## 5. Finantssektori haavatavus

### 5.1. Sektori üldkirjeldus

**Sektori kirjeldus**

Eesti finantssektor on rahvusvahelises võrdluses suhteliselt väike, kuid erinevalt ülejäänud Euroopa Liidust on Eesti finantssektor viimastel aastatel jõudsalt kasvanud. Eesti finantssektor on panganduskeskne. Pangandussektori varade osakaal SKPs ja sektori koguvarades oli 2019. aasta lõpu seisuga vastavalt 101% ja 63%[1]. Finantssektor on Eesti majanduse üks tugisambaid, mis esitab sektorile nõude olla stabiilne ja usaldusväärne. RahaPTS mõistes kohustatud isikute hulka kuuluvad kõik ettevõtted, mis tegutsevad finantssektoris, nimelt:

1) krediidiasutused;
2) finantseerimisasutused.

RahaPTS §-s 6 on toodud vastavate kohustatud isikute nimekiri. Järgnevasse tabelisse on koondatud käesolevas Eesti rahapesu ja terrorismi rahastamise siseriiklikus riskihinnangus finantssektorina käsitletud turuosalised:

**Tabel 20**. Finantssektori ülevaade

| Turuosalised | Turuosaliste arv seisuga 31.12.2019 | Turuosaliste arv seisuga 30.11.2020 | Kohustatud isikute arv | Erialaliidu või katusorganisatsiooni olemasolu |
|---|---|---|---|---|
| Krediidiasutused | 15 | 14 | 100% | Eesti Pangaliit |
| Krediidiandjad | 59 | 56 | 100% | Eesti Liisingühingute Liit, FinanceEstonia |
| Krediidivahendajad | 14 | 15 | 100% | FinanceEstonia |
| Investeerimisühingud | 5 | 5 | 100% | |
| Fondivalitsejad | 15 | 16 | 100% | |
| Tegevusloata väikefondi valitsejad | 27 | 37 | 100% | |
| Investeerimis- ja pensionifondid | 34 | 40 | 100% | |
| Väärtpaberituru osalised | 2 | 2 | 100% | |
| Elukindlustusandjad | 5 | 5 | 100% | Eesti Kindlustusseltside Liit, Eesti Kindlustusmaaklerite Liit |
| Kindlustusmaaklerid | 10 | 10 | 100% | |
| Makseasutused | 11 | 13 | 100% | |
| Makseagendid | 11 | 10 | 100% | |
| Ülepiiriliste makseteenuste pakkujate makseagendid | 3 | 3 | 100% | |
| Valuutavahetajad (MTG tegevusala järgi) | 44 | 38 | 100% | |
| Muud finantseerimisasutused[2] | 276 | 285 | 100% | Pole üldist katusorganisatsiooni, on mõnel teenuseliigil, nt Hoiu-Laenuühistute Liit |
| **Kokku** | **531** | **549** | **100%** | |

Riskihinnangu kontekstis võib sektori eripäraks pidada elektroonilise sideteenuse osutajaid (sideettevõtjaid), kes pakuvad oma klientidele tarbijakrediidi teenuseid (järelmaks) ning omavad

[1] https://www.eestipank.ee/finantsstabiilsus/ulevaade-finantssektori-struktuurist

[2] Majandustegevuse registri tegevusala "finantseerimisasutusena tegutsemine" järgi

krediidiandja tegevusluba. Elektroonilise side teenuste osutajad teostavad maksetehinguid, mis on tegevusloa kohustuse alt välistatud Makseasutuste ja e-raha asutuste seaduse (edaspidi MERAS) §-s 4 sätestatud välistusest tulenevalt (tegevusluba vaja ei ole ja pole ühtlasi RahaPTS-i subjektid), lähtudes seejuures MERAS § 4 lõike 4 toodud piirmääradest (maksetehing ei tohi olla suurem 50 € ja maksetehingute kogusumma ühe kasutaja kohta 300 € kuus) ja maksetehingute sisust.

**Õigusraamistik**

Hinnangu koostamise ajal kohalduvad Eesti finantssektorile lisaks Euroopa Liidu õigusaktidele[3], näiteks Euroopa Parlamendi ja Nõukogu Määrus (EL) 2015/847, muu hulgas alljärgnevad õigusaktid:

- rahapesu ja terrorismi rahastamise tõkestamise seadus (edaspidi RahaPTS),
- rahvusvahelise sanktsiooni seadus (edaspidi RSanS),
- maksualase teabevahetuse seadus, Rahandusministri 23.05.2018 määrus nr 25 „Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord".

Lisaks eeltoodud õigusaktidele reguleerivad sektoris osalejate tegevust eriseadused: krediidiasutuste seadus, krediidiandjate ja -vahendajate seadus, makseasutuste ja e-raha asutuste seadus, kindlustustegevuse seadus, investeerimisfondide seadus ja väärtpaberituru seadus.

Sektoris osalejate üle teostab järelevalvet Finantsinspektsioon ning finantseerimisasutuste puhul ka Rahapesu Andmebüroo. Seega kohalduvad finantssektoris tegutsevatele ettevõtetele lisaks ka Finantsinspektsiooni ja Rahapesu Andmebüroo juhendid:

- Krediidiasutustele, krediidiandjatele ja -vahendajatele, makseasutustele, e-rahaasutustele, kindlustusandjatele, kindlustusmaakleritele, investeerimisühingutele, fondivalitsejatele ja aktsiaseltsina asutatud investeerimisfondidele ning väärtpaberite keskregistrile kohaldub Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks". Kõik finantssektoris osalejad on kohustatud isikud RahaPTS-i järgi ning peavad oma tegevuses lähtuma ka Rahapesu Andmebüroo juhenditest: Rahapesu Andmebüroole esitatava teate vorm, Rahapesu Andmebüroole esitatava teate täitmise juhend, juhend kahtlusega tehingute tunnuste kohta, Rahapesu Andmebüroo soovitused kohustatud isikute tegevusest tulenevate riskide juhtimiseks, Rahapesu Andmebüroo soovitused protseduurireeglite ja sisekontrollieeskirja koostamiseks.

**Tabel 21.** Finantssektoris läbiviidud küsitluse andmed

| Alamsektor | Turuosaliste arv | Valimi maht | Valimi suurus/ nõutud vastuste arv | Väljasaadetud kutsete arv | Saadud vastuste arv | Vastamise määr |
|---|---|---|---|---|---|---|
| Krediidiasutused | 14 | kõik | 13 | 14 | 10 | 77% |
| Krediidiandjad | 55 | kõik | 48 | 55 | 26 | 54% |
| Krediidivahendajad | 14 | kõik | 13 | 14 | 3 | 23% |
| Investeerimisühingud | 5 | kõik | 5 | 5 | 4 | 80% |
| Fondivalitsejad | 15 | kõik | 14 | 15 | 8 | 57% |
| Tegevusloa väikefondi valitsejad | 28 | kõik | 26 | 28 | 3 | 12% |
| Väärtpaberituru osalised | 1 | kõik | 1 | 1 | 1 | 100% |
| Kindlustusandjad | 5 | kõik | 5 | 5 | 5 | 100% |
| Kindlustusmaaklerid | 46 | kõik | 41 | 46 | 11 | 27% |
| Valuutavahetajad | 43 | kõik | 39 | 43 | 9 | 23% |

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847

| | | | | | | |
|---|---|---|---|---|---|---|
| Makseasutused ja makseagendid | 21 | kõik | 20 | 21 | 12 | 60% |
| Sideoperaatorid | 3 | kõik | 3 | 3 | 2 | 67% |
| Ülepiiriliste makseteenuste pakkujate makseagendid | 3 | kõik | 3 | 3 | 2 | 67% |
| Muud finantseerimisasutused | 268 | valim | 158 | 268 | 54 | 34% |

Üldjoontes osales finantssektor NRA raames läbiviidud küsitluses aktiivselt. Vajadusel tehti lisaintervjuud nende alamsektorite esindajatega, kus piisavalt palju tagasisidet ei laekunud.

### 5.2. Riskide tüpoloogiate kirjeldus[4]

Üldlevinud eeldused rahapesu kuritegude toimepanemisele finantssektoris:

- Finantsteenuste pakkujate monitoorimise süsteemid ei suuda piisava efektiivsusega tuvastada kuritegeliku päritoluga rahavooge. Kuritegeliku päritoluga raha allikateks on eelkõige järgmised kuriteod:
  - Pettused (makse- ja kaardipettused, skimmingud[5], BEC kelmused[6], muud kelmused (sh püramiidskeemid, nn investeerimisteenused, rahamuulad));
  - Korruptsioonikuriteod ja maksukuriteod (altkäemaksu andmine ja võtmine, käibemaksu-, tulumaksu pettused jne);
  - Küberkuriteod (rünnakud arvutisüsteemidele, andmete kompromiteerimine (info vargused, manipulatsioonid), rünnakud infrastruktuuridele, finantssektorite süsteemide ründed, veebilehtede nakatamised viirusega, ebaseaduslikud krüptokaevandamised, ründed mobiilsete rahakottide vastu);
  - Narkootikumidega seotud süüteod;
  - Organiseeritud kuritegevus (eeltoodud kuriteod, organiseeritud kuritegelike ühenduste poolt);
  - Inimkaubandus.
- Finantsteenuse pakkuja ei suuda tuvastada tegelikku kasusaajat kliendi või tehingu vastaspoole keerulise omandistruktuuri või tegelike kasusaajate info puudulikkuse tõttu registris.
- Finantsteenuste pakkuja ei suuda tuvastada tehingut, mille vastaspooleks on riikliku taustaga isik, kas skriinimise süsteemi või riikliku taustaga isikute nimekirjade puudulikkuse tõttu.
- Finantsteenuse pakkuja korrespondentsuhetega seotud riskid, sh olukord, kus krediidiasutuse kliendiks on näiteks krüptovaluuta vahendust pakkuv ettevõte, kes ei ole oma klientide suhtes rakendavaid hoolsusmeetmeid nõuetekohaselt korralikult täitnud.
- Finantsteenuse pakkuja ei suuda rakendada vastavaid hoolsusmeetmeid mitteresidentidest klientide või e-residentidest klientide suhtes nende tegeliku riskitaseme tuvastamise keerukuse tõttu.
- Finantsteenuse pakkuja ei suuda tuvastada, kas fiktiivset tehingut (tehinguga seotud fiktiivsed dokumendid) või isikut (fiktiivsed isiku tuvastamise dokumendid).
- Kui Eesti krediidiasutused ja makseteenuse pakkujad keelduvad teostama välismakseid, siis isik võib kasutada rahapesuks ülepiirilisi finantsteenuste pakkujaid.
- Terrorismi rahastamise spetsiifiliste mehhanismide kindlakstegemise keerukuse tõttu ei suuda finantsteenuse pakkuja tuvastada terrorismi rahastamisele suunatuid tehinguid.

[4] Tüpoloogia põhineb riikliku ohuhinnangu finantssektori töörühma töö tulemustel

[5] skimming ehk kaardiandmete kopeerimine

[6] BEC on lühend mõistest `Business E-mail Compromise` ehk ärikirja pettus

- Massihävitusrelvade keerulisest spetsiifikast lähtuvalt ei suuda finantsteenuse pakkuja tuvastada massihävitusrelvade levikut soodustatavaid tehinguid.

## 5.3. Ohud[7]

### 5.3.1. Rahapesu ohud

**<u>Kuritegeliku raha sisenemise oht Eesti finantssüsteemi</u>**

Kurjategijad kasutavad finantssektorit oma kuritegelikul teel teenitud vara liigutamiseks vähemalt ühes kolmest rahapesu faasist (paigutamine, kihitamine, integratsioon). Eesmärk on majandustehingute abil peita kuritegelikku päritoluga vahendeid ning varjata nende tegelikku omanikku. Eestis on rahapesu eelkuriteoks iga kuritegu, ei eristata konkreetseid rikkumisi. Siiski on olulisem see, milliste kuriteoliikidega on võimalik teenida suuremat tulu, mida on vaja paigutada finantssektorisse, et saadud kasu tarbida võimalikult avalikult.

Eestis on enam esinevaks kuriteoliigiks, mille abil enam kuritegelikku tulu finantssüsteemi jõuab (küber)kelmused. Samuti maksudest hoidumisega seotud rikkumised, kusjuures mõlemad seonduvad nii riigisiseste kui ka väliste eelkuritegudega[8]. Kasutatakse ära Eesti väga mugavat ja kiiret pangandussüsteemi, mille kasutamiseks ei ole vaja olla riigis kohapeal.

Samas Eestiga seotud varasemate aastate rahapesu skandaalide kajastus maailma meedias ning kõrgendatud tähelepanu võib kurjategijaid hoida Eesti finantssüsteemi kasutamisest eemale. Lähtudes eeltoodust võib kuritegeliku raha sisenemise ohtu pidada „keskmiseks".

**<u>Tehingute läbipaistmatuse oht</u>**

Tehingute läbipaistmatus aitab kurjategijatel kiirelt liigutada rahalisi väärtusi finantssektoris, näiteks liigutades vara erinevate finantseerimisasutuste vahel või tehes tehinguid finantsinstrumentidega. Kui ei kontrollita, miks ja mille eest raha liigutatakse, siis annab see kurjategijatele võimaluse ära kasutada finantssektorit, et oma kuritegelikul teel saadud raha puhtaks pesta.

Eesti suuremates krediidiasutustes on võimatu liigutada suuri summasid nii, et krediidiasutus ei pööra sellele tähelepanu ning tehingu eesmärk ja sisu jääksid välja selgitamata. Keerulisemate skeemide puhul on piisava läbipaistvuse puudumise oht siiski olemas, seda eriti keerulise omandistruktuuriga ning spetsiifilise tegevusalaga ettevõtete puhul. Samuti on ohu tõenäosus suurem juhul, kui ettevõtte tegevusala muutub või tehingud toimuvad seotud isikute vahel. Väiksemate finantseerimisettevõtete puhul võivad taolised tehingud jääda vastava tähelepanuta kompetentse inimressursi puudumise tõttu. Lähtudes eeltoodust võib tehingute läbipaistmatuse ohtu pidada „kõrgeks keskmiseks".

**<u>Mitteresidentidest ja e-residentidest omanikega äriühingutega kaasnev oht</u>**

Eestis on äriühinguid kerge ja soodne luua ka mitteresidentidel või e-residentidel. Samuti tegutseb hulk äriühinguteenuse pakkujaid, kes loovad äriühinguid, mis müüakse kas mitteresidentidele või e-residentidele, ning müüja jääb ise Eestis dokumentide kättesaajaks, pakkudes ettevõttele näiliselt sidet Eestiga. Tegelikkuses Eestiga seos puudub ning ei ole selge või on väga keerukas välja selgitada, millise tegevusega rahalisi väärtusi liigutatakse. Kolmandatest riikidest pärit mitteresidentide ning e-residentide puhul on probleemiks ka asjaolu, et on piiratud või üldse puudub ülevaade isikute varasemast tegevusest.

[7] Põhineb ametiasutuste tunnetusel ning seni läbi viidud kriminaalmenetlustel

[8] Näiteks võib tuua kohtuotsuse kriminaalasjas nr 1-19-1400 (Eestis asuvate finantsasutuste kaudu Soome ettevõtte Xxx OY vastutavate isikute poolt maksupettuste ja raamatupidamiskuritegude tulemusel saadud rahaliste vahendite legaliseerimine sularahas väljavõtmise kaudu, rahaliste vahendite kogusumma rahaliste vahendite kogusummas 4 273 272 euro ). Samuti kohtuotsus kriminaalasjas 1-18-6825 (Soomes toimepandud maksupettuste ja raamatupidamiskuritegude tulemusel saadud rahaliste vahendite legaliseerimine Eesti finantssüsteemi kaudu. Eesti riigisiseste maksudest hoidumisega kaasnevate rahapesu näidetena võib tuua kriminaalasja nr 1-15-9048.

Eesti krediidiasutused ei ava kergelt arvelduskontosid mitteresidentidest ettevõtetele või Eesti ettevõtetele, millel Eestiga seos on olematu või väga väike. Muud finantseerimisasutused[9] ei esita selles osas sama karme nõudeid. Lähtudes eeltoodust võib mitteresidentidest ja e-residentidest omanikega äriühingutega kaasnevat ohtu pidada „madalaks keskmiseks".

**Virtuaalvääringutega seotud oht**

Digitaalselt rahaliste väärtuste liigutamisega on aina enam kõne all krüptovaluuta kasutamine. Eestis, nagu ka mujal maailmas, on kurjategijad üha enam kasutanud võimalust oma raha legaliseerimiseks kasutades virtuaalvääringuid. Krüptovaluuta rahakottide omanike osas on vähem läbipaistvust ning kuigi tehingute tegemine on tehniliselt küll kõigile avalik, siis selle taga olevad isikud jäävad siiski anonüümseteks. Tehingute peitmiseks kasutatakse hägustamismeetmeid, mis ei võimalda varade liikumist jälgida. Kui krüptoraha muundub rahaks (nn FIAT raha[10]), siis selle makse tegija on enamasti vahendaja ning ei pruugi nähtuda, kes on tegelikkuses vara omanik. Krediidiasutustel ja teistel finantsteenuste pakkujatel on raske kontrollida vara päritolu kui virtuaalvääringute vahendust pakkuv ettevõte ei ole hoolsusmeetmeid korralikult täitnud. Lähtudes eeltoodust võib virtuaalvääringutega seotud ohtu pidada „kõrgeks".

**Maksevahendajatega seotud oht**

Maksevahendaja eesmärgiks on klientidele pakkuda vaid makseteenust. Vahendajaid on palju ning ei ole võimalik piirata nende kaudu kuritegeliku vara liigutamist, kuna liigutatav raha ei jää maksevahendaja kontole ja vahendite liikumine toimub makse algataja ja saaja vahel. Eestis on maksevahendajatega seotud ohud kõrged eelkõige juhul, kui tarbijad kasutavad piiriüleste makseteenuspakkujate teenuseid, kelle tegevuse üle teostatakse kontrolli teenusepakkuja registrijärgses riigis, mistõttu on kurjategijatest klientide tausta ja tegevust keerukam kontrollida. Lähtudes eeltoodust võib maksevahendajatega seotud ohtu pidada „kõrgeks keskmiseks".

**Sularaha tehingute oht**

Sularaha on oma olemuselt anonüümne ning seetõttu on oht finantssüsteemi ärakasutamiseks, kui illegaalset sularaha paigutatakse finantssektorisse. Rahapesu oht esineb ka siis, kui kuritegelikul teel saadud tulu võetakse sularahas välja, et kaotada jälg kuritegeliku tulu ja selle tegeliku kasusaaja vahel.

Eestis on legaalses majanduses sularaha käive väike[11]. Maksudest kõrvalehoidumine või maksude tagastuse pettus ning (küber)kelmustega, narko- ja salakaubandusega teenitud tulu on sularaha mõistes Eestis võimalikeks ohukohtadeks, kus finantssektor võib kokku puutuda suures koguses ebaselge päritoluga sularahaga, mida soovitakse peita või legaalsesse majandusse suunata.
Lähtudes eeltoodust võib sularaha tehingute ohtu pidada „madalaks keskmiseks".

**Teiste riikide raha transiidi oht**

Võimalus kasutada kiiret finantssüsteemi lihtsalt ühe vahepeatusena annab kurjategijatele juurde kuritegeliku või ebaselge päritoluga raha kihistamise võimalusi. Kiired ülepiirilised rahavood riikidest, mis ei tee efektiivselt rahvusvahelist koostööd, annavad kurjategijatele võimaluse oma kuritegelikul teel teenitud tulu läbi finantssüsteemi legaalsesse ärisse suunata.

Eesti ärimaailmal on ärisidemeid nii endiste Nõukogude Liidu kui ka muude Ida-Euroopa riikidega[12], kelle jaoks oli varasematel aastatel Eesti finantssüsteem rahaliste vahendite liigutamise lüliks. Samuti on minevikus märkimisväärsed rahavood finantskeskustega, kellega hetkel on rahavood minimaalsed. Rahavoogudega seotud ohtudest kõige relevantsemaks ohuks on väliskaubandusega seotud rahavood. Krediidiasutustel on keeruline kontrollida raha ja isikute päritolu, kui kaup või teenused ei liigu läbi Eesti ning kohapeal Eestis äritegevust ei toimu, mistõttu tehingutega kaasneva dokumentatsiooni nõuetekohast täitmist ning tõepärasust ei ole tihtipeale võimalik kontrollida, et veenduda finantsasutustele esitatud

[9] Ettevõted, mis tegutsevad RAB poolt väljastatud tegevusloa "finantseerimisasutusena tegutsemine" alusel

[10] FIAT raha on valuuta millel pole sisemist väärtust ehk see pole tagatud nö "füüsilise kaubaga" (nt kuld)

[11] Euroopa Keskpanga maksestatistika andmetel Eestis tehakse sularahas ca 5% maksetest (2019)

[12] Statistikaameti poolt avaldatud väliskaubanduse statistika andmed

andmete ja teabe õigsuses. Lähtudes eeltoodust võib teiste riikide raha transiidi ohtu pidada „kõrgeks keskmiseks“.

**Kliendi osas hoolsusmeetmete rakendamata jätmise oht**

Klientide osas sobilike hoolsusmeetmete rakendamisega on võimalik finantssektorist eemale hoida isikuid, kes seda võiksid kuritarvitada. Vastasel juhul võivad kurjategijad rahalisi väärtusi liigutada läbi variisikute ja -ettevõtete, jättes tegeliku kasusaaja finantseerimisasutusele teadmata.

Eestis on krediidiasutuste puhul vastav oht väike. Hüpoteetiline oht eksisteerib kliendisuhete loomisel veebi vahendusel. Sel juhul on ohukohaks isikut tõendavate dokumentide suurem väärkasutus ning selle tõttu kontode avamine isikutele, kes selleks soovi pole avaldanud. Samas sellisel puhul on suuremahulise rahapesu võimalus piiratud riigi poolt seatud tehingute limiitidega. Väiksematel finantseerimisasutustel võib olla probleeme mitte-residentidest klientide soovitud määral tuvastamisega ning seetõttu võib sattuda finantssüsteemi rahalisi vahendeid, mille omaniku või päritolu osas kindlat selgust pole.
Lähtudes eeltoodust võib kliendi osas hoolsusmeetmete rakendamata jätmise ohtu pidada „madalaks“.

**Järeldus**

Üldiselt võib finantssektori rahapesu ohtude taset pidada keskmiseks. Kõige suuremaks ohuks Eesti finantssektori jaoks on rahavood, mis on seotud:

- Transiidiga SRÜ riikidest ning muudest Ida-Euroopa riikidest;
- Küberkuritegudest saadud vahendite liigutamisega Eesti virtuaalvääringute teenusepakkujate kaudu;
- Mitteresidentide või e-residentide Eestis registreeritud äriühingute tegevusega, mis ei toimu Eestis;
- Vahendustegevusega, mis on seotud teistes riikides tegutsevatele äriühingutele teatud teenuste pakkumisega;
- Äriühinguteenuse pakkujate poolt pakutavate teenustega;
- Maksudest kõrvalehoidumisega nii kohalikul kui ka rahvusvahelisel tasandil.

**Tabel 22**. Rahapesu ohutase finantssektoris

| Sektor | Rahapesu ohutase sektori tasandil | |
|---|---|---|
| Finantssektor | 2,74 | **keskmine/madal** |

Üldjoontes leiti, et rahapesu ohutase finantssektoris on **keskmine/madal**.

### 5.3.2. Terrorismi rahastamise ohud

**Finantsteenuste pakkujate ebapiisav teadlikkus ja sellega kaasnev terrorismi rahastamise suhtes rakendatavate hoolsusmeetmete ebapiisavuse oht**

Eesti väikeriigina ei ole oma geograafilise asukoha ning väikesearvulise moslemikogukonna tõttu terroriaktide toimepanemiseks islamiäärmuslaste jaoks prioriteediks. Samas on Eesti lähinaabruses Skandinaavias ja Venemaal suured moslemikogukonnad, mistõttu mitmed islamiäärmuslikult meelestatud isikud kasutavad Eestit transiitriigina. Siinne soodne majanduskeskkond ning kinnisvaraturg on äratanud aktiivset ärihuvi ka eelmainitud kogukondades. Traditsiooniliste finantsteenuste pakkujate puhul on teadlikkus terrorismi rahastamise ohtudest viimaste aastate lõikes paranenud ning rahapesu tõkestamise üksuste töö tõhustunud. Rakendatud hoolsusmeetmed ning konservatiivne lähenemine mitteresidentide ning e-residentide puhul vähendab märkimisväärselt ka terrorismi rahastamise ohutaset traditsiooniliste finantsteenuse pakkujate puhul. Samas on traditsioonilised finantsteenuse pakkujad konkurentsikeskkonnas surve all kaasa minna uuendustega, tehes koostööd makse– ja virtuaalvääringu teenuse pakkujatega. Eesti innovaatiline ning arenenud finantssektor võib olla atraktiivne

islamiäärmuslaste jaoks terrorismi rahastamise ning toetamise seisukohast, mistõttu tuleb hinnata ohutaset keskmiseks.

- Maksevahendajatega ning virtuaalvääringutega seotud oht

Islamiäärmuslikku vaadet omavate isikute ning rühmituste seas on traditsioonilised (pangad, valuutavahetajad) terrorismi rahastamise kanalid asendumas alternatiivsete ning anonüümsete piiriüleste makseteenuste ning virtuaalvääringu teenuse osutajatega. Kui makseteenuse osutajate puhul on tehingus osapooled osaliselt varjatud, siis virtuaalvääringud tagavad täieliku anonüümsuse. See on kaasa toonud selle, et terroriorganisatsioonid kutsuvad avalikult oma tegevust toetama kas kombineeritult: „makseteenuse osutaja + virtuaalvääring“ või ainult virtuaalvääringus. Samuti ei ole tugevdatud hoolsusmeetmete kohaldamine vaid tehingu piirmäärade ületamisel enam asjakohane ega tõhus (paljud turuosalised lähtuvad jätkuvalt 10 000 euro piirist). Enamik terrorismi rahastamise kahtlusega tehingud on teostatud väikestes summades (sageli alla 10 euro). Lähtudes eeltoodust võib maksevahendajate ning virtuaalvääringutega seotud ohtu pidada „kõrgeks“.

**Järeldus**
Finantssektoris on terrorismi rahastamise oht turuosaliste lõikes erinev: kindlustus- ning investeerimisteenust pakkuvate turuosaliste seas võib ohutaset hinnata madalaks, krediidi- ja finantseerimisasutuste, makseteenuse- ning valuutavahetuse teenuse pakkujate puhul võib seda hinnata keskmiseks, samas kui turuosalised teenindavad virtuaalvääringu teenuse pakkujaid, siis ohtu võib pidada kõrgeks.

## 5.4. Haavatavused

### 5.4.1. Rahapesu tõkestamise haavatavused

#### 5.4.1.1. Kokkupuude ohuga

- Kuritegeliku raha sisenemise oht: Justiitsministeeriumi poolt edastatud kuritegude statistikast nähtub, et 2019. aastal oli Eestis registreeritud 10 657 kuritegu, millest saadud kuritegelik tulu võib olla hüpoteetiliseks rahapesu allikaks. Sellisteks kuritegudeks on korruptsioon ja altkäemaks, väljapressimine, pettus, maksukuriteod, küberkuriteod, võltsimised, vargused, ebaseaduslik kauplemine narkootiliste ja psühhotroopsete ainetega jne. Neis kuritegudes oli 2019. aastal arestitud vara 7,86 mln euro väärtuses.
- Tehingute läbipaistmatuse oht: Riikliku ohuhinnangu käigus turuosaliste seas läbiviidud küsitluse küsimusele kas turuosalised on tuvastanud „kahtlasi ja/või ebaselge päritoluga rahavoogusid, mille eesmärk on varjata tegelikke kasusaajaid ja/või vara päritolu“ saadi „jah“ vastus 80%-lt krediidiasutustest[13].
- Mitteresidentidest ja e-residentidest omanikega äriühingutega kaasnev oht: vastavalt Registrite ja Infosüsteemide Keskuse poolt edastatud andmetele on Eestis registreeritud[14]:

**Tabel 23**. Mitteresidendist kasusaajaga äriühingute arvud aastatel 2018-2020

| | 2018 | 2019 | seisuga 07.2020 |
|---|---|---|---|
| Äriühingud, millel on vähemalt üks mitteresidendist tegelik kasusaaja | 10 206 | 15 408 | 14 610 |
| Mitteresidendist tegeliku kasusaajaga ühingute osakaal kõikidest ühingutest | 5,26% | 7,26% | 6,62% |

[13] Antud juhul tuuakse krediidiasutuste näide, kuna sektori osakaal rahavoogudes on domineeriv (ca 99% Eesti Panga ja Finantsinspektsiooni maksete statistika alusel).
[14] NRA käigus RIK vastus päringule.

- Virtuaalvääringutega seotud oht: Rahapesu andmebüroo poolt läbiviidud „Virtuaalvääringu (VV) teenuse pakkujate uuringust“ selgub, et 2020. aasta 1. augusti seisuga kehtis erinevaid virtuaalvääringuga teenusepakkujate tegevuslubasid kokku 611 (295 VV raha vastu vahetamise teenuse, 261 rahakotiteenuse ja 55 VV teenuseluba)[15]. Samuti küsitluse tulemused näitavad, et Eesti turul tegutsevate virtuaalvääringute teenuste pakkujate vahendatud teenuste kogukäive on kiiresti kasvanud. Kui 2018. aastal oli see suurusjärgus 590 miljonit eurot, siis 2019. a esimesel poolaastal juba kaks korda kõrgem – 1,2 miljardit eurot.[16]
- Maksevahendajatega seotud oht: kuna oht on seotud peamiselt ülepiiriliste makseteenuse pakkujatega, siis riikliku ohuhinnangu käigus neile saadetud küsimustele alates 2017. aastast Eesti residentidele osutatud teenuse mahu kohta on saadud vastused, mille kohaselt võrdub vastav näitaja 250 mln euroga.
- Sularaha tehingute oht: Maksu- ja Tolliameti poolt edastatud Eesti piiril sularaha deklareerimise statistikast järeldub, et Eesti piiridel on perioodil 2017-2019 deklareeritud sularaha summas kokku 193,4 mln eurot (nii suunaga kolmandatest riikidest Eestisse kui ka Eestist kolmandatesse riikidesse).
- Teiste riikide raha transiidi oht: Eesti Pangale krediidiasutuste poolt esitatavast maksete statistikast selgub, et piiriüleste maksete maht oli 2017. aasta III kvartalis 11,7 mlrd eurot makstavad maksed ja 14,6 mlrd eurot laekuvad maksed ja 2020. aasta III kvartalis 14,1 mlrd eurot makstavad maksed ja 18,8 mlrd eurot laekuvad maksed (sisaldab kõikide klientide makseid, sh keskvalitsus, finantseerimisasutustest kliendid jne).
- Kliendi osas hoolsusmeetmete rakendamata jätmise oht: kui seostada vastavat ohtu variisikute kasutamisega, siis NRA käigus turuosaliste seas läbiviidud küsitluse küsimusele „kas olete tuvastanud juhtumeid, kus on tekkinud kahtlus, et tegu on variisikutega“ saadi „jah“ vastus 60%-lt krediidiasutustest.
- Lähtudes eeltoodust võib järeldada, et Eesti finantssektor puutub eeltoodud ohtudega kokku reaalselt, kusjuures ohtudega kokkupuude taset võib pidada ´kõrgeks keskmiseks´.

### 5.4.1.2. Riskiteadlikkus

**Juhtkonna pühendumine ja juhtroll**

Küsitluse tulemused teadlikkuse osas:

NRA raames läbiviidud küsitluse tulemused näitavad seda, et sektori teadlikkus rahapesu tõkestamisest on väga kõrge. Selle põhjuseks võib lugeda asjaolu, et finantssektor on panganduskeskne, krediidiasutusi aga võib pidada selles osas kõige edasijõudnumaks sektoriks. Krediidiasutused investeerivad nii automaatsetesse rahapesu ja terrorismi rahastamise tuvastamise lahendustesse, protseduurireeglitesse kui ka töötajate regulaarsesse koolitamisse. Järgitakse väljatöötatud suuniseid ning FI ja RABi juhendeid, millest on pankade sõnul praktiline kasu. Samas, näiteks, makseasutuste poolt on välja toodud ühiskonnas teadlikkuse tõstmise vajadus läbi koolituste. See näitab soovi ja tahet valdkonnapõhiselt parema riskide tuvastamise protsesside/meetodite/juhendite saavutamiseks ja koostöövalmidust järelvalveasutustega. Erandiks võib pidada tegevusloata väikefondi valitsejaid, kelle teadlikkus rahapesu tõkestamisest on keskpärane. Sektor on teadlik sellest, et rahapesu tõkestamine on oluline teema, kuid sektor on valdavalt asunud seisukohale, et tulenevalt sektori spetsiifikast ei ole rahapesu tõkestamine konkreetses sektoris oluliseks teemaks, st sektoris ei tõusetu rahapesuga seotud riske sellises mahus nagu muude finantseerimisasutuste puhul (mh seetõttu, et väikefondivalitsejad ei hoia investorite rahalisi vahendeid).

Sektori teatamise statistikat toetab küsitluse raames saadud tagasiside, mille kohaselt enamus turuosalisi on kahtlastest tehingutest teavitanud Rahapesu Andmebürood (krediidiasutused 100%). Sektor täidab eeskujulikult oma teatamiskohustust: saadetakse teatiseid nii rahapesu-kahtluse põhiselt kui ka summapõhiselt: kõige suuremaks RABile teatajaks on krediidiasutused, kelle edastatud teadete arv oli 2017. ja 2018. aastal sarnases mahus (vastavalt 2317 ja 2208 teadet), kuid 2019 aastal oli teateid üle 600

[15] Majandustegevuse registri andmete alusel seisuga 31.12.2020 kehtis erinevaid virtuaalvääringuga teenusepakkujate tegevuslubasid kokku 478 (39 VV raha vastu vahetamise teenuse, 34 rahakotiteenuse ja 405 VV teenuseluba).

[16] RAB “Virtuaalvääringu teenuse pakkujate uuring” 22.09.2020

rohkem, kokku 2905 teadet. Tõus oli tingitud just ebaharilike tegevuse teadete esitamise mahtudest. Teiseks suurimaks teatajaks on maksevahendajad (2017 – 1155 teadet, 2018 – 962 teadet ja 2019 – 568 teadet). Makseasutuste poolt esitatav teadete suur arv on seotud summapõhiste teavitustega, milline kohustus näiteks krediidiasutustel puudub. Edastatud teadete arvu poolest kolmandaks teatajaks on arveldus- ja sularahasiirdajad.

**Lühikokkuvõte**

Võttes kokku nii küsitluse tulemusi kui ka Rahapesu Andmebüroole teavitamise statistikat, võib öelda, et finantssektori rahapesu riskiteadlikkus on kõrgel tasemel ning iga aastaga muutub veel paremaks. See väljendub nii turuosaliste juhtkonna kui ka töötajate pühendumises, mis omakorda väljendub nii investeeringutes rahapesu ja terrorismi rahastamise tuvastamise lahendustesse ja töötajate koolitamisse kui ka panustamises Rahapesu Andmebüroo teavitamisse. Samas esineb jätkuvalt vajadus tõsta teadlikkuse taset sektori väiksemate turuosaliste gruppide seas (tegevusloata väikefondi valitsejad, finantseerimisasutused).

### 5.4.1.3. Õigusraamistik ja kontroll

**Järelevalve kvaliteet**

Kontrollimeetmed koosnevad hinnangutest peamiselt kahele aspektile: regulatsioonide tase ja järelevalve piisavus/ebapiisavus.

Regulatsioonide tase on finantssektoris väga kõrge. Sektoris osalejatele kohalduvad eriseadused sätestavad tegevusloa nõude suuremale osale finantsteenuste osutajatest, mis aitab tagada finantssektoris tegutsevate ettevõtete ja kogu finantssektori usaldusväärsuse ja järelevalve kehtestatud nõuete täitmise üle. Tegevusloa nõue on kehtestatud krediidiasutustele, krediidiandjatele ja -vahendajatele, kes pakuvad krediiti tarbijatele, makseasutustele, e-raha asutustele, kindlustusandjatele, kindlustusmaakleritele, investeerimisühingutele, fondivalitsejatele ja aktsiaseltsina asutatud investeerimisfondidele ning väärtpaberite keskregistrile. Eriseadused reguleerivad detailselt vastaval tegevusalal tegutsevate ettevõtete tegevusele esitatavaid nõudeid, aga väga kõrged nõudmised seatakse ka finantssektoris osalejatele endile, et tegevusloa saamiseks kvalifitseeruda. Hindamisel pööratakse suurt tähelepanu lisaks tehnilisele ja finantsilisele valmisolekule ka sektoris osaleva ettevõtte omanike ning juhtorgani liikmete reputatsioonile ja usaldusväärsusele (*fit-and-proper*-nõuded), samuti seatakse tingimused võtmetöötajatele. Kõik finantssektoris osalejad on kohustatud isikud RahaPTS-i kohaselt, mis seab omakorda sektorile spetsiifilised kohustused rahapesu tõkestamise aspektist. Seega on hinnang regulatsioonidele kõrge.

Reguleeriva organi rolli täidab Finantsinspektsioon (va tegevusloata väikefondi valitsejad ja finantseerimisasutused), kus on 2020. aasta seisuga rahapesu tõkestamise järelevalvele spetsialiseerunud 7 täiskohaga järelevalveametnikku, kes koos muude funktsioonidega tegeleb rahapesu tõkestamisega. FI-s on 2020. aasta seisuga 113 täistöökohaga töötajat. Järelevalve kvaliteet antud sektoris on kõrge. Järelevalve tõhusust mõjutab negatiivselt haldustrahvide puudumine, sest ei võimalda rikkumiste puhul määrata proportsionaalseid ja mõjusaid sanktsioone. Probleemiks on ka trahvisummade suurus, mis ei vasta Euroopa Liidu rahapesu tõkestamise direktiivile.

Lisaks järelevalveorganitele panustavad ka erialaorganisatsioonid oma liikmete toetamisse ning koostavad abimaterjale RahaPTS-ist tulenevate nõuete täitmiseks. Krediidiasutusi ühendatav erialaorganisatsioon on Pangaliit, kes panustab liitu kuuluvate ettevõtete koostöösse ja koolitustesse. Avaliku- ja erasektori huve ühendav finantssektori esindusorganisatsioon MTÜ FinanceEstonia on koostanud juhised krediidiandjatele ja -vahendajatele ettevõtte riskihinnangu koostamiseks, mis on heaks kiidetud ka järelevalveasutuste poolt. Eesti Kindlustusseltside Liit on loonud kindlustuse hea tava ning sektor enda tegevust reguleerinud ka teatud määral Liidu põhikirjaga ja eneseregulatsioon tuleb lugeda toimivaks ja täiendavaks, arvestades riigipoolse regulatsiooni detailsusastet.

Samas tunnetavad näiteks makseasutused, et neil ei ole piisavalt tuge erialaorganisatsioonidelt ning neid ei kaasata piisavalt rahapesu ja terrorismi rahastamise tõkestamist puudutavatesse aruteludesse. RAB

tegevusloaga tegutsevatel tegevusloata väikefondivalitsejatel puudub erialaliit, kes jagaks selgitusi ja kujundaks ühtse seisukoha rahapesu tõkestamisega seotud teemades. Nemad pidasid ka järelevalveasutuste poolset teavitustööd väheseks.

**Lühikokkuvõte**

Üldiselt on sektori regulatsioonide ja järelevalve kvaliteedi tase kõrge. Erialaorganisatsioonid panustavad sektori regulatsioonide taseme tõstmisesse ja selgitustöösse juhendmaterjali koostamise ja koolituste läbiviimise kaudu. Samas on väiksem rühm turuosalisi, kel puudub erialaorganisatsioon (nt makseteenuse pakkujad) või ressursi nappuse tõttu on seni järelevalve olnud ebapiisav (tegevusloata väikefondi valitsejad), mis vajab suuremat tähelepanu.

**Vastavuskontrollisüsteemide ja aruandluse tõhusus**

Sektoris kehtivad aruandluse nõuded kehtestatakse eriseadustes, mille järgi esitavad turuosalised aruanded nõutud sagedusega Eesti Pangale ja Finantsinspektsioonile, kus saadud andmete alusel teostatakse teenusepõhiselt rahapesuriskide analüüsi.

Turuosaliste vastavuskontrollisüsteemide tõhusust võib hinnata küsitlustest saadud tulemuste põhjal järgmiselt:

- Vastavuskontrollisüsteemide piisavust hinnatakse regulaarsel alusel[17];
- Suurima mõjuga turuosaliste seiresüsteemid on automatiseeritud[18], reeglina on ka teiste turuosaliste seiresüsteemid automatiseeritud vastavalt teenuste mahtudele[19];
- Suurima mõjuga turuosalistel on majanduskuritegude avastamise süsteemid, rakendatakse riskipõhist lähenemist[20];
- Tehingute seire stsenaariumide valik ja kalibreerimine on reeglina kooskõlas üksuse profiili ning sellest tulenevate riskidega[21], samas on teatud turuosalistel selles osas arenguruumi, et muuta nende võimekus veelgi kõrgema-tasemelisemaks, võimaldades reaalajas tehingute jälgimist ja peatamist ning olles senisest enam riskitundlikumad[22];
- Suurima mõjuga turuosaliste tehingute seiresüsteemid võimaldavad tuvastada teatuid keerukaid või ebatavalisi tehinguid, kuid peaksid olema senisest enam riskitundlikud[23];
- Enamuse turuosaliste puhul on kasutusel kliendi riskitaseme riskipõhist arvutamist võimaldav süsteem[24];
- Enamus turuosalisi investeerib riskijuhtimise tehnilistesse lahendustesse ning peamiselt panustatakse programmidesse ja tarkvarasse[25].

**Lühikokkuvõte**

Üldiselt on sektori vastavuskontrollisüsteemide ja aruandluse tõhusus kõrge[26].

**Kliendi suhtes rakendatavate hoolsusmeetmete raamistiku kvaliteet**

Hoolsusmeetmete üldkirjeldus

RahaPTS sätestab üldised hoolsusmeetmed, mille kohaldamisel tuleb üldkorras teha minimaalselt järgmist:

[17] Krediidiasutuste, makseasutuste, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[18] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[19] Fondivalitsejate, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[20] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[21] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[22] Fondivalitsejate, investeerimisühingute küsitluste tulemuste põhjal

[23] Krediidiasutuste, makseasutuste, investeerimisühingute, eluskindlustusseltside küsitluste tulemuste põhjal

[24] Krediidiasutuste, fondivalitsejate, makseasutuste, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[25] Krediidiasutuste, makseasutuste, investeerimisühingute, elukindlustusseltside, krediidiandjate küsitluste tulemuste põhjal

[26] Erandiks on muud finantseerimisasutusedm kelle puhul vajavad vastavuskontrollisüsteemid hindamist ja arendamist

- kliendi või juhuti tehtavas tehingus osaleva isiku isikusamasuse tuvastamine ning esitatud teabe kontrollimine,
- esindaja isikusamasuse ja esindusõiguse tuvastamine ning kontrollimine,
- tegeliku kasusaaja tuvastamine ja tema isikusamasuse kontrollimiseks meetmete võtmine ulatuses, mis võimaldab kohustatud isikul veenduda selles, et ta teab, kes on tegelik kasusaaja, ja saab aru kliendi või juhuti tehtavas tehingus osaleva isiku omandi- ja kontrollistruktuurist, ärisuhtest, juhuti tehtavast tehingust või toimingust arusaamine,
- teabe hankimine asjaolu kohta, kas isik on riikliku taustaga isik, tema pereliige või tema lähedaseks kaastöötajaks peetav isik ja ärisuhte seire.

RahaPTS sätestab ka erinõudeid mida peavad kohaldama krediidi- ja finantseerimisasutused RahaPTS tähenduses. Näiteks RAB kontaktisiku määramise nõue (RahaPTS § 17 lg 2), keeld luua või jätkata korrespondentsuhteid varipankadega ja selliste krediidiasutuste või finantseerimisasutustega, kes teadaolevalt lubavad varipankadel oma kontosid kasutada (RahaPTS § 18 lg 2), nõuded isikusamasuse tuvastamiseks infotehnoloogiliste vahendite abil (RahaPTS § 31), keeld osutada teenuseid, mida on võimalik kasutada ilma tehingus osalevat isikut tuvastamata ja esitatud teavet kontrollimata, kohustus konto avada ning kontot pidada kontoomaniku nimel, keeld sõlmida lepingut või teha otsust anonüümse konto, hoiuraamatu või hoiulaeka avamise kohta (RahaPTS § 25).

Kliendikontrolli raamistiku kvaliteedi osas läbiviidud küsitluse käigus leitud haavatavused:

- Puudub riikliku taustaga isikute register, riikliku taustaga isikute, nende pereliikmete ja lähedaste kaastöötajate tundmise ja seire ajakohase ning usaldusväärse kvaliteedi saavutamine on keeruline[27];
- Tegelike kasusaajate andmete üle kontrolli puudumine registrisse kandmisel ja vastava teabe uuendamisel[28];
- Tegelike kasusaajate teabe uuendamise protsess ei ole vastavuses otseste ja kaudsete omanike andmete muutumisega Äriregistris või väärtpaberite keskdepositooriumis[29];
- Mitteresidentidest juriidiliste isikute tegelike kasusaajate ajakohase teabe kättesaadavus registritest erineb välisriikide lõikes, teabe kvaliteet varieerub ja on vastuoluline[30];
- Juurdepääs suure riskiga klientide (nt saatkonnad, virtuaalvääringute pakkujad) infole on ebaühtlase kvaliteediga[31],[32];
- Tegevusloata väikefondivalitsejate poolt kliendi suhtes rakendavate hoolsusmeetmete suurim probleem on klientide ringi kindlaksmääramine, kelle osas üleüldse tuleks hoolsusmeetmeid kohaldada. Sektoris valitseb pigem arusaam, et klientideks on väikefondide investorid, mitte aga portfellettevõtjad, kellesse investeeritakse. Eeltoodust tulenevalt jäävad mitmed hoolsusmeetmed kohaldamata paljude isikute (s.o portfellettevõtjate) suhtes, kelle osas hoolsusmeetmeid kohaldama peaks ja kohaldatavaid hoolsusmeetmeid ei kohaldata teadlikult. Samas kohaldatakse iga portfellettevõtja suhtes väga põhjalikku tundmaõppimist, s.h tehakse põhjalik ja kvaliteetne analüüs portfellettevõtja ärimudelile ehk valitakse hoolsusmeetmete kohaldamisel reeglina mitte formaalne ja protseduuril põhinev lähenemine, vaid kliendi sisulisel tundmaõppimisel baseeruv lähenemine[33].

**Lühikokkuvõte**

[27] Krediidiasutuste, fondivalitsejate, makseasutuste, elukindlustusseltside, valuutavahetajate küsitluste tulemuste põhjal

[28] Krediidiasutuste, fondivalitsejate küsitluste tulemuste põhjal

[29] Töögrupi arutelu tulemus küsitluste põhjal

[30] Töögrupi arutelu tulemus küsitluste põhjal

[31] Krediidiasutuste küsitluste tulemuste põhjal

[32] Töögrupi arutelu tulemus küsitluste põhjal

[33] Tegevusloata väikefondivalitsejate intervjuu tulemuste põhjal

Hoolsusmeetmete raamistiku kvaliteet on kõrge. Kliendikontrolli seisukohalt on suurematekss probleemideks riikliku taustaga isikute registri puudumine, samuti tegeliku kasusaaja tuvastamise protsessi keerukus ning usaldusväärse allika puudumine.

#### 5.4.1.4. Sektoriomaste riskide hindamine sektoripõhiste kontrollide kvaliteediga

Sektoriomaste riskide analüüsimisel ja hindamisel on tuvastatud järgmised haavatavad kohad:

- Rahapesu eesmärgil saatkondade kontode kuritarvitamise tuvastamise keerukus[34];
- Rahapesu eesmärgil mittetulundusühenduste ja heategevusorganisatsioonide kuritarvitamise tuvastamise keerukus[35];
- Inimkaubandusega seotud rahavoogude tuvastamise keerukus[36];
- Virtuaalvääringutega seotud kahtlaste tehingute kindlakstegemise keerukus[37].

**Lühikokkuvõte**

Esineb raskusi spetsiifiliste teenuste osutamisega ja valdkondadega seonduvate riskide tuvastamisega. Uudsete teenuste ja lahendustega seotud riskidest teadlikkus on soovitust madalam.

#### 5.4.1.5. Varasemate hindamiste käigus tuvastatud riskidele reageerimise kvaliteet

Varasemate hindamiste käigus on leitud, et finantssektori karistused ja hoolsusmeetmete jõustamise efektiivsus võiksid olla suuremad. Riskide maandamiseks on RahaPTS-is tõstetud rahapesu tõkestamise-alaste sanktsioonide piirmäära, st maksimaalne rahatrahv kohustuse rikkumise eest on nüüdseks 400 000 eurot. Samas on karistuste määramise mehhanism endiselt puudulik ning väga mitmete ja eritahuliste probleemidega.

Samuti toodi välja, et keerukate omandistruktuuride puhul on keeruline tuvastada tegelikku kasusaajat. Riski maandamiseks on Eestis 2018. a loodud äriregistris peetav ja avalikult ligipääsetav tegelike kasusaajate register, kuhu äriühingud kohustuvad märkima oma tegelike kasusaajate andmed.

Rahapesu-alastes kuritegudes on varasemalt toodud välja arvutikelmust, kui kõige enam toime pandud ja kõrge riskiga rahapesu valdkonda. Sellega seoses viidati lisaks, et kohati võib olla keeruline tuvastada kuriteoga saadud vara ning seda eristada muust varast. Seetõttu on lisatud KarS §-i 213 lõige 4, mille kohaselt võib arvutikelmuse toimepanemisel saadud varale kohaldada laiendatud konfiskeerimist, ehk konfiskeerida osa või kogu kuriteo toimepanija vara, kui on alust arvata, et isik on saanud vara kuriteo toimepanemise tulemusena või sellise vara arvel.

Antud sektori osas keskenduti Moneyval 4. hindamisvoorus panganduse- ja väärtpaberisektorile ning käsitleti peamiselt konkreetsete teenustega seotud rahapesu riske. Finantsinspektsioon võttis toodud tähelepanekud arvesse ning neid jälgitakse nii kohapealsete- kui ka kaugkontrollide teostamisel.

Järgmises tabelis on toodud peamised SNRA (2017/2019) leiud ning nendega seotud need ohud ja haavatavused Eesti kontekstis, mis ei ole käesolevas peatükis detailselt käsitletud:

[34] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[35] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[36] Krediidiasutuste küsitluste tulemuste põhjal

[37] Töögrupi arutelu tulemus küsitluste põhjal

**Tabel 24.** SNRA (2017/2019) leitud ohud ja haavatavused Eesti kontekstis

| SNRA | Eesti ohud ja haavatavus[38] |
|---|---|
| Privaatpangandus ja institutsionaalsed investeeringud (eriti läbi maaklerite) ning safe custody teenused[39] | Eestis on privaatpanganduse (PP) kliendiks saamise tingimised väga madalad. Sellest tulenevalt tuleb pöörata tähelepanu eelkõige kõrgema väärtusega PP klientidele, kelle hulk Eestis on väike. PP teenuste osutamine mitteresidentidele tänasel päeval sisuliselt puudub. Oht on keskmine. Teadlikkus ja maandamismeetmed on olemas. Haavatavus on selle tõttu madal. |
| 500 ja 200 euroste kupüüride kasutamine | Eestis sularaha osakaal majanduses madal. Seetõttu risk on keskmine. Teadlikkus ja riskide maandamise protsessid on paigas. Haavatavus on madal. |
| Professionaalne jalgpall, korruptsioon ja rahapesu | Eesti jalgpall ei ole nii kõrgelt hinnatud ega tasustatud. |
| Vaba majanduspiirkonna sadamad (free ports) | Eestis on vabasadamad olemas, kuid praktikas ei ole teada nende kasutamist rahapesu toimepanemiseks. |
| Investeeringute eest kodakondsuse/elamislubade andmine („golden visas“) | Ei ole teada, et mitteresidendid eelistaksid kasutada Eesti elamislubasid, kuna sisse on viidud erinevad tingimused ning toimub kontroll elamislubade üle. Eelistatakse teiste riikide sarnaseid võimalusi. |
| Inimkaubandus (human trafficing) | Eesti ei ole väga tugevalt esindatud ei potentsiaalse siht- ega transiitriigina. Meil on üksikuid kaasuseid eesmärgiga Venemaalt saabuvaid immigrante suunata Lääne-Euroopasse, kuid tegemist on pigem üksikjuhtumitega. |
| Eksootilise floora ja fauna salakaubandus (wildlife trafficking) | Eestis ei ole tuvastatud vastavaid kaasuseid ning Eesti puhul ei ole teada, et on nõudlus eksootilise floora ja fauna esindajate järele. |

#### 5.4.1.6. Järeldus

Skaalal 1-5 on finantssektori haavatavuse hinne rahapesu aspektist 2,69 ehk **keskmisest madalam**.

**Tabel 25.** Rahapesu haavatavuse tase finantssektoris

| Sektor | Rahapesu haavatavuse tase sektori tasandil | |
|---|---|---|
| Finantssektor | 2,69 | **keskmine/madal** |

Sektori tugevamateks külgedeks saab pidada head järelevalvet tegevusloakohustust omavate sektoriosaliste üle ja tugevat õigusraamistikku. Samuti on olulist rolli mänginud Eesti pankasid tabanud suuremahuliste rahapesuskandaalide laine, millest on õpitud ning vastavad süsteemid muutusid veel tõhusamaks.

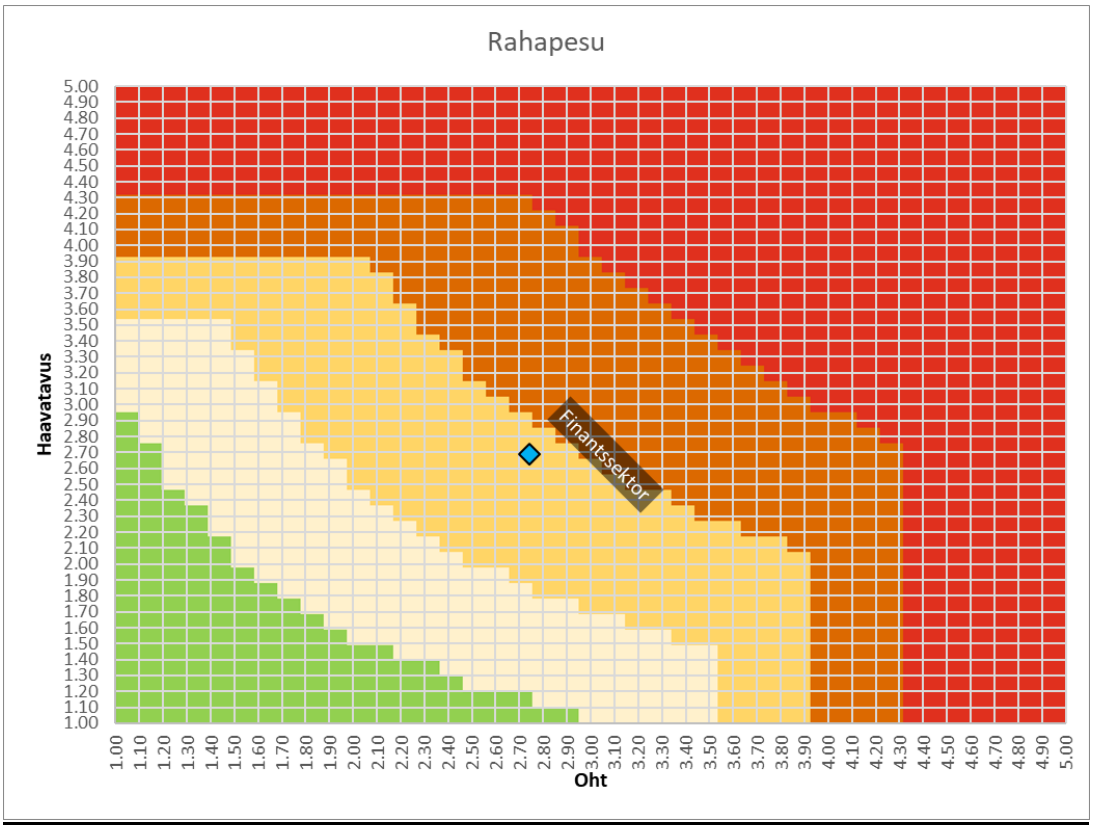
Järelevalve seisukohalt on haavatavamateks kohtadeks järelevalve tegevusloata väikefondide valitsejate ja muude finantseerimisasutuste üle (ehk Rahapesu Andmebüroo järelevalvesubjektid), millest võib järeldada, et antud sektori turuosaliste teadlikkust on tarvis sektorisiseselt tõsta.

Hoolsusmeetmete rakendamise seisukohalt on nõrkadeks kohtadeks peetud tegelike kasusaajate registri andmete usaldatavust ja juurdepääsu riikliku taustaga isikute teabele nii siseriiklikult kui ka rahvusvaheliselt. Antud aspekt vajab lahendamist riiklikul tasandil.

[38] Hinnangud põhinevad riikliku ohuhinnangu finantssektori töörühma töö tulemustel

[39] Safe custody teenused seisnevad kliendile väärtuslike füüsiliste esemete hoiustamiseks seifi või muu turvalise hoiuruumi pakkumises

**Joonis 4.** Finantssektori rahapesu riskitaseme soojuskaart




**Kokkuvõte**

Sektori haavatavuse taseme paiknevus riiklikul pildil on teiste sektorite keskel ning keskmisest madalama hinnangu tasemel. Seega finantssektori haavatavust rahapesu suhtes võib pidada aktsepteeritavaks, kuid on turuosalisi, kelle puhul peab tõstma rahapesu tõkestamise teadlikkust. Samas on teatud turuosalistel selles osas arenguruumi, et muuta nende võimekus veelgi kõrgema-tasemelisemaks, võimaldades reaalajas tehingute jälgimist ja peatamist. Sektoris tuleb rakendada hoolsusmeetmeid tavakorras.

### 5.4.1.7. Riskimaandamise strateegia

#### 5.4.1.7.1. Leevendavad meetmed riiklikul tasandil

Riskihinnangu tulemustest lähtudes tehakse järgmised ettepanekud olukorra parandamiseks riiklikul tasandil:

- Riikliku taustaga isikute andmebaasi loomine;
- RABi poolset sekkumist/järelevalvet tuleb tõhustada RAB tegevusloa alusel tegutsevate turuosaliste puhul;
- Äriregister: tegelike kasusaajate info korrastamine (olemas 100% tegelikest kasusaajatest), kontroll (andmed vastavad tegelikkusele) ja vastavate karistuste karmistamine (seadusandluse muutmine), uuendamine. Osaluse sidumine tegeliku kasusaajaga;
- Pikemas perspektiivis hoolsusmeetmete rakendamise jaoks vajalikud andmed võiksid olla kättesaadavad ühest portaalist;
- Strateegilise analüüsi keskuse loomine, mille töö tulemused jagatakse turuosalistega (nii riikliku kui ka rahvusvahelise info põhjal analüüside teostamine)[40];

[40] Tulemuste jagamine turuosalistega toimub tasemel, mis välistab info leket juhtude kohta, mis on või plaanitakse võtta süüteomenetlusse.

- Võimaldada kohustatud isikutele riiklikest registritest hoolsusmeetmete täitmiseks vajalikku infot tasuta;
- Leevendada õigusraamistiku kehtestades järgmise erandi: RahaPTS mõttes kohustatud subjektide hulgast ja sealhulgas ka finantseerimisasutuse mõiste alt jäävad välja elektroonilise side teenuse kasutaja maksetehingud, mida elektroonilise side ettevõtja täidab (lisaks elektroonilise side teenuste osutamisele) juhul, kui vastavate maksete maht ühe kasutaja kohta ei ületa 1000 eurot kuus;[41]
- Kliendi isiku tuvastamise ja kontrollimise nõuete võimalik lõdvendamine, viies selle võrdväärseks rahvusvaheliselt rakendatavate nõuetega:
  Isiku isikusamasuse tuvastamine ja kontrollimine rahapesu ja terrorismi rahastamise vastu võitlemisel tagab selle, et kohustatud isikud oleksid teadlikud, kes on see klient, kes teenust tarbib või ametitoimingut teostab. Samas on tegemist majanduslikus mõttes tootega/meetmega, mille tootmine allub kahaneva piirkasulikkuse seadusele, mille järgi esimene ühik toodetavat kaupa või teenust toob kõige suurema kasulikkuse, iga järgmise toodetava tooteühiku kasulikkus väheneb jõudes punktini, kus toodetava ühiku tarbimisest saadud kasulikkus on väiksem kui tooteühiku kulu. Teiste sõnadega, karmistuvate kliendi isiku tuvastamise ja kontrollimise nõuete täitmisesse panustatud ressursid ei too peale teatud punktini jõudmist enam kasulikkust rahapesu ja terrorismi rahastamise vastu võitlemise seisukohalt, aga on majanduslikud kulukad ning takistavad konkurentsi.
  Rahapesu tõkestamise direktiiv ja Financial Action Task Force'i (FATF) juhendid annavad liikmesriikidele võimaluse ise määrata nii füüsilise kui ka juriidilise isiku esindaja isiku isikusamasuse tuvastamise usaldusväärse ja sõltumatu allika sisu.
  Käesoleva ohuhinnangu käigus ei ole tuvastatud üldist ohtu või riski, mis on seotud kliendi isiku tuvastamise ja kontrollimise nõuete mittetäitmisega. Samuti ei leitud nii sektori rühmatööde kui ka läbiviidud küsitluse käigus isikusamasuse tuvastamisega seotud haavatavusi. Sealjuures puuduvad reaalsed kaasused, kus kliendi isikusamasuse väär tuvastamine on tähendanud, et klient peseb raha. Vastupidiselt, liiga karmid isikusamasuse tuvastamise reeglid takistavad konkurentsi ja teenuse osutamist ning surub seeläbi tegelikud kurjategijad kasutama mittereguleeritud teenuseid, misläbi kahaneb võimalus rahapesu ja terrorismi rahastamist tuvastada. Järelevalveasutusele on teada reaalsed kaasused, kus kohustatud isikud loobuvad Eestis teenuste osutamisest, sest isikusamasuse tuvastamise nõuded takistavad teenuse osutamist. See on tõsiseks ohuks Eesti konkurentsivõimele, kuid veelgi enam võimaldab teenuste kasutamist mittereguleeritud ettevõtetelt ehk surub teenuse osutamine „põranda alla". Lähtuvalt eeltoodust jõuti riikliku ohuhinnangu käigus järeldusele, et isikusamasuse tuvastamise nõuded tuleks terviklikult üle vaadata, vältimaks mittevajalikku keerukust, kuid juhtides samal ajal kohaselt riske lahendusega, mis reaalselt võib olla võimeline riske tuvastama ja juhtima. Kokkuvõtvalt, isikusamasuse tuvastamise käigus kogutud andmete kontrollimise lahendused tuleb üle vaadata ning viia tegeliku riski ja rahvusvahelise praktikaga kooskõlla, ehk usaldusväärse ja sõltumatu allika valik peaks jääma enam kohustatud isiku riskipõhise otsuse teha.
- Järelevalve tõhustamiseks kehtestada haldustrahvid ning viia trahvimäärad kooskõlla Euroopa Liidu rahapesu tõkestamise direktiiviga. Seeläbi saaks Finantsinspektsioon järelevalveasutusena kohaldada proportsionaalseid ja mõjusaid sanktsioone.

### 5.4.1.7.2. Leevendavad meetmed kohustatud isikute tasandil

Riskihinnangu tulemustest lähtudes tehakse järgmised ettepanekud olukorra parandamiseks kohustatud isikute tasandil:

- Tõsta teadlikkust läbi koolituste ja arutelude rahapesu tüpoloogiate ja stsenaariumide teemal koos Rahapesu Andmebürooga;
- Tõsta sektori teadlikkust järelevalveasutuste koolituste ja ümarlaudadega;

[41] Teostatud vastav analüüs, mille kohaselt sideteenuse osutajate rahapesu ja terrorismi rahastamise ohud on nullilähedased ja haavatavus puudub. Riskid on hinnatud ja saab järeldada, et sideteenuse osutajate poolt pakutavad teenused ei ole võrreldavad teiste finantsasutuste poolt pakutavate teenustega.

- Parendada koostööd erialaliidu ja makseteenuse pakkujate vahel;
- Parendada koostööd erialaliidu ja tegevusloata väikefondi valitsejate vahel. Esindusorganisatsioonid võiksid koondada kogu sektori, et koondada sektoris osalejad ühtsesse infovälja ja seeläbi sektoripõhiste ümarlaudade ja arutelude kaudu maandata üksikute sektoris osalejatega seotud riske ja suurendada sektori teadlikkust rahapesuga seotud riskidest.

### 5.4.2. Terrorismi rahastamise tõkestamise haavatavused

#### 5.4.2.1. Kokkupuude ohuga

- Finantsteenuste pakkujate ebapiisav teadlikkus ja sellega kaasnev terrorismi rahastamise suhtes rakendatavate hoolsusmeetmete ebapiisavus. NRA käigus turuosaliste seas läbiviidud küsitluse tulemustest järeldub, et terrorismi rahastamise tüpoloogiate keerukuse tõttu esineb turuosalistel raskusi terrorismi rahastamise stsenaariumite loomisel.
- Maksevahendajatega ning virtuaalvääringutega seotud oht. Finantssektoris võib kõikide turuosaliste puhul suurimaks kokkupuutemomendiks ohuga pidada teenuste osutamist makseteenuste ning virtuaalvääringu teenuste vahendusel. Rahapesu Andmebüroo poolt läbiviidud „Virtuaalvääringu teenuse pakkujate uuringust“ selgub, et 2020. aasta 1. augusti seisuga kehtis erinevaid virtuaalvääringuga teenusepakkuja tegevuslube kokku 611 (295 VV raha vastu vahetamise teenuse, 261 rahakotiteenuse ja 55 VV teenuseluba)[42]. Samuti küsitluse tulemused näitavad, et Eesti turul tegutsevate virtuaalvääringute teenuste pakkujate vahendatud teenuste kogukäive on kiiresti kasvanud. Kui 2018. aastal oli see suurusjärgus 590 miljonit eurot, siis 2019. a esimesel poolaastal juba kaks korda kõrgem – 1,2 miljardit eurot. Ka terrorismi rahastamise puhul on peamine oht seotud peamiselt ülepiiriliste makseteenuse pakkujatega - riikliku ohuhinnangu käigus neile saadetud küsimusele alates 2017. aastast Eesti residentidele osutatud teenuse mahu kohta on saadud vastused, mille kohaselt võrdub vastav näitaja 250 mln euroga.

#### 5.4.2.2. Riskiteadlikkus

**Juhtkonna pühendumine ja juhtroll**

Küsitluse tulemused teadlikkuse osas:

Riikliku ohuhinnangu raames läbiviidud küsitluse tulemused näitavad seda, et sektori teadlikkus terrorismi rahastamise tõkestamisest on keskmisest kõrgemal tasemel[43]. Selle põhjuseks võib lugeda RABi juhendi olemasolu ning RABi ja KAPO koolituste läbiviimist. Samas praktiliste kaasuste puudumise tõttu jääb teadlikkuse tase teoreetiliseks.

Sektor täidab oma teatamiskohustust tagasihoidlikult – 2019. aastal on krediidiasutuste poolt RABile esitatud kaks terrorismi rahastamise kahtluse teadet (kokku 2019. aastal on RABile kõikide sektorite poolt esitatud 4 terrorismi rahastamise kahtluse teadet).

Kokkuvõtvalt võib öelda, et finantssektori teadlikkus terrorismi rahastamisest on väga heal tasemel, kusjuures juhtkond panustab teadlikkuse tõstmisesse. Teatamiskohustuse tagasihoidliku täitmise taga on pigem teatamiskohustuse aluse puudumine.

[42] Majandustegevuse registri andmete alusel seisuga 31.12.2020 kehtis erinevaid virtuaalvääringuga teenusepakkujate tegevuslubasid kokku 478 (39 VV raha vastu vahetamise teenuse, 34 rahakotiteenuse ja 405 VV teenuseluba).

[43] Krediidiasutuste küsitluste tulemuste põhjal

### 5.4.2.3. Terrorismi rahastamise avastamise ja massihävitusrelvade leviku rahastamise tõkestamise kvaliteet

**Järelevalve kvaliteet**

Regulatsioonide tase on finantssektoris väga kõrge. Sektoris osalejatele kohalduvad eriseadused sätestavad tegevusloa nõude suuremale osale finantsteenuste osutajatest, mis aitab tagada finantssektoris tegutsevate ettevõtete ja kogu finantssektori usaldusväärsuse ja järelevalve kehtestatud nõuete täitmise üle. Kõik finantssektoris osalejad on kohustatud isikud RahaPTS kohaselt, mis seab omakorda sektorile spetsiifilised kohustused terrorismi rahastamise tõkestamise aspektist. Seega on hinnang regulatsioonidele kõrge.

Reguleeriva asutuse rolli täidab Finantsinspektsioon (v.a tegelusloata väikefondi valitsejad ja finantseerimisasutused). FI õigused ja pädevus järelevalve teostamisel on ulatuslikud ja kooskõlas sektori regulatsioonide tõhususe tagamise vajadusega. Järelevalve kvaliteet antud sektoris on kõrge.

**Vastavuskontrollisüsteemide ja aruandluse tõhusus**

Sektoris kehtivad aruandluse nõuded kehtestatakse eriseadustes, mille kohaselt esitavad turuosalised nõutud aruanded nõutud sagedusega Eesti Pangale ja Finantsinspektsioonile. Finantsinspektsioonis saadud andmete alusel teostatakse teenusepõhiselt terrorismi rahastamise riskide analüüsi.

Turuosaliste vastavuskontrollisüsteemide tõhusust võib hinnata küsitlustest saadud tulemuste põhjal järgmiselt:

- Vastavuskontrollisüsteemide piisavust hinnatakse regulaarsel alusel[44];
- Suurima mõjuga turuosaliste seiresüsteemid on automatiseeritud, reeglina on ka teiste turuosaliste seiresüsteemid automatiseeritud vastavalt teenuste mahtudele[45];
- Tehingute seire stsenaariumide valik ja kalibreerimine on reeglina kooskõlas üksuse profiili ning sellest tulenevate riskidega[46], samas on teatud turuosalistel selles osas arenguruumi, et muuta nende võimekus veelgi kõrgematasemelisemaks, võimaldades reaalajas tehingute jälgimist ja peatamist ning olles senisest enam riskitundlikumad[47];
- Suurima mõjuga turuosaliste tehingute seiresüsteemid võimaldavad tuvastada teatuid keerukaid või ebatavalisi tehinguid[48], kuid peaksid olema senisest enam riskitundlikud; Terrorismi rahastamise spetsiifiliste stsenaariumide väljatöötamine on problemaatiline nende keerukuse tõttu[49];
- Enamuse turuosaliste puhul on kasutusel kliendi riskitaseme riskipõhist arvutamist võimaldav süsteem[50];
- Enamus turuosalisi investeerib riskijuhtimise tehnilistesse lahendustesse ja peamiselt panustatakse programmidesse ja tarkvarasse[51].

**Lühikokkuvõte**

Üldiselt on sektori vastavuskontrollisüsteemide ja aruandluse tõhusus kõrge, kuigi esineb probleeme terrorismi rahastamise spetsiifiliste stsenaariumide väljatöötamisega nende keerukuse tõttu.

**Kliendi suhtes rakendatavate hoolsusmeetmete raamistiku kvaliteet**

Kliendikontrolli raamistiku kvaliteedi osas läbiviidud küsitluse käigus leitud haavatavused:

- Riigi registrites sisalduv tegelikke kasusaajaid käsitlev teave ei ole alati usaldusväärne[52];

[44] Krediidiasutuste, makseasutuste, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[45] Krediidiasutuste, makseasutuste, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[46] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[47] Fondivalitsejate küsitluste tulemuste põhjal

[48] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[49] Fondivalitsejate, makseasutuste küsitluste tulemuste põhjal

[50] Krediidiasutuste, fondivalitsejate, makseasutuste, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[51] Krediidiasutuste, makseasutuste, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[52] Krediidiasutuste, fondivalitsejate, makseasutuste, elukindlustusseltside, krediidiandjate küsitluste tulemuste põhjal

- Raskendatud on juurdepääs teabele, mis on vajalik tegelike kasusaajate kindlakstegemiseks[53];
- Raskendatud on juurdepääs teabele, mis on vajalik teiste suure riskiga klientide (nt saatkonnad, virtuaalvääringute pakkujad, rahateenuseid pakkuvad ettevõtjad, mittetulundusühendused jms) kindlakstegemiseks ja kontrollimiseks[54].

**Lühikokkuvõte**

Hoolsusmeetmete raamistiku kvaliteet on reeglina kõrge. Kliendikontrolli seisukohalt on suurematekss probleemideks riikliku taustaga isikute registri puudumine, samuti tegeliku kasusaaja tuvastamise protsessi keerukus ning usaldusväärse allika puudumine.

**Sektoripõhiste rahvusvaheliste sanktsioonide kindlakstegemise kvaliteet**

Rahvusvaheliste sanktsioonide kindlakstegemise kvaliteedi osas läbiviidud küsitluse käigus leitud haavatavused:

- Sanktsioonidest kõrvalehoidmise tuvastamise mehhanismid ei ole alati tõhusad (näiteks nimekirjade andmekvaliteedi probleemi tõttu)[55],[56];
- Kohaldatavate sektoripõhiste sanktsioonide teadmine ja rakendamine ei ole piisavad kõikide turuosaliste puhul[57];
- Varade külmutamise mehhanismid ei ole alati tõhusad[58].

**Lühikokkuvõte**

Rahvusvaheliste sanktsioonide kindlakstegemise kvaliteet on reeglina kõrge. Kõige suuremaks probleemiks on sanktsioonide nimekirjades sisalduva info andmekvaliteedi ja identsuse probleem.

### 5.4.2.4. Sektoriomaste riskide hindamine sektoripõhiste kontrollide kvaliteediga

Sektoriomaste riskide analüüsimisel ja hindamisel on tuvastatud järgmised haavatavad kohad:

- Terrorismi rahastamist hõlbustavate rahateenuseid osutavate ettevõtete tuvastamine on problemaatiline[59];
- Terrorismi rahastamise eesmärgil tarbimislaenude ja väikese väärtusega laenude kuritarvitamise tuvastamise keerukus[60];
- Rahapesu või terrorismi rahastamise eesmärgil saatkondade kontode kuritarvitamise tuvastamise keerukus[61];
- Rahapesu või terrorismi rahastamise eesmärgil mittetulundusühenduste ja heategevusorganisatsioonide kuritarvitamise tuvastamise keerukus[62];
- Virtuaalvääringutega seotud kahtlaste tehingute kindlakstegemise keerukus[63],[64].

[53] Krediidiasutuste, fondivalitsejate, makseasutuste, elukindlustusseltside, krediidiandjate küsitluste tulemuste põhjal

[54] Krediidiasutuste, makseasutuste, krediidiandjate, muude finantseerimisasutuste küsitluste tulemuste põhjal

[55] Fondivalitsejate, valuutavahetajate küsitluste tulemuste põhjal

[56] Töögrupi töö tulemus

[57] Fondivalitsejate, makseasutuste, krediidiandjate, muude finantseerimisasutuste küsitluste tulemuste põhjal

[58] Krediidiasutuste, fondivalitsejate, makseasutuste, investeerimisühingute, krediidiandjate, muude finantseerimisasutuste küsitluste tulemuste põhjal

[59] Töögrupi töö tulemus

[60] Töögrupi töö tulemus

[61] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[62] Krediidiasutuste, makseasutuste küsitluste tulemuste põhjal

[63] Fondivalitsejate, makseasutuste küsitluste tulemuste põhjal

[64] Töögrupi töö tulemus

**Lühikokkuvõte**
Sektoriomaste riskide hindamise kvaliteet on reeglina keskmisest kõrgem. Probleemiks on terrorismi rahastamise stsenaariumide vähesus, mis on tingitud terrorismi rahastamise mitmekesisusest ja keerukusest.

#### 5.4.2.5. Varasemate hindamiste käigus tuvastatud riskidele reageerimise kvaliteet

Finantssektoris olid terrorismi rahastamise hinnangud varasemalt terviklikuna üsna puudulikud.

Terrorismi rahastamise kuriteokoosseisu osas leiti, et see on mõnevõrra puudulik. Terrorismi rahastamise kvalifikatsiooni on muudetud 2019. a (RahaPTS § 5 ja KarS § 237.3 ja 237.6).

SNRA (2017/2019) leiti antud sektori osas, et Euroopa-üleselt on potentsiaalseks ohuks „väikelaenud terrorismi rahastamise võtmes“. Eestis on sellega seoses vajalik mainida, et Eestis ei ole tuvastatud selliseid kaasuseid. Oht ja haavatavus on madalad.

#### 5.4.2.6. Järeldus

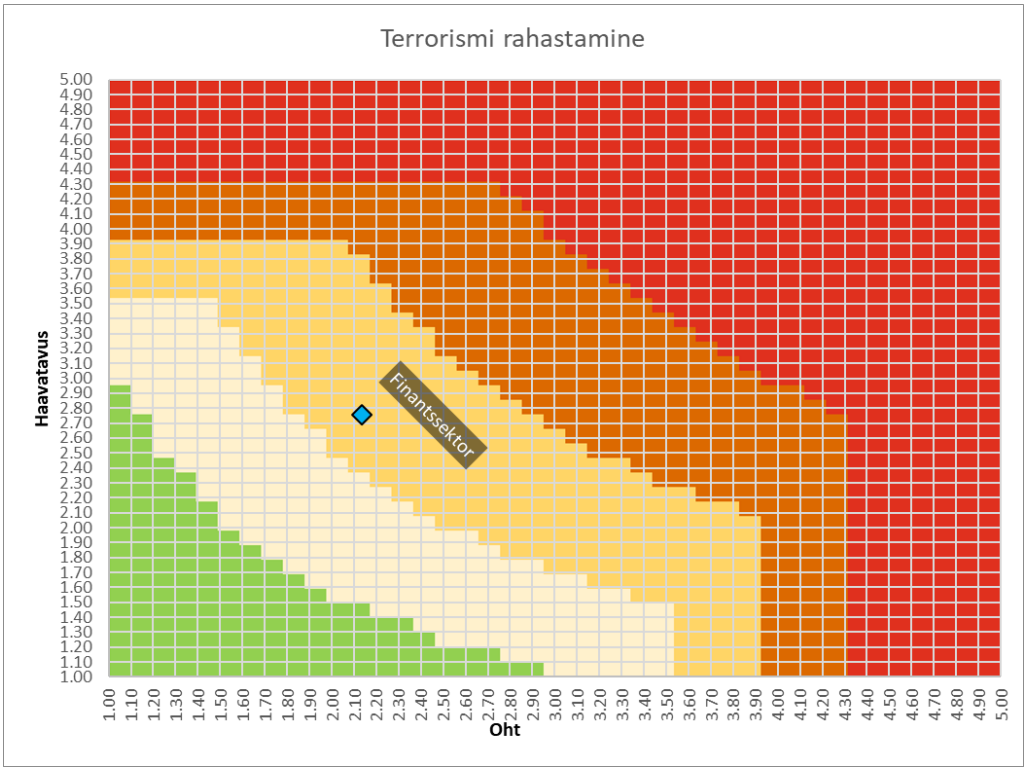
Skaalal 1-5 on finantssektori haavatavuse hinne terrorismi rahastamise aspektist 2,75 ehk **keskmiselt madal.**

**Tabel 26.** Terrorismi rahastamise haavatavuse tase finantssektoris

| Sektor | Terrorismi rahastamise haavatavuse tase sektori tasandil | |
|---|---|---|
| Finantssektor | 2,75 | **keskmine/madal** |

Kuna sektori TR haavatavuse tase on madal, pole eeltoodud põhjusel regulatsioonide või järelevalve tõhustamine antud sektori suhtes tõenäoliselt vajalik ning keskenduda tuleks saavutatud taseme hoidmisele.

**Joonis 5.** Finantssektori terrorismi rahastamise riskitaseme soojuskaart




**<u>Kokkuvõte</u>**

Sektori haavatavuse taseme paiknevus riiklikul pildil on teiste sektorite keskel **keskmisest madalama** hinnangu tasemel. Seega keskenduda tuleks terrorismi rahastamise suurema hulga stsenaariumide väljatöötamisele ning järelevalve taseme hoidmisele. Sektoris tuleb rakendada hoolsusmeetmeid tavakorras.

### 5.4.2.7. Riskimaandamisstrateegia

#### 5.4.2.7.1. Leevendavad meetmed riiklikul tasandil

Riskihinnangu tulemustest lähtudes tehakse järgmised ettepanekud olukorra parandamiseks riiklikul tasandil:

- Virtuaalvääringu teenusepakkujate kliendibaaside täisskoobiga seire teostamine perioodilisel alusel ja/või klientide andmebaasi loomine (klient + kontaktandmed), krediidi- ja makseasetuste teavitamine.

#### 5.4.2.7.2. Leevendavad meetmed kohustatud isikute tasandil

Riskihinnangu tulemustest lähtudes tehakse järgmised ettepanekud olukorra parandamiseks kohustatud isikute tasandil:

- Koolitused ja arutelud terrorismi rahastamise tüpoloogiate ja stsenaariumide teemal koos RABi ja KAPOga.