MAINSTON INTERNATIONAL OÜ

RISKIHINNANG 2022

Kinnitatud MAINSTON INTERNATIONAL OÜ juhatuse poolt 01.06.2022.a.

1. Riskihindamise alus ja uuendamisprotsess

1.1. Riskihindamise aluseks on rahapesu ja terrorismi rahastamise tõkestamise seadus, rahapesu andmebüroo suunised, ELi direktiivi 2015/849 artikli 17 ja artikli 18 lõike 4 alusel koostatud ühised suunised, Eesti 2020. aasta riiklik rahapesu ja terrorismi rahastamise riskihinnang ning rahvusvaheliste organisatsioonide suunised.

1.2. Riskihinnangu koostamisel kaardistab MAINSTON INTERNATIONAL OÜ oma tegevusega seotud rahapesu ja terrorismi rahastamisega seotud riskid, seejärel hindab kaardistatud riskide mõju MAINSTON INTERNATIONAL OÜ tegevusele ja analüüsib võimalikke vastumeetmeid, mida saab kasutada riskide maandamiseks.

1.3. MAINSTON INTERNATIONAL OÜ dokumenteerib riskihindamise ja riskivalmiduse tuvastamise ning ajakohastab neid dokumente vastavalt vajadusele, kuid vähemalt kord aastas ja vastavalt riikliku riskihindamise tulemusele.

1.4. Riskihindamise tulemusena tuvastab MAINSTON INTERNATIONAL OÜ:

1.4.1. väiksema ja suurema rahapesu ja terrorismi rahastamise riskiga valdkonnad;

1.4.2. riskivalmiduse, sealhulgas äritegevuse käigus pakutavate toodete ja teenuste mahu ja ulatuse;

1.4.3. riskijuhtimise mudeli tuvastatud riskide maandamiseks.

1.5. Riskivalmiduse kindlaksmääramisel võetakse arvesse riske, mida MAINSTON INTERNATIONAL OÜ on valmis võtma või mida ta soovib vältida seoses oma äritegevusega, ning kvalitatiivseid ja kvantitatiivseid kompensatsioonimehhanisme, näiteks kavandatud tulu, kapitali või muude likviidsete

vahendite abil rakendatavad meetmed või muud asjaolud, nagu maineriskid ja rahapesu ning terrorismi rahastamise või muu ebaeetilise tegevusega kaasnevad õiguslikud ja muud riskid.

2. Riskivalmidus

2.1. Selleks, et vältida riske, mida MAINSTON INTERNATIONAL OÜ ei ole valmis oma äritegevuses võtma, on tuvastatud riskitegurid ja omadused, mille esinemine riskiprofiiliga isikul välistab ärisuhte sõlmimise

2.1.1. isikutega, kelle suhtes ei ole võimalik rakendada hoolsusmeetmeid;

2.1.2. isikutega, kelle kohta on teada rahapesu ja/või terrorismi rahastamisega tegelemine või kelle suhtes tekib hoolsusmeetmete käigus vastav kahtlus;

2.1.3. anonüümsete ja/või fiktiivsete isikute ja variisikutega;

2.1.4. varipankade ja selliste krediidiasutuste või finantseerimisasutustega, mis teadlikult lubavad varipankadel kasutada oma kontosid (korrespondentsuhet ei ole loodud);

2.1.5. isikutega, kes on kantud ÜRO, OFACi ja ELi sanktsioonide nimekirja;

2.1.6. rahapesuvastase töökonna hinnangul suure riskiga riikidest (kus on ebapiisavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks) pärit füüsiliste ja juriidiliste isikutega;

2.1.7. segamisteenuse osutajatega;

2.1.8. isikutega, kelle esitajaaktsiad või muud esitaja väärtpaberid moodustavad üle 10 protsendi kapitalist.

3. Ettevõtte ja selle teenuste taust

3.1. Ettevõte on registreeritud Eestis registrinumbriga 14763925, registrijärgne aadress on Viru väljak 2, Kesklinna linnaosa, Tallinn, Harju maakond 10111.

3.2. Ettevõte on virtuaalvaluutateenuse osutaja, kellel on rahapesu tõkestamise seaduse paragrahvi 70 kohaselt väljastatud tegevusluba nr FVT000240.

3.3. Ettevõtte äritegevus seisneb virtuaalvaluuta vahetamise ja rahakoti teenuse pakkumises, mille raames kliendid saavad ettevõtte veebisaidil https://mainston.com/ virtuaalvaluutasid hoiustada ja vahetada.

3.4. Ettevõte kasutab klientide tuvastamise ja kontrollimise teenuste osutamiseks kolmandaid teenusepakkujaid, kes on kas spetsialiseerunud teenusepakkujad või kes on ise rahapesu tõkestamise seaduse alusel litsentseeritud. Rahapesu / terrorismi rahastamisega seotud riskide juhtimine, sealhulgas ettevõtte riskijuhtimise mudeli, riskivalmiduse, menetluste, asjakohase korralduse ja täideviimise kavandamine toimub ettevõtte enda poolt.

3.5. Klientide tuvastamiseks ja kontrollimiseks ning riikliku taustaga isikute ja sanktsioonide kontrollimiseks kasutab ettevõte Onfido SAS, Shufti Pro Limited teenuseid.

3.6. Tehingute seireks kasutab ettevõte Tangany GmbH teenuseid.

3.7. Plokiahelate seireks kasutab ettevõte lahendust Qlue.

4. Ettevõtte ärimudeli üldine riskianalüüs

4.1. Ettevõtte ärimudeli ja tema tegevuse laadi tõttu esineb ettevõttel märkimisväärne hulk rahapesu / terrorismi rahastamise riske.

4.2. Vastavalt ettevõtte ärimudelile võimaldab ettevõte klientidel hoiustada, vahetada ja osta virtuaalvaluutasid ettevõtte rakenduses. Kliendid saavad oma virtuaalvaluutasid salvestada ka ettevõtte pakutavasse digitaalsesse rahakotti ning teha virtuaalvaluutas sisse- ja väljamakseid selle digitaalse rahakoti ning teiste teenusepakkujate digitaalsete rahakottide vahel.

4.3. Kui ettevõte otsustab vastu võtta usaldusraha, võib ettevõte võtta kliendilt usaldusraha makseid vastu ainult volitatud makseteenuse pakkujate (maksekontode ja krediitkaartide pakkujate) kaudu sama makseteenuse pakkuja vahendusel, või ettevõte võtab usaldusraha sissemakseid vastu ainult rahakoti omanike kontodelt tehtavatest SEPA-ülekannetest. Kui aga usaldusraha on vahetatud virtuaalvaluutaks, ei kohaldata teise digitaalsesse rahakotti ülekandmise suhtes sarnaseid eeskirju. Seega kaasnevad ettevõtte ärimudeliga rahapesu / terrorismi rahastamise riskid, mis on tavapärased virtuaalvaluutateenuse pakkujate puhul, kes võimaldavad klientidel maksta ja teha tehinguid virtuaalvaluutaga.

4.4. Ettevõtte roll piirdub saadud rahaliste vahendite kontrollimisega ja usaldusvaluuta vahetamisega virtuaalvaluutaks vastavalt kliendilt saadud konkreetsetele juhistele.

4.5. Rahapesu ja terrorismi rahastamise riskide maandamiseks nõuab ettevõte iga kliendi tuvastamist ja isikusamasuse kontrollimist vastavalt rahapesu tõkestamise seadusele, kasutades selleks väliste teenusepakkujate pakutavaid tehnoloogilisi lahendusi. See võimaldab ettevõttel suurendada kindlustunnet, et igasugune pettus avastatakse.

4.6. Riskide klassifikatsioon

4.6.1. Riskihinnangu koostamisel ja kliendi riskiprofiili kindlaksmääramisel võetakse arvesse vähemalt järgmisi riskikategooriaid:

1) kliendiga seotud risk;
2) riikide, geograafiliste piirkondade või jurisdiktsioonidega seotud risk;
3) toodete, teenuste või tehingutega seotud risk;
4) risk, mis on seotud MAINSTON INTERNATIONAL OÜ ja kliendi vaheliste suhtlus- või vahenduskanalitega või toodete, teenuste või tehingute edastuskanalitega.

5. Heakskiitmismaatriks

Kliendi riskiklass	AML/KYC spetsialist	Kontaktisik	Juhatus
Suur		✓	
Keskmine	✓		
Väike	✓		
Riikliku taustaga isikud			✓

6. Kliendiga seotud risk

6.1. Kui riskitegurid tulenevad isikust, kes on tehingu osapool või klient:

6.1.1. isiku elukoht;

6.1.2. kas isiku vara päritolu või tehingu tegemiseks kasutatud raha allikat ja päritolu on lihtne kindlaks teha;

6.1.3. kas isiku kohta on meedias negatiivset teavet;

6.1.4. kliendi juriidiline vorm, juhtimisstruktuur, sealhulgas kas klient on usaldusfond, tsiviilõiguslik ühing või muu selline lepinguline juriidiline isik;

6.1.5. kas isiku tegelike tulusaajate kindlakstegemine on raskendatud keeruliste ja läbipaistmatute omandisuhete tõttu;

6.1.6. ettevõtluse kestus ja kogemus;

6.1.7. kas klient on riikliku taustaga isik;

6.1.8. kas kliendi suhtes kohaldatakse sanktsioone;

6.1.9. kas klient tegeleb sularahamahuka äritegevusega.

6.2. Kliendiga seotud riski suurendavad asjaolud on järgmised:

6.2.1. ärisuhe toimib ebatavalistel asjaoludel või esinevad ebatavalised tehingumustrid, millel ei ole selget majanduslikku või õiguspärast eesmärki;

6.2.2. klient on suurema riskiga geograafilise piirkonna resident;

6.2.3. kliendil või temaga seotud äriühingul on variaktsionärid või esitajaaktsiad;

6.2.4. ebatavaline või keeruline omandistruktuur

6.3. Kliendiga seotud riskide maandamine Mainston OÜ-s:

6.3.1. Mainston OÜ on rakendanud Eesti rahapesu tõkestamise seaduse nõudeid oma sisemistes rahapesu ja terrorismi rahastamise tõkestamise menetlustes;

6.3.2. Mainston OÜ kasutab tuntud IT-süsteeme ja punktides 3.5–3.7 nimetatud KYC-teenuse pakkujaid, et tagada iga kliendi tuvastamine ja taustakontroll;

6.3.3. Mainston OÜ teostab teenusepakkujate pistelist kontrolli, et tagada kõikide nimekirjade ajakohasus;

6.3.4. kliendiks ei võeta ebatavalise või põhjendamatult keerulise omandistruktuuriga isikuid, kui see muudab kliendi tegelike tulusaajate tuvastamise võimatuks;

6.3.5. kliendiks ei võeta riikliku taustaga isikuid.

6.4. Kliendiga seotud riske maandavad üldised asjaolud:

6.4.1. klient on reguleeritud turul noteeritud äriühing, kelle suhtes kohaldatakse avalikustamiskohustust, millega on kehtestatud nõuded, et tagada tegeliku tulusaaja puhul piisav läbipaistvus;

6.4.2. klient on Euroopa Liidu asutus;

6.4.3. klient on isik, kes on EMP resident.

7. Geograafiline risk

7.1. Geograafiline risk või risk, mis tuleneb õiguskeskkonna erinevustest erinevates riikides, millega klient või kliendi esindaja või tegelik tulusaaja on seotud, sealhulgas:

7.1.1. kas riik rakendab rahapesu ja terrorismi rahastamise tõkestamise rahvusvahelistele standarditele vastavaid õigusnorme;

7.1.2. kas riigis on kõrge kuritegevuse tase, sealhulgas narkokuritegevuse tase;

7.1.3. kas riik teeb koostööd kuritegeliku organisatsiooniga; kas kuritegelikud organisatsioonid kasutavad konkreetset riiki oma tegevuse teostamiseks;

7.1.4. kas riik osaleb massihävitusrelvade leviku rahastamises;

7.1.5. kas riigis on kõrge korruptsioonitase;

7.1.6. kas riigi suhtes on kohaldatud või kohaldatakse rahvusvahelisi sanktsioone;

7.1.7. kas riigi suhtes on kohaldatud muid meetmeid või on avaldatud rahvusvaheliste organisatsioonide seisukohti riigi suhtes.

7.2. Geograafilist riski suurendavad asjaolud on eelkõige olukorrad, kus tehingus osalev isik või tehing ise on seotud riigi või jurisdiktsiooniga,

7.2.1. kus usaldusväärsete allikate, näiteks vastastikuste eksperdihinnangute, üksikasjalike hindamisaruannete või avaldatud järelaruannete kohaselt ei ole tõhusaid rahapesu ja terrorismi rahastamise tõkestamise süsteeme;

7.2.2. kus usaldusväärsete allikate kohaselt on korruptsiooni või muu kuritegevuse tase märkimisväärne;

7.2.3. mille suhtes kohaldatakse sanktsioone, embargosid või sarnaseid meetmeid, näiteks Euroopa Liidu või ÜRO poolt kehtestatud sanktsioone, embargosid või sarnaseid meetmeid;

7.2.4. mis rahastab või toetab terrorismi või mille territooriumil tegutsevad Euroopa Liidu või ÜRO nimekirja kantud organisatsioonid.

7.3. Geograafilist riski maandavad asjaolud on eelkõige olukorrad, kus osapoole asukoht või tehingu toimumiskoht on mõnes järgmistest riikidest:

7.3.1. Euroopa Majanduspiirkonna lepinguriik;

7.3.2. kolmas riik, kus on tõhusad rahapesu ja terrorismi rahastamise tõkestamise süsteemid;

7.3.3. kolmas riik, kus usaldusväärsete allikate kohaselt on korruptsiooni ja muu kuritegevuse tase madal;

7.3.4. kolmas riik, kus usaldusväärsete allikate, näiteks vastastikuste eksperdihinnangute, aruannete või järelaruannete kohaselt on rahapesu ja terrorismi rahastamise vastased nõuded kehtestatud ja kooskõlas rahapesuvastase võitluse nõukogu muudetud soovitustega ning toimivad tõhusalt.

7.4.

Riik	**Otsus**	**Riskiparameeter**	**Tulemus**
Euroopa Liit, Šveits	Väike		Võib kohaldada rahapesu tõkestamise käsiraamatu kohaseid lihtsustatud hooldusmeetmeid.
Ülejäänud maailm	Keskmine		Kohaldatakse rahapesu tõkestamise käsiraamatu kohaseid standardseid hooldusmeetmeid.
Venemaa (rahvusvaheliste sanktsioonide all olevad riigid)	Suur		Kogu taotlusele määratakse suur risk. Kohaldatakse rahapesu tõkestamise käsiraamatu kohaseid

			tugevdatud hoolsusmeetmeid.
Afganistan Bosnia ja Hertsegoviina Cambodgia Korea Demokraatlik Rahvavabariik Etioopia Ghana Guyana Island Iraan Iraak Laos Mongoolia Põhja-Makedoonia Pakistan Panama Sri Lanka Süüria Trinidad ja Tobago Tuneesia Uganda Ameerika Ühendriigid Vanuatu Jeemen	Keelatud		Taotlus lükatakse tagasi.

8. Toodete, teenuste või tehingutega seotud risk

8.1. Toote või teenusega seotud risk on see, kui riskitegurid tulenevad kliendi majandustegevusest ja konkreetse toote või teenuse kokkupuutest võimalike rahapesuriskidega:

8.1.1. klient ostab virtuaalvaluutat sularaha eest;

8.1.2. kliendil on rohkem kui kolm rahakotikontot;

8.1.3. kliendi poolt vahetatud virtuaalvaluuta on üle kantud pimeveebi kaudu või kahtlustatakse segamisteenuse kasutamist;

8.1.4. virtuaalvaluuta või kliendi raha päritolu ei ole hõlpsasti tuvastatav.

8.2. Toote või teenusega seotud riski suurendavad asjaolud on eelkõige järgmised olukorrad:

8.2.1. anonüümsust soodustada võiva tehingu tegemine või korraldamine;

8.2.2. maksete saamine tundmatutelt või mitteseotud kolmandatelt isikutelt;

8.2.3. ärisuhe või tehing, mis on loodud või algatatud viisil, mille puhul klient, tema esindaja või tehingu osapool ei viibi samas kohas ja mille isik ei ole infotehnoloogiliste vahenditega kontrollitud;

8.2.4. uued tooted või uued äritavad, sealhulgas uue ülekandemehhanismi või uue või areneva tehnoloogia kasutamine nii uute kui ka olemasolevate toodete puhul.

8.3. Toote või teenusega seotud riski maandavad asjaolud on eelkõige järgmised olukorrad:

8.3.1. finantstoodete või -teenustega pakutakse asjakohaselt määratletud ja piiratud teenuseid konkreetsetele kliendirühmadele, et suurendada finantsteenuste kättesaadavust;

8.3.2. tooted, mille puhul rahapesu ja terrorismi rahastamise riski juhitakse muude tegurite, näiteks rahaliste piirmäärade abil.

8.4. Tokenite vahetamisega seotud risk. Ainult piiratud vahetus (STON-USDT).

8.4.1. Vahetustehingutega seotud klassikalised riskid: valeidentiteedi kasutamine, kauplemine varadega, mille päritolu ja ajalugu ei ole teada.

8.4.2. Vahetusega seotud riskide vähendamiseks on Mainston OÜ maksimaalselt piiranud vahetusteenuseid, välistades vahetuse usaldus- ja sularahaga. Iga kliendi isik tuvastatakse, sh aadressi tõendamisega. Suurema summaga (mis ületavad Mainstoni poolt kehtestatud piirmäärasid) toimingute puhul, samuti ettevõtte identiteedi kasutamise puhul, harjutatakse 3. ja 4. tasandi registreerimismeetmete rakendamist.

8.5. Rahakotiteenusega seotud risk.

8.5.1. Klassikalised virtuaalvaluutateenuse riskid: valed isikuandmed ja aadress, vale IP.

8.5.2. Rahakotiteenusega seotud riskide maandamiseks rakendab Mainston OÜ 1., 2., 3. ja 4. tasandi kliendikontrolli (KYC) põhimõtteid, mis vähendavad riskid miinimumini, kuna iga klient on dokumentaalselt tuvastatud ja tema aadress tõendatud, et välistada riigi, territooriumi, riikliku taustaga isikute ja sanktsioonidega seotud riskid.

9. Sidekanaliga seotud risk

9.1. Sidekanaliga seotud riski puhul tulenevad riskitegurid erinevate sidekanalite kasutamisest:

9.1.1. kas veebiplatvormi logitakse sisse varem kasutatud või uuelt IP-aadressilt;

9.1.2. kas tegemist on uue kliendiga või kliendiga, kes on teenust juba kasutanud;

9.1.3. kas klienti on võimalik tuvastada ja kontrollida reaalajas toimuvate küsitluste abil, kasutades sünkroniseeritud heli- ja videovoogu;

9.1.4. kas esitatud andmeid, isikutunnistusi ja muid dokumente saab kontrollida usaldusväärse ja sõltumatu allika abil;

9.1.5. kas IP-aadress, millelt klient alustab tehinguid, ei vasta kliendi / kliendi esindaja elukohariigile;

9.1.6. kas klient / kliendi esindaja kasutab telefoninumbrit, mis ei vasta tema elukohariigile.

9.2. Sidekanaliga seotud riski maandamine Mainston OÜ-s:

9.2.1. Mainston OÜ on rakendanud Eesti rahapesu tõkestamise seaduse nõudeid oma sisemistes rahapesu ja terrorismi rahastamise tõkestamise menetlustes;

9.2.2. Mainston OÜ kasutab identifitseerimiseks, kontrollimiseks ja tehingute seireks punktides 3.5–3.7 nimetatud tuntud IT-süsteeme ja teenusepakkujaid;

9.2.3. Mainston OÜ teostab teenusepakkujate pistelist kontrolli, et tagada kõikide nimekirjade ajakohasus.

10. Meetmed virtuaalvaluuta vahetamise teenustega seotud riskide maandamiseks

10.1. Kliendilt küsitakse mobiiltelefoni numbrit ja meiliaadressi, mille kehtivust kontrollitakse kord kuue kuu jooksul (kontrollkoodide saatmisega);.

10.2. Teenuse osutamise riske maandatakse automaatse kontrolli ja sisekontrolli abil, et pidevalt hinnata süsteemi võimet tuvastada ebatavalisi või kahtlasi tehinguid, muudatusi sanktsioonide nimekirjades, klientide poolt esitatud tehingute mahtu ja kvaliteeti jne.

10.3. Kliendi rahakoti aadressi tuvastamiseks ja virtuaalvaluuta tehingute seireks kasutatakse heakskiidetud teenusepakkujat.

10.4. Seireprogramm on üles ehitatud nii, et see tuvastab vastaspoole kattumise riikliku taustaga isikute ja sanktsioonide nimekirjas olevate isikute/ettevõtetega.

10.5. Seireprogramm on üles ehitatud nii, et see tuvastab ühe kliendi puhul mitme rahakoti omamise ja nendega seotud tehingute tegemise.

10.6. Seireprogramm on üles ehitatud nii, et see võimaldab tuvastada kahtlasi ja ebatavalisi tehinguid.

10.7. Vajaduse korral saab kontrollida tehingus kasutatud vahendite allikat ja päritolu.

10.8. Kõik kliendid, kes kasutavad veebiplatvormi, tuvastatakse isikut tõendava dokumendi ja nn profiilifoto (selfi) võrdlemise teel.

11. Kliendi riskitase

11.1. Riskitaseme määramine kliendile tuleb dokumenteerida ja vajaduse korral tuleb riskitaset ärisuhte jooksul ajakohastada. Riskifaktorite hindamine peab tagama, et

- riskihindamist ei mõjuta põhjendamatult ainult üks riskitegur;
- riskihindamist ei mõjuta majanduslikud või kasumiga seotud kaalutlused.

11.1.1. MAINSTON INTERNATIONAL OÜ poolt kasutatav CRM-programm määrab kliendi tuvastamise käigus kogutud andmete põhjal igale kliendile riskitaseme vastavalt riskikategooriate ja riskitegurite hindamisel saadud punktisummale.

11.1.2. Riskitasemed on väike, keskmine ja suur. Põhiparameetrid, mida CRM-programm kasutab riskitasemete määramiseks, on järgmised:

11.1.2.1. kliendi elukoht või tegevuskoht ja tegeliku tulusaaja elukoht (geograafiline risk);

11.1.2.2. riskiprofiili mõjutavad eriomadused (riikliku taustaga isiku staatus, negatiivne meediakajastus jne);

11.1.2.3. majandustegevus (hinnanguline igakuine käive, tegevus ja kogemus antud tegevusalal, tegutsemine tegevusalal, kuskaubeldakse uute ja/või arenevate tehnoloogiatega ja/või edastatakse teenuseid mittetraditsiooniliste müügikanalite kaudu);

11.1.2.4. vastaspooled ja nendega seotud riskid (sealhulgas tegutsemine tegevusalal, kus kaubeldakse uute ja/või arenevate tehnoloogiatega ja/või edastatakse teenuseid mittetraditsiooniliste müügikanalite kaudu).

11.2 Väikese riski tunnused

11.2.1. Üheski suurema riski kategoorias ei ole mõjukat riskitegurit ja esineb vähemalt üks riski maandav tegur, seega võib väita, et klienti ja tema tegevust iseloomustavad tunnused ei erine tavapärase ja läbipaistva tegevusega isiku tunnustest, mistõttu ei ole põhjust kahtlustada, et kliendi tegevus võib suurendada rahapesu ja terrorismi rahastamise tõenäosust.

11.2.2. Klient ja tema tehingupartnerid asuvad ELi või EMP riikides.

11.2.3. Teave kliendi ja tema tegeliku tulusaaja kohta on avalikult kättesaadav, isiku tegevus ja tehingud on kooskõlas tema igapäevase äritegevusega ega erine teiste sarnaste klientide maksekäitumisest või tehingu sooritamisele on kehtestatud kvantitatiivsed või muud absoluutsed piirangud.

11.2.4. Klient maksab virtuaalvaluuta eest maksekonto kaudu, mis asub ELi või EMP riigis asutatud või teenuseid pakkuvas krediidiasutuses, e-raha asutuses või makseasutuses.

11.2.5. Virtuaalvaluuta rahakotti kasutatakse ainult MAINSTON INTERNATIONAL OÜ-lt ostetud virtuaalvaluutade hoidmiseks ning virtuaalvaluutade ülekandeid kolmandatele isikutele ja kolmandatelt isikutelt ei tehta.

11.2.6. Klient ja/või tema vastaspooled asuvad kolmandates riikides, kus on tõhusad rahapesu ja terrorismi rahastamise vastased süsteemid.

11.3. Keskmise riski tunnused

11.3.1. Klient maksab virtuaalvaluuta eest maksekonto kaudu, mis asub väljaspool Euroopa Majanduspiirkonna lepinguriiki asuvas krediidiasutuses, e-raha asutuses või makseasutuses.

11.3.2. Klient teeb virtuaalvaluuta ülekandeid virtuaalvaluuta rahakottidesse, mis on avatud finantsasutuses, mille suhtes ei kohaldata rahapesu tõkestamise seaduse nõuetega samaväärseid nõudeid.

11.4. Suure riski tunnused

11.4.1. Kliendiga seotud risk on üldiselt suur, kui riskikategooriate hindamisel tervikuna tekib kahtlus, et kliendi tegevus ei ole tavapärane või läbipaistev, st esineb vähemalt üks suurema riski kategooria, mis võib viia rahapesu ja terrorismi rahastamise suure või oluliselt suurenenud tõenäosuseni. Kliendiga

seotud risk on suur ka siis, kui seda tingib mõni riskiteguri näitaja (nt kahtlus, et tema suhtes kohaldatakse rahvusvahelisi sanktsioone). Suur risk ei tähenda siiski tingimata, et klient on seotud rahapesu või terrorismi rahastamisega.

11.4.2. Riski peetakse alati suureks, kui tegemist on kliendiga, kelle esindaja või tegelik tulusaaja asub suure riskiga kolmandas riigis või territooriumil, kus ei ole rakendatud piisavaid meetmeid rahapesu ja terrorismi rahastamise tõkestamiseks, või kui see riik või territoorium ei tee rahvusvahelist koostööd rahapesu või terrorismi rahastamise tõkestamisel või on madala maksumääraga territoorium.

11.4.3. Riski peetakse alati suureks, kui tehingu asjaolud viitavad rahapesule ja terrorismi rahastamisele või on tõenäoliselt seotud rahapesu ja terrorismi rahastamisega, sealhulgas keeruliste, suure väärtusega ja ebatavaliste tehingute puhul, millel ei ole mõistlikku majanduslikku eesmärki.

11.4.4. Kui MAINSTON INTERNATIONAL OÜ töötaja peab kliendi või tehingus osaleva isikuga seotud riski suureks, peab ta rakendama tugevdatud hoolsusmeetmeid.

12. Uute ja olemasolevate tehnoloogiate, toodete ja teenustega seotud riskide kindlakstegemine

12.1. Enne uue finantsteenuse või -toote või uute või ebatraditsiooniliste müügikanalite pakkumist klientidele või uute või arenevate tehnoloogiate kasutuselevõtmist hindab MAINSTON INTERNATIONAL OÜ juhatus koostöös rahapesu andmebüroo kontaktisikuga (rahapesu tõkestamise eest vastutav ametnik) toodete või teenustega seotud rahapesu ja terrorismi rahastamise riske.

12.2. Riskide hindamiseks kaardistab MAINSTON INTERNATIONAL OÜ juhatus koos määratud rahapesu andmebüroo kontaktisikuga (rahapesu tõkestamise eest vastutava ametnikuga) ja vajadusel teiste töötajatega iga uue toote teenuse, tehnoloogia või müügikanaliga seotud riskid.

12.3. Riskihindamise käigus hinnatakse nii tegelikke kui ka potentsiaalseid riske ning vajaduse korral kogutakse lisateavet riskide ja riskimaandamismeetmete kohta.

12.4. Pärast riskide kaardistamist hindab MAINSTON INTERNATIONAL OÜ juhatus riski realiseerumise tõenäosust ja riski taset, pöörates erilist tähelepanu riske suurendavatele ja vähendavatele asjaoludele.

12.5. Pärast riskide ja nende mõju hindamist hindab MAINSTON INTERNATIONAL OÜ kõige sobivamaid vastumeetmeid konkreetsete riskide maandamiseks MAINSTON INTERNATIONAL OÜ riskivalmidusele vastavale tasemele ja vajadusel korraldab vastavate meetmete rakendamise.

12.6. MAINSTON INTERNATIONAL OÜ hindab, kas meetmete rakendamine võib viia uute finantsteenuste või -toodetega, uute või ebatraditsiooniliste müügikanalite või uute või arenevate tehnoloogiatega seotud rahapesu ja terrorismi rahastamise riskid tasemele, mis vastab MAINSTON INTERNATIONAL OÜ riskivalmiduse tasemetele.

12.7. Uue finantsteenuse või toote, uute või ebatraditsiooniliste müügikanalite pakkumist kliendile või uue või areneva tehnoloogia kasutuselevõtmist võib alustada ainult siis, kui sellega seotud rahapesu ja terrorismi rahastamise riskid on kooskõlas MAINSTON INTERNATIONAL OÜ riskivalmidusega või neid riske on võimalik viia vastuvõetavale tasemele.

13. Riskijuhtimise mudel

13.1. MAINSTON INTERNATIONAL OÜ juhatus arvestab käesolevas riskihinnangus esitatud riske ja riskivalmidust ettevõtte üldjuhtimist puudutavate otsuste tegemisel (äristrateegia koostamine, uute toodete/teenuste arendamine). Rahapesu ja terrorismi rahastamise riskide vähendamiseks on võtmetähtsusega hoolsusmeetmete proportsionaalne ja riskipõhine kohaldamine.

13.2. Teabe edastamine juhatuse ja töötajate vahel

13.2.1. Riskivalmiduse mahtu jälgib igapäevaselt üks juhatuse liige.

13.2.2. Rahapesu andmebüroo kontaktisik (rahapesu tõkestamise eest vastutav ametnik) annab kord aastas juhatusele aru riskide realiseerumise/ennetamise kohta.

13.2.3. Töötajad teavitavad rahapesu andmebüroo kontaktisikut (rahapesu tõkestamise eest vastutavat ametnikku) või juhatuse vastutavat liiget nende vastutusalasse kuuluvate tegevuste, toodete ja protsessidega seotud riskide tuvastamisest, sealhulgas tööjuhistes ja/või programmis esinevate vigade tuvastamisest.

13.2.4. Riskivalmiduse või riskihinnangu muutmise korral teavitab juhatus viivitamata töötajaid muudatustest ja teeb need elektrooniliselt kättesaadavaks.

13.2.5. Tagatakse, et töötajad, kes teatavad rahapesu või terrorismi rahastamise kahtlusest või rahapesu tõkestamise seaduse rikkumisest MAINSTON INTERNATIONAL OÜ-sisesele rahapesu andmebüroo kontaktisikule (rahapesu tõkestamise eest vastutavale ametnikule), on kaitstud teiste töötajate, juhatuse liikmete või klientide ähvarduste või vaenuliku tegevuse ning ebasoodsa ja diskrimineeriva ametialase kohtlemise eest.

13.3. Riskide vältimiseks juhatus

13.3.1. täiustab ja ajakohastab pidevalt olemasolevaid IT-lahendusi;

13.3.2. võtab kasutusele uusi, täielikult automatiseeritud tarkvaralahendusi, mis viivad inimliku eksimuse või eeskirjade tahtlike eiramise võimaluse peaaegu nulli;

13.3.3. võtab uute teenuste arendamisel arvesse riskivalmidust ja viib vajaduse korral läbi täiendavaid riskihindamisi;

13.3.4. annab töötajatele kiiresti juhiseid;

13.3.5. tagab tõhusa sisekontrolli töötajate töö üle, määrates selleks siseaudiitori.