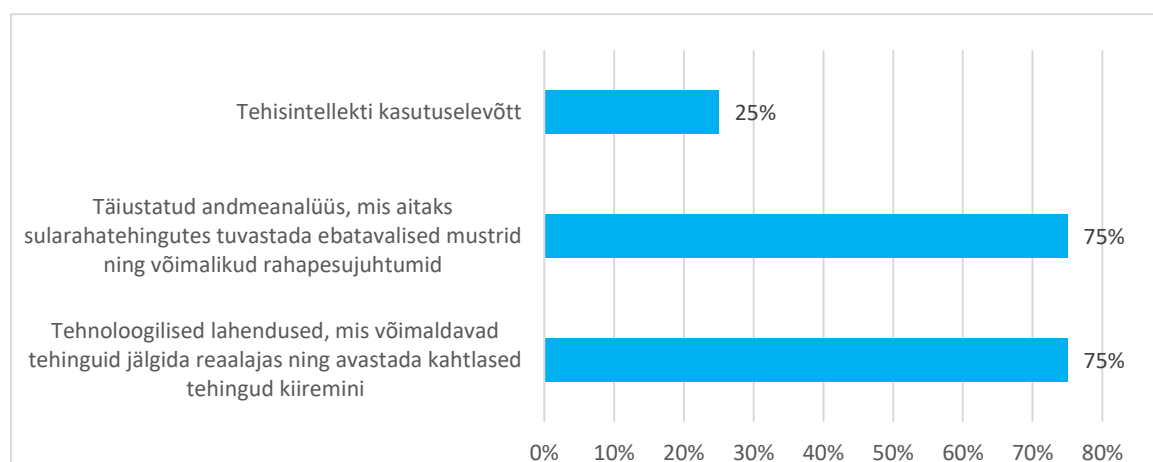
Neljas küsimus AML osakonna töötajatele oli sularahatehingute eesmärgi kohta, mis aitaks sellest paremini aru saada ning mis muudaks oluliselt kontrolli teostamist. Kõige rohkem arvati, et see peaks olema seadusega reguleeritud. Juhul, kui Euroopa Liidu üleselt oleks reguleeritud summad, millest alates sularaha sisse- ja väljamaksed oleks lubatud, lihtsustaks see oluliselt sularahatehingute jälgimist.

Viies küsimus AML osakonna töötajatele oli rikkumiste ja kahtluste kohta, mida pangatöötajad sageli seoses sularahatehingutega tuvastavad. Kõige rohkem valitud variandid olid puuduliku dokumentatsiooni esitamine sularahatehingute kohta ning mitmete klientide sarnasuste märkamine sularahatehingute osas, mis võivad viidata ühele suuremale rahapesuvõrgustikule. Mõlema vastuse osakaal oli 75%. Järgmine enim vastuseid saanud vastusevariant oli sagedased suured sularahatehingud, mis ei ole klientide teadaoleva tegevusmahuga kooskõlas. Antud vastuse valis vastanutest 50%. Vastanutest 25% valis kahtlaste tehingute tuvastamine, näiteks suuremahulised sularaha sissemaksed. Üks vastanutest valis ka variandi „muu“, kuhu kirjutas „analüüsi käigus tuvastatakse, et laekunud vahendid isiku enda välismaa kontolt pärinevad sularahast“. Kui vahendid laekuvad kliendi enda välismaa panga kontolt, siis on keeruline teha kindlaks vahendite



Joonis 12. Pangatöötajate tuvastatavad rikkumised ja kahtlused seoses sularahaga (autori koostatud)

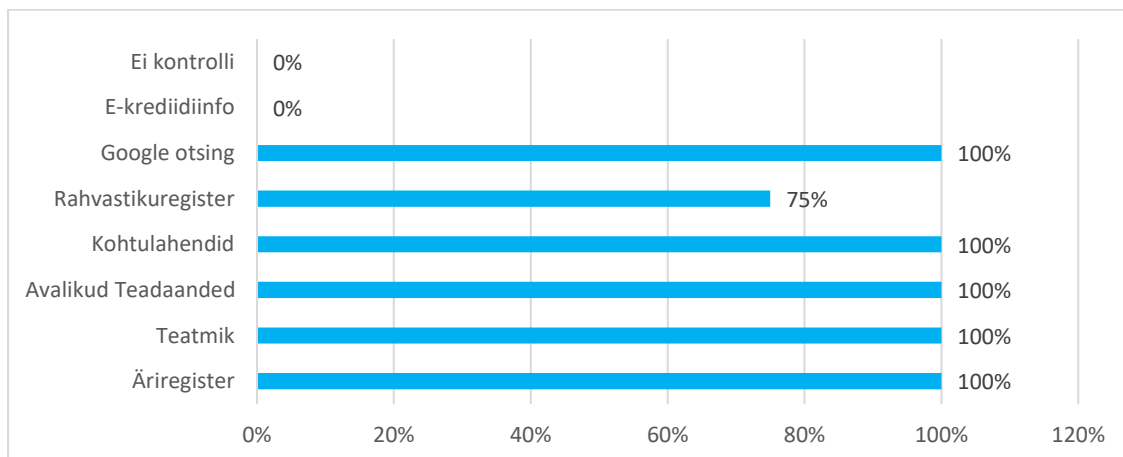
Kuues küsimus AML osakonna töötajatele oli seotud tehnoloogiliste lahendustega või programmidega, mis muudaksid sularahatehingute kontrolli kiiremaks, lihtsamaks ja efektiivsemaks. Vastustes eelistati pigem tehnoloogilisi lahendusi, mis võimaldavad tehinguid jälgida reaalsajas ning avastada kahtlased tehingud kiiremini ning täiustatud andmeanalüüsi, mis aitaks sularahatehingutes tuvastada ebatavalised mustrid ning võimalikud rahapesujuhtumid. Mõlemate vastuste osakaal vastanute seas oli 75%. Valikus oli ka tehisintellekti kasutuselevõtt, mille valisid vastanutest 25%. Sellest võime järeldada, et ainult väike osa vastanutest näeb tehisintellekti kasutuselevõtu potentsiaali rahapesu tõkestamisel ja sularahatehingute kontrollimisel. Seega ei ole praegu laialdane konsensus tehisintellekti kasutamise vajaduse või tõhususe osas selles valdkonnas.



Joonis 13. Tehnoloogilised lahendused või programmid, mis muudaks sularahatehingute kontrollimise tõhusamaks (autori koostatud)

Seitsmes küsimus, mis esitati AML osakonna töötajatele, seisnes arvamuses, millega pangad seisavad silmitsi sularahatehingute jälgimisel. Kõik vastanutest ehk 100% leidis, et peamine asi, millega AML töötajad seisavad silmitsi on tehingutesse reaalses sekkumise võimekus. See kinnitab teaduskirjanduse põhjal koostatud teoreetilist osa, kus tuli välja sama probleem. Töötajatest 50% leidis, et sularahatehingute jälgimisel seisavad pangad silmitsi ka tehingute mahukusega. See näitab, et sularahatehingud on endiselt laialt levinud ja võivad moodustada olulise osa pangandustehingutest. Sellest tulenevalt on oluline, et pangad suudaksid tõhusalt jälgida ja hallata sularahatehinguid, et tagada nende seaduslikkus ja vältida võimalikku rahapesu. Keegi vastanutest ei leidnud, et pangad seisavad silmitsi tööpuuduse või õigusaktide pideva muutumisega.

Kaheksas küsimus, mis AML osakonnale esitati, proovis välja selgitada, milliseid allikaid kasutatakse oma klientide tausta kontrolliks. Kõik vastanutest kasutavad oma klientide kontrolliks Äriregistrit, Teatmiku, Avalikke Teadaandeid, Kohtulahendeid ja Google otsingut. Kõik vastajad valisid eelpool mainitud vastused (100%). Vastanutest 75% kasutab kontrolliks ka Rahvastikuregistrit. Vastajad, kes valisid variandi „muu“ kirjutasid allikaid mida veel kasutatakse ning tõid välja näiteks Kinnistusraamatu, Dow Jones'i, 2lingual'i ning kui tegemist on välismaalasest kliendiga, siis kontrollitakse nende tausta ka päritoluriigi allikatest.



Joonis 14. Kliendi taustakontrolli allikad (autori koostatud)

Kõikide osakondade töötajate käest uuriti viimase küsimusega, millised on nende ettepanekud või nägemused, kuidas saaks tõhustada sularahatehingute järelevalvet ja rahapesu ennetamist. Tegemist oli avatud vastusega, mis tähendab, et kõigil oli võimalus oma ettepanekutest nii pikalt kirjutada, kui nad soovisid. Esmalt pakuti välja väiksemad

sularaha limiidid. Mitmed vastajad soovivad väiksemate sularaha limiitide kehtestamist, et muuta tehingute jälgimine lihtsamaks. See lähenemine võib aidata vähendada suurte sularahatehingute arvu ja seeläbi raskendada rahapesu. Mõned vastajad soovivad sularahatehingute piirmäärade seadusandlikku reguleerimist, eelistatult Euroopa Liidu tasandil. See võiks lihtsustada tehingute jälgimist ja rahapesu ennetamist, muutes reeglid selgemaks ja ühtsemaks kõigis liikmesriikides.

Paljud vastajad rõhutavad tehnoloogiliste arengute olulisust, et avastada ebatavalisi tehinguid kiiremini ja tõhusamalt. Oluliseks peetakse ka paremat infovahetust pankade vahel ning koostööd nii teiste finantsasutuste kui ka riigiasutustega. See võimaldaks kiiremat reageerimist ja paremat jälgimist rahapesu kahtluste korral. Kokkuvõttes näitavad vastused, et sularahatehingute järelevalve ja rahapesu ennetamine nõuab mitmetahulisi lähenemist, sealhulgas nii seadusandlikke meetmeid kui ka tehnoloogilisi lahendusi ning tihedat koostööd erinevate asutuste vahel.

2.3 Järeldused ja ettepanekud

Küsitluse analüüsist võib järeldada, et enamik vastajatest (68,8%) usub, et Eesti pankadel on praegusel hetkel piisav võimekus teostada sularahatehingute kontrolli ja vähendada seeläbi rahapesu ning sellega kaasnevat riski. Siiski väiksem, kuid märkimisväärne osa vastanutest (31,3%) on veendunud, et tegelikult pankadel seda võimekust praegu ei ole. See viitab sellele, et kuigi enamik vastajatest usub, et pankadel on piisavalt ressursse ja võimekust rahapesu vastu võitlemiseks, on siiski oluline tunnistada, et osa töötajaid leiab vastupidist. Seega võib järeldada, et rahapesu ennetamiseks ja sularahatehingute kontrollimiseks võivad olla vajalikud täiendavad meetmed või ressursid, et tagada tõhusam ja usaldusväärsem süsteem.

Vastanud kes leidsid, et pankadel puudub hetkel piisav võimekus leiavad, et üks peamisi muresid on seotud sularahatehingute algse päritolu kontrollimise raskustega eriti juhul, kui vahendid on pärit mitmest erinevast allikast või maksevahendajalt. Lisaks on välja toodud, et pangad ei suuda alati piisavalt kiiresti reageerida uutele petuskeemidele ja rahapesu meetoditele. Samuti on märkimisväärne, et regulatsioonid võivad piirata pankadevahelist infovahetust ja koostööd korrakaitseasutustega, mis omakorda võib takistada efektiivset rahapesu tõkestamist.

Tellerite ja KYC osakonna jaoks on probleem klientidega koostöö tegemine, sest paljud kliendid ei soovi esitada dokumentatsiooni oma sularaha päritolu kohta. Tellerite küsitluse tulemustest selgus, et suurim osa vastajatest, 33%, märkis, et mõned kliendid on vastumeelsed või ei soovi jagada üksikasju sularahatehingute ja vara päritolu kohta. KYC osakonnas enamik vastanutest, 67%, täheldas, et mõned kliendid on vastumeelsed või ei soovi jagada üksikasju nende tehingute ja varade päritolu kohta. Selline vastumeelsus võib olla tingitud ka klientide soovist hoida oma finantsasjad konfidentsiaalsena või puudulikust teadlikkusest regulatsioonidest ja nõuetest. See rõhutab vajadust pakkuda klientidele selget teavet ning luua usaldusväärne ja toetav keskkond, mis julgustaks kliente oma sularahatehingute ja varade päritolu selgitama. Lisaks võib see näidata vajadust rakendada tõhusaid meetmeid klientide veenmiseks ja nende usalduse võitmiseks, et tagada nõuetekohane jälgimine ja rahapesu ennetamine.

Küsitluse tulemustest lähtuvalt võib järeldada, et sularahatehingute kontrollimine, eriti väljamaksed mujal kui pangakontoris, on üks keerukamaid ja ressursimahukamaid ülesandeid AML osakonnale. Suur osa vastanutest (75%) tõstis esile just väljamaksete kontrolli keerukust ja ressursinõudlust väljaspool pangakontorit, näidates, et see valdkond nõuab erilist tähelepanu ja jõupingutusi. Samas näitasid vastused, et sularaha väljamaksed pangakontoris ei tundu olevat nii suureks väljakutseks, kuna ükski vastaja ei valinud seda kui kõige keerulisemat ja ressursinõudvamat valikut. See võib viidata sellele, et sellised tehingud võivad olla turvalisemad ja hõlpsamini kontrollitavad võrreldes muude sularahatehingutega.

AML osakonna töötajate jaoks on oluline kasutada tehnoloogilisi lahendusi sularahatehingute kontrollimise kiirendamiseks, lihtsustamiseks ja efektiivsemaks muutmiseks. Enamik vastanutest eelistas selliseid lahendusi, mis võimaldavad tehinguid jälgida reaajas ja avastada kahtlased tehingud kiiremini. Samuti rõhutati täiustatud andmeanalüüsi olulisust, mis aitaks tuvastada ebatavalisi mustreid ja potentsiaalseid rahapesujuhtumeid. Kuigi tehisintellekti kasutuselevõtt oli üks võimalus, mida osa vastanutest mainis, ei näinud enamik vastanutest sellel valdkonnas laialdast potentsiaali. Ainult 25% vastanutest näitas huvi tehisintellekti vastu rahapesu tõkestamisel ja sularahatehingute kontrollimisel. Seega ei ole hetkel üldist konsensust tehisintellekti kasutamise vajaduse või efektiivsuse osas selles valdkonnas. See näitab, et edasiste tehnoloogiliste lahenduste arendamisel tuleks arvestada erinevate eelistuste ja vajadustega ning tehisintellekti rakendamise potentsiaal võib nõuda täiendavat analüüsi ja uurimist.

Küsitluse tulemuste põhjal võib järeldada, et AML osakonnad seisavad sularahatehingute jälgimisel silmitsi mitmete väljakutsetega. Kõik vastanud märkisid, et peamine väljakutse seisneb tehingutesse reaalajas sekkumise võimekuses. See tulemus kinnitab ka varasemaid teoreetilisi järeldusi, mis rõhutavad sarnast probleemi. Lisaks märkis 50% vastanutest, et oluline väljakutse on tehingute mahukus, mis viitab sularahatehingute laialdasele levikule ja nende olulisele osale pangandustehingutest. See rõhutab vajadust tõhusa jälgimise ja haldamise järele, et tagada tehingute seaduslikkus ja ennetada rahapesu.

Kõikide osakondade töötajad said teha ettepanekuid, kuidas saaks tõhustada sularahatehingute järelevalvet ja rahapesu ennetamist. Vastustest tulid välja mitmed puudused. Kuigi tehnoloogilised arengud võivad olla olulised rahapesu ennetamiseks, võivad mõnedel riikidel ja finantsasutustel olla piiratud ressursid või võimekus investeerida uuenduslikesse tehnoloogiatesse (vt käesolev töö, lk. 18). See võib takistada efektiivset reageerimist ja jälgimist. Olenemata sellest, et parem infovahetus pankade vahel ja riigiasutustega on oluline, võivad olla takistused seoses andmekaitse, konfidentsiaalsuse ja andmevahetuse protokollidega. Need takistused võivad piirata kiiret ja tõhusat reageerimist rahapesu kahtlustele.

Väiksemate sularaha limiitide paika panemine võib olla tõhus meede sularahatehingute järelevalve ja rahapesu ennetamiseks mitmel viisil. Esmalt võib väiksemate limiitide kehtestamine vähendada suurte sularahatehingute arvu, mis võib omakorda raskendada rahapesu, kuna suured summad on sageli seotud ebatavaliste või kahtlaste tehingutega. Lisaks võimaldavad väiksemad limiidid pangandusasutustel paremini jälgida ja analüüsida tehinguid ning tuvastada ebatavalisi mustreid või käitumist, mis võivad viidata rahapesule. Teiseks võib väiksemate sularaha limiitide kehtestamine suurendada läbipaistvust ja vastutust sularahatehingute osas, kuna see sunnib kliente tegema suuremaid tehinguid pangakontode kaudu, kus tehinguid on kergem jälgida ja kontrollida. See võib vähendada ka sularaha kasutamist kuritegelike tegevuste rahastamiseks, kuna suuremad summad peavad läbima panga jälgimise ja kontrolli (vt käesolev töö, lk. 13-14). Väiksemate sularaha limiitide paika panemine võib olla oluline samm sularahatehingute järelevalve ja rahapesu ennetamise tõhustamisel, kuid see nõuab tihedat koostööd ja koordineeritud jõupingutusi nii pangandusasutuste kui ka regulatiivsete organite vahel.

Pärast analüüsi ja teoreetiliste seisukohtade uurimist esitab autor järgmised ettepanekud:

1. Väiksemate sularahalimiitide kehtestamine.

Väiksemad limiidid muudavad suuremate sularahatehingute tegemise raskemaks, vähendades seeläbi rahapesu riski. (vt käesolev töö, lk. 13-14). Väiksemad sularaha limiidid võimaldavad pankadel ja järelevalveasutustel tehinguid lihtsamini jälgida ja analüüsida. See võimaldab kiiremat reageerimist kahtlastele tehingutele ning suurendab tervikuna finantsjärelevalve efektiivsust. Antud ettepaneku töid välja ka paljud küsitlusele vastanud erinevatest osakondadest.

2. Paremate tehnoloogiliste lahenduste kasutuselevõtt

Töö teooria osas tuli välja, et praegu on üheks probleemiks tehingute reaalses jälgimise võimatus (vt käesolev töö, lk. 18). Seda kinnitas ka läbiviidud küsitlus. Reaalses jälgimise süsteemid võimaldavad pankadel avastada ebatavalisi tehinguid kiiremini ja võtta vajalikke meetmeid rahapesu või pettuste kahtluse korral. Täiustatud tehnoloogilised lahendused võimaldavad sügavamalt andmete analüüsi ja tuvastada keerulisi mustreid, mis võivad viidata rahapesule või muudele ebaseaduslikele tegevustele.

3. Parem infovahetus pankade vahel ning riigiasutustega

Luues pankadele ja riigiasutustele tõhusamad kanalid teabe vahetamiseks, saavad nad kiiremini reageerida kahtlastele tehingutele või klientidele. See võimaldaks avastada ja tõkestada rahapesujuhtumeid enne, kui need jõuavad laiemate tagajärgedeni. Infovahetus võimaldab erinevatel asutustel jagada teavet ja analüüsida seda tervikuna. See võimaldaks kombineerida erinevaid teadmisi ja ressursse ning luua tõhusam ja täpsem arusaam kahtlastest tegevustest või tehingutest.

KOKKUVÕTE

Rahapesu on Eesti pangandussektoris murettekitav probleem, kuna sularahaintensiivsete teenuste rahapesuohu tase on tõusnud, mis on põhjustatud sularahatehingute sagenemisest, kiirest inflatsioonist ja majanduslangusest. Sularahatehingud moodustavad endiselt olulise osa majandusest, võimaldades ebaseaduslikke rahalisi tegevusi ellu viia ja varjata. Sellest tulenevalt püstitati küsimus: kas praegusel hetkel suudetakse pangas kontrollida nii põhjalikult sularahatehinguid, et vähendada rahapesu ning sellega kaasnevaid riske? Lõputöö eesmärk oli välja selgitada pangandussektoris esinevad probleemid sularahaga seotud rahapesu tõkestamisel, lähtudes pangandussektori finantsametnike küsitlustest, kes tegelevad sularahaga ja rahapesuvastaste meetmete rakendamisega.

Esimene uurimisküsimus oli soov uurida, milliseid hoolsusmeetmeid rakendatakse sularaha kontrollimisel. Rahapesu ja terrorismi rahastamise tõkestamise seaduse järgi on krediidasutused kohustatud läbi viima isikute tuvastamise protseduure, mis tähendab, et neil lasub vastutus rakendada hoolsusmeetmeid kliendisuhete loomisel ning selle kestel. Kliendi hoolsusmeetmed hõlmavad mitmeid olulisi samme, sealhulgas klientide tuvastamist, mis tähendab nende isikuandmete kogumist ja kontrollimist vastavalt seaduslikele nõuetele. Kõik need meetmed tuleb rakendada nii uute kliendisuhete loomisel kui ka selle kestel, tagades seeläbi tõhusa ja pideva jälgimise ning riskide maandamise sularahatehingute osas.

Teise uurimisküsimusega oli soov teada saada, millised probleemid ilmnevad pankadel sularaha päritolu kontrollimisel. Uurimuse käigus ilmnis, et pankadel on praegu piiratud võimekus sularahatehingute päritolu tõhusaks kontrollimiseks, eriti juhtudel, kui raha on pärit mitmest erinevast allikast või on vahendatud läbi mitme maksevahendaja. Samuti tuvastati, et oluline tegur vara päritolu kindlakstegemisel on klientide koostöövalmidus. Probleemiks kujunes klientide vastumeelsus teha koostööd, selgitada sularaha päritolu ning esitada nõutavat dokumentatsiooni. See võib olla tingitud mitmest tegurist, sealhulgas soovist varjata raha ebaseaduslikku päritolu või lihtsalt ebamugavusest seoses vajalike protseduuridega. Need probleemid seavad pankadele väljakutseid sularaha päritolu kontrollimisel ning rõhutavad vajadust paremate meetmete ja protsesside järele klientide veenmiseks ja koostöö saavutamiseks, et tagada rahapesu ja terrorismi rahastamise tõhus tõkestamine.

Kolmanda uurimisküsimusega oli soov leida antud probleemidele võimalikud lahendused. Esiteks, väiksemate sularahalimiitide kehtestamine muudab suurte tehingute tegemise keerulisemaks, vähendades sellega rahapesu riski. Teiseks, täiustatud tehnoloogilised lahendused võimaldavad reaalajas jälgimist ja sügavamat andmete analüüsi, kiirendades kahtlaste tehingute avastamist ja ennetavat sekkumist. Kolmandaks, tõhusamate kanalite loomine infovahetuseks pankade ja riigiasutuste vahel võimaldab kiiremat reageerimist kahtlastele olukordadele ning aitab ennetada rahapesujuhtumeid. Need meetmed koos võivad oluliselt suurendada finantsjärelevalve efektiivsust ja aidata kaasa finantsüsteemi turvalisusele.

Esimene uurimisülesanne oli anda ülevaade rahapesu õigusaktidest, et mõista nende tähtsust ja mõju rahapesuvastases võitluses. Teiseks uurimisülesandeks oli anda ülevaade sularahaga seotud rahapesu riskidest ja riskihinnangust, et mõista paremini nende riskide olemust ja ulatust ning hinnata nende mõju finantsüsteemile ja ühiskonnale. See ülevaade oli oluline, kuna see aitas kujundada arusaamist rahapesu riskide laadist ja levikust ning pakkus alust edasiseks uurimistööks, mis keskendub nende riskide tõhusale maandamisele ja ennetamisele. Kolmandaks oli analüüsida pangandussektori rahapesuga seotud finantsametnike hinnanguid sularahaga seotud rahapesu hoolsusmeetmete rakendamise kohta. Uuringu tulemusi analüüsidest ilmnes, et enamik finantsametnikke on veendunud, et hetkel rakendatavad hoolsusmeetmed suudavad tagada piisava kontrolli sularahatehingute üle. Neljandaks uurimisülesandeks oli analüüsida võimalikke lahendusi ning teha selle põhjal järeldusi. Võimalikud lahendused praegu esinevatele probleemidele võiks olla sularaha limiitide vähendamine, paremate tehnoloogiliste lahenduste kasutuselevõtt ning parem infovahetus pankade vahel ja riigiasutustega. Praeguste probleemide lahendamiseks võiks kaaluda mitmeid lähenemisviise. Üks võimalik lahendus oleks sularaha limiitide vähendamine, mis vähendaks oluliselt suurte sularahatehingute sagedust ja suurust, aidates seeläbi vähendada võimalikke riske ja piirata ebaseaduslike tehingute võimalusi. Lisaks võiks keskenduda paremate tehnoloogiliste lahenduste rakendamisele, mis võimaldaksid tõhusamat ja täpsemat jälgimist ning tuvastaksid kiiremini kahtlaseid tehinguid või musta turu tegevust. Samuti on oluline tugevdada infovahetust pankade vahel ning riigiasutustega, sealhulgas maksu- ja järelevalveasutustega. Parema infovahetuse kaudu saaksid asutused kiiremini reageerida kahtlastele tegevustele ja jagada olulist teavet, mis võimaldaks tõhusamat järelevalvet ja ennetavat tegevust.

SUMMARY

Money laundering is a concerning issue in the Estonian banking sector, as the level of money laundering risk related to cash-intensive services has increased due to the increase in the number of cash transactions, rapid inflation and economic recession. Consequently, the question was: can the bank currently control cash transactions sufficiently to reduce money laundering and related risks? The thesis aimed to pinpoint issues in the banking sector regarding the prevention of cash-related money laundering.

The first research question was what due diligence measures are applied when checking cash. Customer diligence involves several steps, including customer identification, which means collecting and verifying their personal data according to legal requirements. These measures must be applied both during the establishment of new client relationships and throughout their duration, ensuring effective and continuous monitoring and risk mitigation in cash transactions.

The second research question was what problems appear in banks when checking the origin of cash. The study revealed that banks currently have limited capability to effectively verify the origin of cash transactions, particularly in cases involving funds from multiple sources or intermediaries. Additionally, customer cooperation became an important factor in determining the origin of assets.

The third research question was finding possible solutions to the given problems. The analysis of the study showed that possible solutions could include the establishment of lower cash limits, the introduction of high-tech solutions and the creation of more efficient information exchange channels between banks and state authorities.

Consequently, the author recommends a thorough reassessment of the existing cash limits, advocating their reduction. In addition, the proposal includes equipping employees with advanced technological tools to optimize their workflows. Moreover, the establishment of more effective channels for information exchange between banks and government agencies to increase overall operational efficiency.

VIIDATUD ALLIKATE LOETELU

Alaküla, A., 2018. *Rahapesu tõkestamise hoolsusmeetmete rakendamine pangandussektori näitel. Lõputöö*. Tallinn: Sisekaitseakadeemia.

Babbie, E., 2010. *The Practice of Social Research*. Belmont, CA, Wadsworth, London: Cengage Learning

Beilmann, M., 2020. *Küsimustiku koostamine*. [Võrgumaterjal] Leitav: <https://samm.ut.ee/k%C3%BCsimustiku-koostamine> [Kasutatud 16.03.2024].

Council of Europe, 2022. *Anti-money laundering and counter-terrorist financing measures Estonia. Fifth Round Mutual Evaluation Report*. Strasbourg: Council of Europe.

Council of Europe, 2023. *MONEYVAL Strategy on anti-money laundering, combating the financing of terrorism and proliferation financing (2023-2027)*. [Võrgumaterjal] Leitav: <https://rm.coe.int/moneyvalstrategy2023-2027-en/1680ab0b06> [Kasutatud 27.02.2024].

Custers, B. H., Pool, R. L. & Cornelisse, R., 2019. Banking malware and the laundering of its profits. *European Journal of Criminology*, 16(6) pp. 735-736.

Domashova, J., Mikhailina, N., 2021. Usage of machine learning methods for early detection of money laundering schemes. *Procedia Computer Science*, 190, pp. 185.

Doughty, C., 2005. Know your customer: Automation is key to comply with legislation. *Business Information Review*, 22 (4), pp. 249.

Eesti Pangaliit, *Rahapesu ja terrorismi rahastamise tõkestamise ning finantssanktsioonide rakendamise poliitika ja suunised*. [Võrgumaterjal] Leitav: <https://www.pangaliit.ee/files/AML%20hoolsusmeetmed%2018.03.19.pdf> [Kasutatud 11.02.24].

Eesti Pank, 2023. *Pangateenuste toimepidevus*. [Võrgumaterjal] Leitav: <https://www.eestipank.ee/maksed-arveldused/pangateenuste-toimepidevus> [Kasutatud 25.01.2024]

Eldridge, J., E., 1986. The Bank Secrecy Act: Privacy, Comity, and the Politics of Contraband. *North Carolina Journal of International Law*, 11 (3), pp. 668.

Euroopa Keskpank. *Sularaha roll*. [Võrgumaterjal] Leitav: https://www.ecb.europa.eu/euro/cash_strategy/cash_role/html/index.et.html [Kasutatud 06.03.2024].

Euroopa Liidu Nõukogu, 2024a. *Infograafik – Mida rahapesu tähendab?* [Võrgumaterjal] Leitav: <https://www.consilium.europa.eu/et/infographics/anti-money-laundering/> [Kasutatud] 02.03.2024].

Euroopa Liidu Nõukogu, 2024b. *Võitlus rahapesu ja terrorismi rahastamise vastu ELis*. [Võrgumaterjal] Leitav: <https://www.consilium.europa.eu/et/policies/fight-against-terrorism/fight-against-terrorist-financing/#fight> [Kasutatud 26.02.2024].

Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2015/849, 20. mai 2015, *mis käsitleb finantsüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja 46 tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ*.

Europol, 2015. *Why is cash still king?* [Võrgumaterjal] Leitav: <https://www.europol.europa.eu/sites/default/files/documents/europolcik%20%281%29.pdf> [Kasutatud 19.02.2024].

Europol, 2023. *Money Muling*. [Võrgumaterjal] Leitav: <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling> [Kasutatud 03.03.2024].

FATF, 2012. *Rahapesu ning terrorismi ja massihävitusrelvade leviku rahastamise vastu võitlemise rahvusvahelised standardid. FATFi soovitused*. [Võrgumaterjal] Leitav: https://www.fi.ee/sites/default/files/FATF_eeesti_keeelne_tolge.pdf [Kasutatud 11.02.2024].

FATF, 2014. *Guidance for risk-based approach the banking sector*. [Võrgumaterjal] Leitav: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf> [Kasutatud 10.02.2024].

Finantsinspektsioon, 2018a. *Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks*. [Võrgumaterjal] Leitav: https://fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf [Kasutatud 17.02.2024].

Finantsinspektsioon, 2018b. *Suunised riskitegurite kohta*. [Võrgumaterjal] Leitav: https://fi.ee/sites/default/files/2018-08/pp_nr_10_Guidelines_on_Risk_Factors_ET_04-01-2018.pdf [Kasutatud 24.02.2024].

Finantsinspektsioon, 2021. *Rahvusvahelise finantssanktsiooni kohaldamine krediidi- ja finantseerimisasutustes* [Võrgumaterjal] Leitav: https://www.fi.ee/sites/default/files/2021-11/Finantsinspektsiooni%20soovituslik%20juhend%20Finantssanktsiooni%20kohaldamine_0.pdf [Kasutatud 10.02.2024].

Georgieva, N., Buzlevski, B., 2021. Analysis of the abuse of cash transactions, money cards and international transfers in function of money laundering in banks. *Scientific Journal of Contemporary European and Balkan Politics: Law, Economics, Security Issues, Cultural and Ethnic Studies and Environmental Policies*, 4 (2), pp. 39-40.

Goldbarsht, D., 2018. Shedding Light on Shadow Banking. *The Journal of Criminal Law*, 82 (3), pp. 265.

Haq, I., El Shahat, I., Abatemarco, M., Bates, C., 2022. The Impact of 9/11 on Money Laundering. *American Behavioral Scientist*, 0, pp. 3.

Hirsjärvi, S., Remes, P. & Sajavaara, P., 2007. *Uuri ja kirjuta*. Tallinn: Medicina.

Holcomb, Z.-C., 2017. *Fundamentals Of Descriptive Statistics*. 1. edition. New York: Routledge.

Hädaolukorra seadus (2017) RT I, 06.07.2023, 33.

Ilma, M. A., & Aryati T., 2022. Bank role in preventing money laundering and cyber security. *Technium Social Science Journal*, 37, pp. 289.

Irvine, M., R., & King, D., R., 1987. The Money Laundering Control Act of 1986: Tainted Money and the Criminal Defense Lawyer. *McGeorge Law Review*, 19 (1), pp. 182.

International Finance Corporation, 2019. *Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks*. [Võrgumaterjal] Leitav: <https://www.ifc.org/content/dam/ifc/doc/mgrt/45464-ifc-aml-report.pdf> [Kasutatud 06.03.2024].

Jaarsveld. I., L., 2011. *Aspects of money laundering in South African Law*. Doktoritöö. Pretoria: University of South Africa

Mathers, C., 2005. *Kuritegevuse kool: Rahapesu*. Tallinn: Olion

Mencken, J., A., 1998. Supervising Secrecy: Preventing Abuses Within Bank Secrecy and Financial Privacy Systems. *Boston College International and Comparative Law Review*, 21 (2), pp. 476.

Mikkelsen, D., Pravdic, A., Richardson, B., 2019. *Flushing out the money launderers with better customer riskrating models* [Võrgumaterjal] Leitav: <https://www.mckinsey.de/~ /media/McKinsey/Business%20Functions/Risk/Our%20Insights/Flushing%20out%20the%20money%20launderers%20with%20better%20customer%20risk%20rating%20models/Flushing-out-the-money-launderers-VF.pdf> [Kasutatud 11.02.2024].

Mitsilegas, V., Vavoula, N., 2016. The Evolving EU Anti-Money Laundering Regime. Challenges for Fundamental Rights and the Rule of Law. *Maastricht Journal of European and Comparative Law*, 23 (2), pp. 279.

Moreno, S. M. B. M., Seigneur, J-M., Gotzev, G., 2021. *Handbook of Research on Cyber Crime and Information Privacy*. Hershey, Pennsylvania: IGI Global.

Nikolosk, N., Simonovski, I., 2012. Role of banks as entity in the system for prevention of money laundering in the Macedonia. *Procedia - Social and Behavioral Sciences*, 44 (Part of special issue), pp. 455-456.

Politsei- ja piirivalveamet, 2019. *Juhend kahtlaste tehingute tunnuste kohta*. [Võrgumaterjal] Leitav: <https://www.politsei.ee/files/Rahapesu/juhendkahtlastetehingutetunnustekohta.pdf?222a84e8fa> [Kasutatud 17.03.2024].

Rahandusministeerium, 2023. *Rahapesuga võitlevad organisatsioonid Eestis*. [Võrgumaterjal] Leitav: <https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/rahapesuga-voitlevad> [Kasutatud 25.12.2023].

Rahapesu Andmebüroo, 2018. *Rahapesu andmebüroo soovitusel kohustatud isikute tegevusest tulenevate riskide juhtimiseks* [Võrgumaterjal] Leitav: <https://fiu.ee/oigusaktid-ja-juhendid/juhendid#soovitused-kohustatu> [Kasutatud 11.02.2024].

Rahapesu Andmebüroo, 2022. Juhend kahtlaste tehingute tunnuste kohta. [Võrgumaterjal] Leitav: <https://fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh> [Kasutatud 24.02.2024].

Rahapesu Andmebüroo, 2023. *Korduma kippuvad küsimused*. [Võrgumaterjal] Leitav: <https://fiu.ee/kasulik-info/kkk#kkk-rahapesu-tokest> [Kasutatud 01.12.2023].

Rahapesu Andmebüroo, 2023a. *Sularahaga seotud rahapesuoht Eestis püsib*. [Võrgumaterjal] Leitav: https://fiu.ee/uudised/sularahaga-seotud-rahapesuoht-eestis-pusib?fbclid=IwAR0jSlm8_qkfdyPTiF76a6pr7GWf6rjgU-VT7_0jNwUYZci3jyagdem73fU [Kasutatud 13.10.2023]

Rahapesu Andmebüroo, 2023b. *Sularahaga seotud rahapesu ja terrorismi rahastamise riskid Eestis* [Võrgumaterjal] Leitav: <https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#sularahaga-seotud-ra> [Kasutatud 13.10.2023]

Rahapesu ja terrorismi rahastamise tõkestamise seadus (2017) RT I, 06.07.2023, 71.

Rahapesu ja terrorismi rahastamise tõkestamise seadus (2023) RT I, 17.03.2023, 19

Rajput, V. U., 2013. Research on Know Your Customer (KYC). *International Journal of Scientific and Research Publications*, 3 (7), pp. 1.

Signicat, 2023. *Customer Due Diligence (CDD) and its importance in risk management and compliance*. [Võrgumaterjal] Leitav: <https://www.signicat.com/blog/customer-due-diligence-cdd-and-its-role-in-banking> [Kasutatud 28.02.2024].

Silva, P. G., 2019. Recent developments in EU legislation on anti-money laundering and terrorist financing. *New Journal of European Criminal Law*, 10 (1), pp. 59.

Unger, B., 2013. Can Money Laundering Decrease? *Public Finance Review* Volume 41(5), pp. 659-660.

Wilkes, C., 2020. A Case for Reforming the Anti-Money Laundering Regulatory Regime: How Financial Institutions' Criminal Reporting Duties Have Created an Unfunded Private Police Force. *Indiana Law Journal*, 95 (2), pp. 655.

Lisa 1. Küsimustik telleritele

- 1. Kas Teie arvates on Eesti pankadel praegusel hetkel piisav võimekus teostada sularahatehingute kontrolli, et vähendada rahapesu ning sellega kaasnevaid riske?**
 - a. Jah
 - b. Ei

- 2. Kui vastasite eelnevale küsimusele "ei", siis palun põhjendage miks.**

- 3. Kuidas teete kindlaks kliendi sularaha päritolu ning kuidas hindate selle tõelisust?**
 - a. Lasen kliendil täita vara päritolu dokumendi
 - b. Küsin juurde täiendavad dokumendid (tehingut kinnitav dokument, teise panga kontoväljavõtte jms)
 - c. Pean nõu AML osakonnaga
 - d. Palun kliendil tehingut selgitada ning küsin täpsustavaid küsimusi
 - e. Muu

- 4. Milliseid dokumente palute kliendil esitada sularaha päritolu tõestamiseks?**
 - a. Ostu-müügileping
 - b. Muu tehingut tõestav document
 - c. Pangaväljavõtted või muud dokumendid, mis selgitavad sularaha päritolu
 - d. Ametlikud dokumendid ettevõtte või vara omandamise kohta.
 - e. Maksudokumendid või tuludeklaratsioonid
 - f. Muu

- 5. Kuidas hindate üldiselt klientide valmidust anda selgitusi sularahatehingute ja vara päritolu kohta?**
 - a. Kliendid on üldiselt valmis andma selgitusi ja esitama dokumente sularahatehingute ja vara päritolu kohta.
 - b. Mõned kliendid on vastumeelsed või ei soovi jagada üksikasju sularahatehingute ja vara päritolu kohta.

- c. Enamus kliente reageerib positiivselt ja koostöövalmilt sularahatehingute ja vara päritolu selgitamisele.
- d. Kliendid võivad olla valmis selgitusi andma, kuid neil võib olla piiratud võimekus dokumentide esitamisel.
- e. Mõned kliendid on avatud koostööle, kuid nõuavad täiendavat veenmist ja selgitust sularahatehingute ja vara päritolu kohta.
- f. Kliendid ei soovi teha tavaliselt koostööd

6. Millistes olukordades pöörduate AML osakonna poole?

- a. Kui kliendi tegevus tundub ebatavaline või kahtlane
- b. Kui tekib kahtlus, et kliendi sularahatehingud võivad olla seotud rahapesuga
- c. Kui tekib kahtlus, et kliendi suaraha pärineb kuritegevusest
- d. Kui klient soovib teha suuremahulisi sularahatehinguid
- e. Kui on vaja lisateavet kliendi tausta või eelnevate tehingute kohta
- f. Kui tekib kahtlus, et klient võib olla variisik
- g. Kui klient ei suuda/ei taha esitada tõendeid oma vara päritolu kohta
- h. Kui ei suuda kindlaks teha kliendi sularaha päritolu
- i. Muu

7. Kuidas toimite, kui klient toob panka sularaha, mis jääb alla piirmäära, aga Teil tekib kahtlus vara päritolu osas?

- a. Tegemist ei ole märkimisväärse summaga, võtan sularaha vastu
- b. Palun kliendil täita vara päritolu ankeedi
- c. Palun juurde täiendavad dokumendid
- d. Kontakteerun AML osakonnaga, et neid teavitada ja saada edasised juhised
- e. Vestlen kliendiga ja küsin suunavaid küsimusi
- f. Muu

8. Kuidas Teie tuvastate, et tegemist võib olla variisikuga, kes teeb sularahasissemakseid teise inimese eest?

9. Millised on Teie ettepanekud või nägemused, kuidas saaks tõhustada sularahatehingute järelvalvet ja rahapesu ennetamist pangakontoris?

Lisa 2. Küsimustik KYC osakonnale

- 1. Kas Teie arvates on Eesti pankadel praegusel hetkel piisav võimekus teostada sularahatehingute kontrolli, et vähendada rahapesu ning sellega kaasnevaid riske?**
 - a. Jah
 - b. Ei

- 2. Kui vastasite eelnevale küsimusele "ei", siis palun põhjendage miks.**

- 3. Kuidas teete kindlaks kliendi sularaha päritolu ning kuidas hindate selle tõelisust?**
 - a. Küsin juurde täiendavad dokumendid (tehingut kinnitav dokument, teise panga kontoväljavõtte jms)
 - b. Teen kliendile põhjaliku taustakontrolli
 - c. Palun kliendil tehingut selgitada ning küsin täpsustavaid küsimusi
 - d. Pean nõu AML osakonnaga
 - e. Hindan sularaha päritolu tõelisust analüüsides selle esitatud dokumente ja võrreldes neid kliendi esitatud informatsiooniga
 - f. Muu

- 4. Milliseid dokumente palute kliendil esitada sularaha päritolu tõestamiseks?**
 - a. Ostu-müügileping
 - b. Muu tehingut tõestav document
 - c. Pangaväljavõtted või muud dokumendid, mis selgitavad sularaha päritolu
 - d. Ametlikud dokumendid ettevõtte või vara omandamise kohta.
 - e. Maksudokumendid või tuludeklaratsioonid
 - f. Muu

- 5. Millistest allikates kontrollite oma klientide tausta?**
 - a. Äriregister
 - b. Teatmik
 - c. Avalikud Teadaanded
 - d. Kohtulahendid

- e. Rahvastikuregister
- f. Google otsing
- g. E-krediidiinfo
- h. Ei kontrolli
- i. Muu

6. Mis aitaks paremini aru saada sularahatehingute eesmärgist?

7. Kuidas hindate üldiselt klientide valmidust anda selgitusi sularahatehingute ja vara päritolu kohta?

- a. Kliendid on üldiselt valmis andma selgitusi ja esitama dokumente sularahatehingute ja vara päritolu kohta.
- b. Mõned kliendid on vastumeelsed või ei soovi jagada üksikasju sularahatehingute ja vara päritolu kohta.
- c. Enamus kliente reageerib positiivselt ja koostöövalmilt sularahatehingute ja vara päritolu selgitamisele.
- d. Kliendid võivad olla valmis selgitusi andma, kuid neil võib olla piiratud võimekus dokumentide esitamisel.
- e. Mõned kliendid on avatud koostööle, kuid nõuavad täiendavat veenmist ja selgitust sularahatehingute ja vara päritolu kohta.
- f. Kliendid ei soovi teha tavaliselt koostööd

8. Millistes olukordades pöördate AML osakonna poole?

- a. Kui kliendi tegevus tundub ebatavaline või kahtlane
- b. Kui tekib kahtlus, et kliendi sularahatehingud võivad olla seotud rahapesuga
- c. Kui tekib kahtlus, et kliendi suaraha pärineb kuritegevusest
- d. Kui klient soovib teha suuremahulisi sularahatehinguid
- e. Kui on vaja lisateavet kliendi tausta või eelnevate tehingute kohta
- f. Kui tekib kahtlus, et klient võib olla variisik
- g. Kui klient ei suuda/ei taha esitada tõendeid oma vara päritolu kohta
- h. Kui ei suuda kindlaks teha kliendi sularaha päritolu
- i. Muu

9. Kuidas Teie tuvastate, et tegemist võib olla variisikuga, kes teeb sularahasissemakseid teise inimese eest?

10. Millised on Teie ettepanekud või nägemused, kuidas saaks tõhustada sularahatehingute järelvalvet ja rahapesu ennetamist?

Lisa 3. Küsimustik AML osakonnale

- 1. Kas Teie arvates on Eesti pankadel praegusel hetkel piisav võimekus teostada sularahatehingute kontrolli, et vähendada rahapesu ning sellega kaasnevaid riske?**
 - a. Jah
 - b. Ei

- 2. Kui vastasite eelnevale küsimusele "ei", siis palun põhjendage miks.**

- 3. Milliste sularahatehingute kontrolli peate praegusel hetkel kõige keerulisemaks ja ressursi nõudvamaks?**
 - a. Sularaha sissemaksud mujal kui pangakontoris
 - b. Sularaha sissemaksud pangakontoris
 - c. Sularaha väljamaksud mujal kui pangakontoris
 - d. Sularaha väljamaksud pangakontoris
 - e. Ei oska öelda

- 4. Mis muudaks oluliselt kontrolli teostamist ja aitaks paremini aru saada sularahatehingute eesmärgist?**

- 5. Milliseid rikkumisi ja kahtlusi tuvastavad pangatöötajad sageli seoses sularaha tehingutega?**
 - a. Kahtlaste sularahatehingute tuvastamine, näiteks suuremahulised sularahasissemaksud.
 - b. Puuduliku dokumentatsiooni esitamine sularahatehingute kohta.
 - c. Sagedased suured sularahatehingud, mis ei ole klientide teadaoleva tegevusmahuga kooskõlas.
 - d. Mitmete klientide sarnasuste märkamine sularahatehingute osas, mis võivad viidata ühele suuremale rahapesuõrgustikule.
 - e. Muu

- 6. Millised tehnoloogilised lahendused või programmid muudaksid sularahatehingute kontrolli kiiremaks, lihtsamaks ja efektiivsemaks?**

- a. Tehnoloogilised lahendused, mis võimaldavad tehinguid jälgida reaajas ning avastada kahtlased tehingud kiiremini
- b. Täiustatud andmeanalüüs, mis aitaks sularahatehingutes tuvastada ebatavalised mustrid ning võimalikud rahapesujuhtumid
- c. Tehisintellekti kasutuselevõtt
- d. Muu

7. Millega Teie arvates seisavad pangad silmitsi sularahatehingute jälgimisel?

- a. Tööjõupuudus
- b. Tehingute mahukus
- c. Tehingutesse reaajas sekkumise võimekus
- d. Õigusaktide pidev muutumine
- e. Muu

8. Kuidas Teie tuvastate, et tegemist võib olla variisikuga, kes teeb sularahassemakseid teise inimese eest?

9. Millistest allikates kontrollite oma klientide tausta?

- a. Äriregister
- b. Teatmik
- c. Avalikud Teadaanded
- d. Kohtulahendid
- e. Rahvastikuregister
- f. Google otsing
- g. E-krediidiinfo
- h. Ei kontrolli
- i. Muu

10. Millised on Teie ettepanekud või nägemused, kuidas saaks tõhustada sularahatehingute järelevalvet ja rahapesu ennetamist? Palun kirjeldage paari lausega.