Finantsinspektsioon

Finantsinspektsiooni soovituslik juhend

Tallinn

NÕUDED OPERATSIOONIRISKI JUHTIMISE KORRALDAMISEKS

Soovituslik juhend on kehtestatud Finantsinspektsiooni juhatuse 18.05.2005 otsusega nr 1.1-7/63 ja muudetud Finantsinspektsiooni juhatuse 12.02.2018 otsusega nr 1.1-7/42 ning 05.08.2019 otsusega nr 1.1-7/93 Finantsinspektsiooni seaduse § 57 lõike 1 ja lõike 3 alusel.

I OSA Üldsätted ja mõisted

1. Soovitusliku juhendi kohaldamine ja eesmärk

1.1. Käesolev juhend reguleerib operatsiooniriskide juhtimist Finantsinspektsiooni seaduse § 2 lõikes 1 toodud finantsjärelevalve subjektides (edaspidi *ettevõtja*).

1.2. Juhendis esitatud juhised on mõeldud järgimiseks kooskõlas õigusaktides kehtestatud nõuetega.

1.3. Juhendis toodud nõuded on üldistused, mida ettevõtja peab arvestama organisatsiooni vajadustele ja võimalustele vastava operatsiooniriski juhtimise korraldamisel.

1.4. Juhendi rakendamise ulatus sõltub ettevõtja organisatsioonistruktuurist ja –kultuurist, äritegevuse mahust ja riskitasemest, pakutavate finantsteenuste ja -toodete õiguslikust keerukusest ning riskijuhtimislikust ja raamatupidamislikust iseärasusest.

1.5. Juhendi eesmärgiks on aidata kaasa ettevõtja:
- tegevuses sisalduvate operatsiooniriskide identifitseerimisele ja juhtimisele vastavalt ettevõtja äritegevuse ulatusele, keerukusele ja varasemale kogemusele;
- võimele anda adekvaatne hinnang operatsiooniriskile;
- operatsiooniriski juhtimise kahjusid ennetavale tegevusele.

1.6. Käesolevas juhendis on operatsiooniriski määratlemisel ja soovituste kujundamisel kasutatud Baseli Pangajärelevalve Komitee poolt 2003.a veebruaris välja antud dokumendi “Sound Practices for the Management and Supervision of Operational Risk” sisu ja standardeid.

2. Juhendis kasutatavad mõisted

2.1. **Operatsioonirisk** – risk saada kahju sisemiste protsesside, inimeste tegevuse või süsteemide ebaadekvaatsusest või mittetoimimisest oodatud viisil või välistest sündmustest. Mõiste sisaldab juriidilist riski, kuid ei sisalda strateegilist, reputatsiooni ja süsteemiriski.

2.2. **Juriidiline risk** – risk, et õigustatud osapool ei saa rakendada oma õigusi või oodata kohustuste täitmist, kuna kohustatud osapool ei täida võetud kohustusi.

2.3. Strateegiline risk – konkurentsi ja tegevuskeskkonna, järelevalve mõju ettevõtja otsustele ja tegevusele ning ärieesmärkide saavutamisele.

2.4. Reputatsioonirisk – negatiivne avalikkuse tähelepanu ettevõtja äritegevuse suhtes, sõltumata selle tõesusest, toob kaasa kliendibaasi kahanemise, vähendab sissetulekuid või tõstab kulutusi õigusabile.

2.5. Süsteemirisk – probleemid ühe ettevõtja tegevuses mõjutavad teiste ettevõtjate ja / või kogu finantssüsteemi toimimist.

2.6. Operatsiooniriski positsioon – ettevõtja üksuse / ärivaldkonna / toote, teenuse või muu üheselt määratletava organisatsiooniosa või tegevuse võimalike operatsiooniriski kahjujuhtumite rahalises ekvivalendis väljendatud suurus.

2.7. Riskiprofiil – ettevõtja sisemine, kvalitatiivne hinnang organisatsiooni, üksuse, ärivaldkonna, toote ja teenuse või muu üheselt määratletava organisatsiooniosa või tegevuse operatsiooniriski suurusele.

2.8. Sisekontroll – meetmed, mille rakendamist korraldavad organisatsiooni nõukogu, juhatus ja töötajad ning mis on suunatud tagama piisavat kindlust, et organisatsiooni eesmärkide saavutamiseks on tagatud:
- tegevuse efektiivsus ja tõhusus;
- finantsaruannete usaldusväärsus ja õigsus;
- vastavus kehtivale seadusandlusele ja sise-eeskirjadele.

2.9. Sisekontrolli keskkond – ettevõtjasisene käitumiskultuur, mis kujundab töötaja suhtumise sisekontrolli. Keskkonda mõjutavateks teguriteks on organisatsiooni eetilised põhimõtted, sisemised formaalsed ja mitteformaalsed käitumiseeskirjad ning nõukogu, juhatuse ja struktuuriüksuste juhtide käitumine ning juhtimisstiil (õiguste ja kohustuste volitamine, organisatsiooni ja töötajate arendamine jms).

2.10. Siseaudit – sõltumatu, objektiivne kindlust andev (hindav) ja konsulteeriv tegevus, mille eesmärgiks on aidata kaasa organisatsioonil kindlate reeglite järgi hinnata ja tõhustada riskijuhtimise, kontrolli ning organisatsiooni haldamise tulemuslikkust.

2.11. Välise teenusepakkuja kasutamine (*outsourcing*) - ettevõtja igapäevategevuse teostamiseks vajaliku tegevuse (nt infotehnoloogia arendamine ja haldamine, sularahakäitlus, administreerivad tegevused, personalihaldus, kinnisvarahaldus, transport jms) teostamise volitamine kolmandale isikule.

2.12. Äritegevuse jätkuvuse tagamine (*business continuity management*) – tegevus, mille eesmärk on tõsta ettevõtja valmisolekut reageerida äritegevuse katkestusele, võimaldades taastada võtmetegevused, süsteemid ja protsessid kokkulepitud aja jooksul, säilitades samal ajal organisatsiooni kriitilised tegevused.

II OSA Operatsiooniriski juhtimine

3. Operatsiooniriski määratlemine

3.1. Operatsioonirisk on iseseisev riskivaldkond.

3.2. Iga ettevõtja peab sisemiseks kasutamiseks andma omapoolse operatsiooniriski definitsiooni. Operatsiooniriski mõiste sisustamisel tuleb lähtuda ettevõtja tegevuse ulatusest ja keerukusest, varasematest riskijuhtimise kogemustest ning selgelt määratleda ettevõtjas operatsiooniriski põhjustavad tegurid (vt juhendi Lisa 1).

3.3. Operatsiooniriski mõiste sisu peab olema vastavuses ettevõtja äritavadega (kasutatavad IT lahendused ja nende keerukus, väliste teenusepakkujate kasutamine, personalipoliitika, pakutavate teenuste ja toodete riskijuhtimise keerukus, välise kindlustuse kasutamine jms).

4. Operatsiooniriski juhtimise korraldamine

4.1. Operatsiooniriski juhtimine on iseseisev riskijuhtimisvaldkond.

4.2. Operatsiooniriski juhtimine peab olema osa organisatsiooni üldisest juhtimisest ja riskijuhtimissüsteemist.

4.3. Operatsiooniriski juhtimisega peab kaasnema ettevõtja paremini määratletud ja positsioneeritud tegevus, liikumine kaitsvalt riske analüüsivale ja kahjujuhtumeid ennetavale tegevusele.

4.4. Operatsiooniriski juhtimise korraldamisel peab arvestama, et operatsiooniriski kahjud ei ole kõigil juhtudel mõõdetavad ja võivad realiseeruda olulise viivitusega ja / või kaudselt.

4.5. Operatsiooniriski juhtimine on protsess, mis eeldab kogu organisatsiooni ühtset arusaama operatsiooniriskist ning toetub kõrgele organisatsioonikultuurile koos vastava riskikultuuri ja positiivse suhtumisega sisekontrolli.

4.6. Operatsiooniriski juhtimisel tuleb hoiduda alusetu “turvatunde” tekkimisest, mis võib viia valede eesmärkide seadmise ja soovimatute tulemusteni (eelkõige tegevuse jätkuvuse tagamise korraldamisel).

4.7. Ettevõtja peab juhendi rakendamisel leidma organisatsiooni jaoks optimaalse, majanduslikult mõistliku lahenduse, mis on kooskõlas äritegevuse ulatusega ja hõlmab organisatsioonistruktuuri kõiki juriidilisi ja ärilisi üksuseid. Juhendis toodud nõuete rakendamisel organisatsiooni erinevates allüksustes tuleb vältida liigset bürokraatiat ja lähtuda operatsiooniriski juhtimise tõhususe ning loodava lisaväärtuse eeldusest.

4.8. Olulisel kohal on ettevõtja arusaam äritegevuses sisalduvatest operatsiooniriskidest ning valmisolek lisaks tavapärastele riskijuhtimissüsteemidele ja –vahenditele (analüüsimudelid ja –programmid, stresstestid jms) pöörata tähelepanu operatsiooniriski juhtimisele.

4.9. Juhendis toodud ettevõtja nõukogu ja juhatuse vaheline kohustuste ja vastutuse jaotus on tinglik, sõltudes konkreetse ettevõtja juriidilisest ja organisatsioonilisest struktuurist ning juhtimiskultuurist. Kohase ja tõhusa operatsiooniriski juhtimise korraldamise eelduseks on juhendis toodud põhimõtete ettevõtjasisene kehtestamine ja rakendamine.

4.10. Ettevõtja operatsiooniriski juhtimise-alane tegevus peaks olema sõltumatu ülevaatuse ja hinnangu objektiks.

5. Ettevõtja nõukogu ülesanded

5.1. Nõukogu ülesandeks on tagada ettevõtja operatsiooniriski juhtimiseks vajaliku organisatsioonilise, äritegevuse ja riskijuhtimise struktuuri ning tegevuse kontrollimise üldpõhimõtete kinnitamine.

5.2. Kui ettevõtte tegevuse maht ja ulatus ei võimalda otstarbekusest lähtuvalt tagada äri- ja kontrollistruktuuride eraldatust, tuleb organisatsioonis leida võimalused riskide maandamiseks teisi meetmeid kasutades (nt täiendavad kontrollid, aruandlus, nelja-silma põhimõte jms).

5.3. Nõukogu ülesanne on tagada sisekontrolli keskkonna kujundamine, mis toetab tõhusat, kõiki ettevõtja üksusi ja tegevusi hõlmavat operatsiooniriski juhtimist.

5.4. Nõukogu peab kinnitama operatsiooniriski mõiste ja riski juhtimise üldpõhimõtted (poliitika) ning neid regulaarselt üle vaatama, arvestades muudatustega ettevõtja tegevuses ja tegevuskeskkonnas.

5.5. Nõukogu peab koostöös juhatusega eraldama operatsiooniriski juhtimise pidevaks arenguks ja rakendamiseks vajalikud ressursid (eelarvelised vahendid, vastava kvalifikatsiooniga ja motiveeritud töötajad).

5.6. Nõukogu peab olema teadlik ja omama selget arusaama ettevõtja organisatsiooni (IT, personal jms), tegevusvaldkondade ja –keskkonna peamistest operatsiooniriskidest. Nõukogu peab saama regulaarseid aruandeid ja ülevaateid ettevõtja operatsiooniriski positsiooni, selle muutumist põhjustanud asjaolude ja operatsiooniriski kahjujuhtumite kohta.

5.7. Nõukogu peab tagama ettevõtja siseauditi võime (vastava kompetentsiga ja motiveeritud personal) hinnata operatsiooniriski juhtimisega seotud sise-eeskirju ja tegevusi. Siseauditi tegevus peab olema piisava ulatusega saamaks kinnitust operatsiooniriski juhtimise adekvaatsusest ja tõhususest.

5.8. Siseaudit ei tohiks olla vastutav operatsiooniriski juhtimisega seotud otseste tegevuste eest, kuid sõltuvalt ettevõtja tegevusmahust ja riskide iseloomust tuleb leida koostöös riskijuhtimist teostavate üksustega optimaalne, majanduslikult ja sisuliselt mõttekas lahendus.

6. Ettevõtja juhatuse ülesanded

6.1. Juhatuse ülesandeks on organisatsiooni struktuuri kujundamine selliselt, et selgelt on määratletud struktuuriüksuste vastutusvaldkonnad, alluvussuhted ja aruandluskord. Tagatud peab olema organisatsiooni äri- ja kontrollistruktuuride vastutus- ja aruandlussuhete eraldatus.

6.2. Juhatuse ülesandeks on rakendada organisatsioonis rutiinid, mis lähtuvad heast riskijuhtimistavast (funktsioonide lahusus, nelja-silma põhimõte jms.), tagada nende täitmine ja kindlustada sisekontrolli keskkonna toimimine kasutades regulaarseid aruandeid ning vajadusel kaasates siseauditi.

6.3. Juhatus on vastutav nõukogu poolt kinnitatud operatsiooniriski juhtimise põhimõtete (poliitika) ellurakendamise eest organisatsioonis.

6.4. Operatsiooniriski juhtimise poliitika peab rakenduma kogu organisatsioonis ja kõik organisatsioonitasemed peavad mõistma operatsiooniriski juhtimisega seotud vastutust ning tagama seonduvate kohustuste täitmise.

6.5. Juhatus vastutab ettevõtja kõigi toodete, tegevuste, protsesside ja süsteemide operatsiooniriski juhtimise alampoliitikate ning sise-eeskirjade väljatöötamise eest. Kuigi iga struktuuriüksuse juht vastutab oma vastutusala operatsiooniriski juhtimise põhimõtete ja sise-eeskirjade sobivuse ning tõhususe eest, peab juhatus kirjeldatud tegevuse toimimise tagamiseks selgelt määratlema volitused, vastutuse ja aruandluskorra.

6.6. Juhatus peab tagama, et operatsiooniriski juhtimise poliitika ja selle rakendamise sise-eeskirjad ning tegevused on edastatud kogu personalile kõigis operatsiooniriskile avatud struktuuriüksustes. Tagatud peab olema töötajate selge arusaam oma ametikohaga seotud riskijuhtimisalastest õigustest ja kohustustest.

6.7. Juhatus peab kindlustama, et operatsiooniriski juhtimisega seotud igapäevategevusi teostaks kvalifitseeritud ja piisava kogemuse ning tööks vajalike tehniliste vahenditega kindlustatud personal.

6.8. Organisatsiooni riskijuhtimise jälgimise ja elluviimise eest vastutavatel töötajatel peavad olema tema poolt järelevalvatavatest struktuuriüksustest ja tegevustest sõltumatud volitused.

6.9. Operatsiooniriski juhtimise eest vastutav personal peab olema pidevas infovahetuses krediidi-, turu- ja muude riskide eest vastutavate töötajatega.

6.10. Juhatus peab organisatsioonis rakendama kompenseerimispoliitikat (töötasu, lisatasud, hüvitised jms), mis on vastavuses ettevõtja riskiprofiiliga ja toetab head riskijuhtimistava ning sisekontrolli keskkonda.

7. Operatsiooniriski poliitika

7.1. Operatsiooniriski poliitika eesmärgiks on anda riski mõiste ja määratleda riski identifitseerimiseks, mõõtmiseks, jälgimiseks ja maandamiseks ning kontrolliks kasutatavad meetodid ning vahendid.

7.2. Operatsiooniriski poliitika peab olema aluseks kogu ettevõtja operatsiooniriski-alase tegevuse juhtimisel. Nimetatud dokumendis antav sisu peab olema kooskõlas ettevõtja tegevuse ulatuse ja mahuga ning hõlmama kõiki ettevõtja tegevuses sisalduvaid operatsiooniriske.

7.3. Operatsiooniriski poliitika peab sisaldama viiteid operatsiooniriski juhtimise seisukohalt olulistele valdkondadele. Sellisteks valdkondadeks on näiteks organisatsiooni füüsiline turvalisus, IT süsteemide käideldavus ja andmekaitse, tegevuse jätkuvus, rahapesu tõkestamine, personalipoliitika jms.

7.4. Sõltuvalt ettevõtja tegevuse ulatusest ja mahust ning pakutavate teenuste ja toodete iseloomust tuleb operatsiooniriski poliitikas määratleda tegevused, mille eesmärk ja sisu otseselt või kaudselt mõjutab organisatsiooni tegevust operatsiooniriski juhtimisel. Sellisteks tegevusteks on näiteks uute toodete ja teenuste väljatöötamine, väliste teenusepakkujate valimine, arendustegevused (sh IT) jms.

8. Operatsiooniriski identifitseerimine ja hindamine

8.1. Operatsiooniriski identifitseerimise ja klassifitseerimise aluseks peab olema üleorganisatsiooniline arusaam operatsiooniriski kahjujuhtumitest. Kahjujuhtumite selge määratlus võimaldab operatsiooniriski krediidi- ja tururiskist eristada ning kvantitatiivselt hinnata.

8.2. Ettevõtja peab identifitseerima ja hindama kõigi toodete, tegevuste, protsesside ning süsteemidega seotud operatsiooniriske. Samuti tuleb kindlustada, et enne uue toote, tegevuse, protsessi ja süsteemi tutvustamist või kasutuselevõtmist toimub sellega seotud operatsiooniriskide adekvaatne hindamine.

8.3. Tõhus riski identifitseerimine peab arvestama nii siseseid (nt organisatsioonistruktuuri keerukus, tegevuse iseloom, personali kompetents, organisatsioonilised muutused ja personali voolavus) kui väliseid faktoreid (nt tegevusharu muutused ja tehnoloogia areng), mis võivad avaldada negatiivset mõju ettevõtja eesmärkide saavutamisele.

8.4. Lisaks operatsiooniriskide identifitseerimisele peab ettevõtja hindama oma tundlikkust antud riskide suhtes. Tõhus riskihindamine võimaldab paremini mõista ettevõtja riskiprofiili ja kõige otstarbekamalt kasutada riskijuhtimise vahendeid.

8.5. Operatsiooniriski identifitseerimiseks kasutatavate protsesside / tegevuste näideteks on:

- riskide kaardistamine, mille käigus organisatsiooni allüksus või äri- ja abiprotsessi omanik kaardistab oma üksuse / valdkonna / protsessi riskid riski tüübi alusel;
- riskihindamine, mille käigus organisatsiooni allüksus või äri- ja abiprotsessi omanik teostab olulisemate riskide osas riskijuhtumi esinemise tõenäosuse ja finantsilise mõju analüüsi (vajadusel kasutades selleks riskijuhtimise valdkonna töötajate ja / või väliskonsultantide abi);
- tähtsamad riskiindikaatorid (*key risk indicators*): riskiindikaatoriteks on statistika ja/või meetrika (mõõtmised), sageli finantsilised, mis annavad informatsiooni riskipositsiooni kohta. Antud indikaatoreid vaadatakse tavaliselt üle regulaarselt (kuiselt või kvartaalselt) olemaks kursis riski kaasa tuua võivate muutustega. Sarnasteks indikaatoriteks võivad olla ebaõnnestunud tehingute arv, personali voolavuse määr ning vigade ja tegematajätmiste sagedus ja/või raskusaste;
- riskiindikaatoritega seotud piiride / limiitide jälgimine: antud piirangute ületamine annab juhtkonnale informatsiooni potentsiaalsete probleemidega valdkondade olemasolust.

8.6. Informatsiooni ettevõtja operatsiooniriskile avatuse hindamiseks võivad anda andmed varasemate perioodide kahjude kohta. Tõhus viis antud informatsiooni kogumiseks ja kasutamiseks on luua klassifikatsioon süstemaatiliseks, konkreetsete kahjujuhtumite sageduse, raskusastme ja muu informatsiooni leidmiseks ja salvestamiseks.

8.7. Klassifitseerimissüsteemi aluseks on otstarbekas võtta Baseli Pangajärelevalve Komitee poolt välja töötatud klassifikatsioon (vt juhendi Lisa 2). Klassifikatsioonisüsteem võib ettevõtjates erineda, kuid üldjuhul peab süsteem hõlmama järgmiseid kahjujuhtumite liike:

- sisemine pettus;
- väline pettus;
- värbamispraktika ja töökeskkonna turvalisus;
- kliendid, tooted ja äripraktika;
- varaline kahju;
- äritegevuse katkestus ja süsteemivead;
- tehingute teostamine, edastamine ja protsessi juhtimine.

8.8. Operatsiooniriski kahjujuhtumite konkreetsetesse klassidesse määramine, lähtudes operatsiooniriski juhtumi üldisest olemusest, annab võimaluse hinnata mainitud juhtumite tõenäosuse ja mõju vähendamiseks kasutatavaid riskimaandamise meetmeid. Kahjujuhtumite klassifitseerimise süsteem peab ettevõtjal aitama määrata potentsiaalselt olulist kahju tekitavate juhtumite tüübid ja andma otsest informatsiooni riskijuhtimismeetmete kasutamise vajaduse ning efektiivsuse/tõhususe kohta.

8.9. Ettevõtjal on soovitatav, lisaks operatsiooniriski klassifitseerimisele kahjujuhtumi tüübi alusel, klassifitseerida kahjumeid ka peamiste äritegevuste lõikes. Nimetatud klassifitseerimise aluseks olevad äritegevused võivad ettevõtjates erineda. Krediidiasutusel on soovitatav lähtuda juhendi Lisas 3 toodud klassifikatsioonist.

8.10. Kahjujuhtumite andmed koosnevad peamiselt tavapärastest, sagedastest ja väikese mõjuga juhtumitest ning harvadest suure mõjuga juhtumitest. Otstarbekas on kehtestada raporteerimissüsteem, mis võimaldab leida ja registreerida mõlemat tüüpi kahjujuhtumeid, kaasa arvatud välisinfo suurte kahjujuhtumite kohta.

8.11. Ettevõtjasiseste suure mõjuga kahjujuhtumitega kaasneb üldjuhul vastava valdkonna, tegevuse (või kogu ettevõtja samadele kriteeriumitele vastavate valdkondade, tegevuste) kontrollisüsteemi parendamine, mis peab oluliselt vähendama sarnaste kahjujuhtumite tulevikus esinemise tõenäosust. Saavutamaks kahjujuhtumeid ennetav kontrollikeskkond on oluline pöörata tähelepanu ettevõtjaga sarnastes organisatsioonides toimunud suure mõjuga kahjujuhtumitele, nende toimumise tingimustele ja asjaoludele. See annab võimaluse kontrollida sarnaste kahjujuhtumite esinemise võimalikkust ja testida organisatsiooni kontrollikeskkonna toimimist ning tunduvalt vähendada kahjujuhtumite toimumise tõenäosust ja/või majanduslikku mõju.

9. Operatsiooniriski jälgimine

9.1. Tõhus jälgimisprotsess on hädavajalik adekvaatse operatsiooniriski juhtimise tagamiseks. Regulaarne tegevuste jälgimine annab võimaluse operatsiooniriski juhtimise poliitikates, protsessides ja sise-eeskirjades leiduvate vigade kiireks avastamiseks ja parandamiseks ning kahjude ärahoidmiseks.

9.2. Lisaks operatsiooniriski kahjujuhtumine jälgimisele peab ettevõtja identifitseerima ja jälgima indikaatoreid, mis aitaksid tulevasi kahjusid ennetada. Mainitud riskiindikaatorid (*key risk indicators*) peavad olema ettevaatavad ja peegeldama potentsiaalseid operatsiooniriski allikaid nagu kiire kasv, uute toodete tutvustamine, personali voolavus, ülekannete ja tegevuste katkestused, süsteemi katkestused jne. Kui riskiindikaatorite limiidid on otseselt seotud mainitud indikaatoritega, aitab tõhus jälgimisprotsess olulisi riske läbipaistvalt identifitseerida ja annab võimaluse tegutseda vastavalt (kasvavatele) riskidele.

9.3. Riskiindikaatorid võivad olla nii konkreetse äriliini põhised kui ka hõlmata ettevõtja kõiki tegevusvaldkondi ja üksusi. Indikaatorite näideteks on:
- kliendikaebuste arv;
- klientide kompenseerimiste arv;
- katkestatud ülekannete ja tehingute arv;
- töötajate voolavus;
- järelevalve poolsete märkuste / ettekirjutuste arv;
- (IT) süsteemide mittetoimimise juhtumite arv, käideldavus;
- uuendamist vajavate sisemiste poliitikate ja sise-eeskirjade arv.

9.4. Jälgimine on tõhusaim kui kontrollisüsteem on integreeritud ettevõtja tegevusse ja on kehtestatud vastav regulaarne aruandlus. Mainitud jälgimise tulemused peavad kajastuma lisaks vastava valdkonna juhile esitatavas aruandluses ka juhatusele ja nõukogule esitatavates aruannetes. Antud jälgimise sisendiks võib olla ka järelevalve poolt koostatud raportite sisu.

9.5. Juhatus ja nõukogu peavad saama regulaarseid raporteid nii äriüksustelt kui siseauditi üksuselt (lisaks peavad raportid olema kättesaadavad ka kõigile nende sisuga seotud üksuste juhtidele). Raportid peavad sisaldama sisemist finants-, tegevus- ja regulatsioonidele vastavuse informatsiooni ning käsitlema kõiki identifitseeritud probleemseid valdkondi ja motiveerima kasutama õigeaegseid meetmeid.

9.6. Kirjeldatud riski ja auditi raportite kasulikkuse ning usaldusväärsuse tagamiseks peab juhtkond regulaarselt hindama raporteerimissüsteemi ja sisekontrolli õigeaegsust, täpsust ja asjakohasust, kasutades selleks väljaspool organisatsiooni ettevalmistatud raporteid (audiitorid, järelevalve). Raporteid peab analüüsima eesmärgiga parandada olemasoleva riskijuhtimise tulemusi ja ette valmistada uusi riskijuhtimise poliitikaid, sise-eeskirju ja praktikaid.

10. Operatsiooniriski kontrollimine ja maandamine

10.1. Ettevõtjal peavad olema poliitikad, protsessid ja sise-eeskirjad oluliste operatsiooniriskide kontrollimiseks ja maandamiseks. Hinnata tuleb alternatiivsete riskilimiteerimise ja - kontrolli strateegiate sobivust ning kohandada operatsiooniriski profiili sobivate strateegiate abil, arvestades ettevõtja üldist riskitaluvust ja -profiili.

10.2. Identifitseeritud riskide käsitlemiseks peavad olema ette nähtud kontrollitegevused. Kontrollitavate riskide puhul peab ettevõtja otsustama, mil määral soovitakse kontrollitoiminguid ja muid sobivaid meetmeid kasutada ning mil määral riski lihtsalt aktsepteerida. Mittekontrollitavate riskide puhul peab ettevõtja otsustama kas riski aktsepteerida või vähendada või loobuda antud riskiga seotud tegevusest.

10.3. Ettevõtjal peab olema välja töötatud ning rakendatud kontrollitoimingud ja sise-eeskirjad tagamaks tegevuse vastavust kehtestatud sisemistele riskijuhtimise poliitikatele. Selles sisalduvateks põhielementideks võiksid olla:
- tipptaseme ülevaated arendustegevuses püstitatud eesmärkide saavutamisel;
- dokumenteeritud volituste ja kinnituste andmise süsteem, kindlustamaks et toiminguid teostatakse sobival/õigel juhtimistasandil;
- mittevastavuste ülevaatamist, käsitlemist ja lahendamist reguleerivad poliitikad, protsessid ja sise-eeskirjad.

10.4. Kuigi formaalsete ning kirjalike poliitikate ja sise-eeskirjade süsteem on hädavajalik, tuleb kontrollitegevusi ellu viia tugeva sisekontrolli abil. Tõhususe tagamiseks peavad kontrollitegevused olema igapäevategevuste integreeritud osa, mis võimaldab kiirelt reageerida tingimuste muutustele ning vältida ebavajalikke kulusid.

10.5. Tõhus sisekontrolli keskkond eeldab piisava funktsioonide lahususe olemasolu ja personalile potentsiaalset huvide konflikti tekitada võivate ülesannete määramise vältimist. Huvide konflikti sisaldavate ülesannete määramine töötajale või organisatsiooni üksusele võib soodustada personali poolt kahjude, vigade või ebasobivate tegevuste teostamist. Seetõttu tuleb potentsiaalsed huvide konfliktid identifitseerida, minimiseerida, võtta need sõltumatu jälgimise alla ja tagada vastavate andmete kaasatus riskiraportitesse.

10.6. Lisaks ülesannete lahususele peab ettevõtja kindlustama, et operatsiooniriski kontrollimiseks on rakendatud ka teisi meetmeid, nagu näiteks kehtestatud limiitide ja piirmäärade jälgimine, varadele ja dokumentidele juurdepääsu ja kasutuse kontroll (turvalisuse tagamine), personali piisava kogemuse ja koolituse tagamine, oodatust olulisel määral erinevate tulemustega äritegevuste ja toodete identifitseerimine ning regulaarne ülekannete ja kontode vastavuse kontrollimine (*reconciliation*) ning kooskõlastamine.

10.7. Avatus operatsiooniriskile on suurem, kui ettevõtja on alustanud uusi tegevusi või välja töötanud uusi tooteid (eriti kui need tegevused ja tooted ei ole vastavuses põhitegevuse strateegiaga) või sisenenud uutele turgudele. Lähtudes ärieesmärkidest ja nende tavapärasest eelistamisest, eksisteerib oht, et riskijuhtimine ei suuda kindlustada sisekontrolli järelejõudmist uue äritegevuse kasvule. Seetõttu on hädavajalik kirjeldatud olukordades pöörata erilist tähelepanu sisekontrolli arendamisele ja toimimisele.

10.8. Mõned olulised operatsiooniriskid on madala tõenäosusega, kuid potentsiaalselt väga suure majandusliku mõjuga. Kõiki riske ei saa ettevõtja kontrollida (näiteks loodusõnnetused), kuid potentsiaalse kahju või sageduse ja/või raskusastme vähendamiseks saab kasutada maandamise vahendeid või tegevusi. Näiteks saab kasutada kindlustust tõsiste, eriti kohese ja konkreetse väljamaksekohustusega, kuid harvade kahjujuhtumite (näiteks veast ja tegemata jätmisest tingitud kolmanda isiku nõue, töötaja või kolmanda isiku pettus, loodusõnnetus jms) väljapoole ettevõtjat suunamiseks.

10.9. Ettevõtja peab riskide maandamise vahendeid (sh kindlustuslepinguid) käsitlema kui sisemise operatsiooniriski kontrolli lisa, mitte selle asendajat. Tähelepanu tuleb pöörata, millise piirini riskimaandamise vahendid tõesti riske vähendavad või on tegu riski kandumisega teise ärivaldkonda või uue riski loomisega.

10.10. Operatsiooniriski maandamisel on oluline roll investeeringutel pangatehnoloogiasse ja infotehnoloogia turvalisus. Tähelepanu tuleb pöörata asjaolule, et suurenenud automatiseerimine võib sagedase ja väikese kahjumi muuta suureks, kuid harva esinevaks kahjumiks, mille põhjustajaks võib olla sisemistest või välistest faktoritest tingitud tegevuse katkemine või kestev häiritus. Ettevõtja peab mainitud riski käsitlemiseks ette valmistama äritegevuse jätkuvuse plaanid.

III OSA Lõppsätted

11. Juhendi jõustumine

Juhend käesolevas redaktsioonis jõustub alates 30.09.2019.

Lisa 1. Operatsiooniriski põhjustavad tegurid

Töötajad	Vargused Lubamatud tegevused / pettused / väärteod Tööseadusandluse rikkumine Töötajate organiseeritud tegevus Võtmetöötajate puudus või kaotus
Protsessid	Maksed / arveldused / üleandmine Dokumentatsioon / lepingud Väärtuse määramine / hinnastamine Puudused sise- ja välisraportites Seadusandlusele mittevastamine Müügitegevused
Süsteemid	Investeeringud tehnoloogiasse Arendamine ja rakendamine Võimsuse / mahu puudumine Süsteemi häired / katkestused Turvalisus, infoturve
Välised	Kriminaalne tegevus Välised teenusepakkujad Kohtuasjad Katastroofid, infrastruktuuri häired Poliitiline risk Järelevalve

Lisa 2. Operatsiooniriski kahjujuhtumite klassifikatsioon

Kahjujuhtumi liik	Definitsioon	Kategooriad	Juhtumi näide
Sisemine pettus [*Internal Fraud*]	Kahju, mis tuleneb tegudest, mille eesmärgiks on pettus, seadusevastane vara omandamine või õigusaktidest või ettevõtja poliitikast möödahiilimine, sealhulgas vahetegemise/ diskrimineerimise juhtumid, milles osaleb vähemalt üks sisemine osapool.	Lubamatu tegevus [Unauthorized Activity]	Hooletus tehingute aruandluses, raporteerimata tehingud Lubamatu tehingu tegemine Positsioonide väär esitamine
		Vargus ja pettus [*Theft and Fraud*]	Pettus, krediidipettus, tühjad deposiidid Vargus Väljapressimine Raiskamine Rööv Panga/kliendi vahendite lubamatu kasutamine Teise identiteedi, konto või depoo lubamatu kasutamine Maksukuritegu/maksudest kõrvalehoidmine Altkäemaks Kuritahtlik varade hävitamine *Insider* tehingud (enda nimel)
Väline pettus *[External Fraud]*	Kahju, mis tuleneb tegudest, mille eesmärgiks on pettus, seadusevastane vara omandamine või õigusaktidest möödahiilimine kolmanda osapoole poolt.	Vargus ja pettus *[Theft and Fraud]*	Vargus Rööv Võltsimine Pettus
		IT-turvalisus *[System Security]*	Tungimine IT süsteemi, arvutitesse Informatsiooni vargus
Värbamispraktika ja töökeskkonna turvalisus *[Employment Practices and Workplace Safety]*	Kahju, mis tuleneb tööhõive-, tervisekaitse- või ohutusalaste seaduste või kokkulepetega vastuolus olevatest tegudest, isikukahjunõuete väljamaksmisest või vahetegemise/ diskrimineerimise juhtumitest.	Töösuhted *[Empolyee Relations]*	Kompensatsiooni, hüvitise maksmise ja töösuhe lõpetamisega seotud probleemid Töötajate organiseeritud tegevus
		Töökeskkond [*Safe Environment]*	Üldine tsiviilvastutus Töötajate tervisekaitse ja tööohutuseeskirjadega seonduvad juhtumid Kompenseerimine
		Diskrimineerimine *[Diversity & Discrimination]*	Diskrimineerimine
Kliendid, tooted ja äripraktika *[Clients, Products & Business Practices]*	Kahju, mis tuleneb konkreetsete klientide ees ametialaste kohustuste (sealhulgas usaldus- ja sobivusnõuete) tahtmatust või	Informatsiooni-kohustus, sobivus ja usaldus *[Suitability, Disclosure & Fiduciary]*	Usaldusisikuna kohustuse / juhise rikkumine Pangasaladuse avaldamise juhtum Pangasaladuse hoidmise kohustuse rikkumine tarbija suhtes Agressiivne müük Privaatsuse rikkumine Konfidentsiaalse info väärkasutus Ülemäärane kauplemine kliendi arvel

	hooletust täitmatajätmisest või toote olemusest või konstruktsioonist.		eesmärgiga saada põhjendamatut tasu Laenuandja vastutus
		Sobimatud ärimeetodid *[Improper Business or Market Practices]*	Keelatud tehing / turutava Turuga manipuleerimine Tegutsemine ilma loata Rahapesu *Insider* tehing (ettevõtja nimel)
			Litsentseerimata tegevus
		Puudulikud tooted või teenused *[Product Flaws]*	Puudus või viga toote või teenuse vormistuses (nt riskianalüüsi heakskiiduta) Puudus või viga mudelis
		Puudulik kliendihinnang *[Selection, Sponsorship & Exposure]*	Kõrvalekalle kliendi hindamise instruktsioonist Kliendilimiidi ületamine
		Nõustamine *[Advisory Activities]*	Vaidlus teostatud nõustamise üle
Varaline kahju *[Damage to Physical Assets]*	Kahjud, mis tulenevad materiaalsete varade kaotusest või kahjustumisest loodusõnnetuse või muude sündmuste tõttu.	Kallaletungid, katastroofid ja õnnetused *[Disasters and other events]*	Loodusõnnetused Terrorism Vandalism
Äritegevuse katkestus, süsteemirikked *[Business Disruption and System Failures]*	Kahju, mis tuleneb äritegevuse katkestustest või süsteemiriketest.	Süsteemid *[Systems]*	Tarkvara Riistvara Telekommunikatsioonid Tehniline rike / katkestus (vesi, elekter jne)
Tehingu teostamine, edastamine ja protsessijuhtimine *[Execution, Delivery & Process management]*	Kahju ebaõnnestunud tehingutöötlusest või protsessi-juhtimisest, suhetest kaubanduspartnerite ja tarnijatega.	Tehingute alustamine, teostamine ja hooldamine *[Transaction Capture, Execution & Maintenance]*	Puudus kommunikatsioonis Viga andmehankes, andmete säilitamises ja andmevahetuses Ületatud tähtaeg või täitmata kohustus Mudeli / süsteemi väär kasutamine Raamatupidamisviga Muu ülesande puudulik täitmine Tarneviga Tagatise väärkäsitlemine Võrdlusandmete hooldamise viga

		Järelevalve ja aruandlus *[Monitoring and Reporting]*	Aruandmiskohustuse täitmata jätmine Viga avalikus aruandes
		Informatsioon ja dokumentatsioon kliendi kohta *[Customer Intake and Documentation]*	Puudub kliendi heakskiit / kinnitus Puudub / puudulik õigusdokument
		Kliendi konto käsitlemine [*Customer / Client Account Management*]	Volitamata ligipääs kontole Viga kliendi andmetes (tekkinud kahju) Kahju kliendi vahenditele, mille on tinginud hooletus
		Vastaspool finantsinstrumenti-dega kauplemisel *[Trade Counterparties]*	Valesti osutatud teenus vastaspoolelt, kes ei ole klient
		Teenuse ja toote tarnija [*Vendors & Suppliers]*	*Outsourcing* Vaidlus tarnijaga

Lisa 3. Äritegevuse valdkondade klassifikatsioon

Ärivaldkond	Tegevus
Ettevõtterahandus *(Corporate Finance)*	-nõuandmine ühinemiste ja liitumiste, erastamiste, väärtpaberite, emissioonide, börsiletulekute korral ning omanikele, nõukogule ja juhatusele -garantii andmine ettevõtja finantseerimisele ja liitumistele -erainvesteering noteerimata ettevõtja aktsiatesse -kapitalihanked -riskikapital
Kauplemine ja müük *(Trading & Sales)*	-kauplemine, maakleritegevus ning fondipaberite ja finantsinstrumentide nagu rendi-, valuuta- ja toorainega seotud instrumentide, aktsiate ja teiste väärtpaberite analüüs. -kohustused, nt turugarant -oma pikaajaliste/strateegiliste väätpaberite haldus -väärtpaberilaenud ja repod -omafinantseerimine ja likviidsuskäsitlus (*treasury*)
Jaepangandus *(Retail Banking)*	-massturule ja jõukatele eraklientidele mõeldud pangateenused, nt sisselaenamine, väljalaenamine, nõuandmine, makseteenused, sularahakäitlus, säästutoodete vahendamine ja müük (nt eramaaklerlus) jms. -lühiteenused
Äripangandus *(Commercial Banking)*	-väljalaenamine ja muu finantseerimine suurkliendituru puhul (nt traditsiooniline väljalaenamine, garantiide andmine, ekspordi finantseerimine, projektifinantseerimine, faktooring, liising jne) -kliendi-inkasso
Maksed ja arveldus *(Payment & settlement)*	-maksevahendus -arveldus ja akordeerimine
Administreerimisteenused *(Agency services)*	-deponeerimine, väärtpaberihaldus ja juurdekuuluvad teenused (*corporate actions*) -sihtkapitalihaldus ja notariteenused -väärtpaberilaenu administreerimine
Varahaldus *(Asset management)*	-mis tahes varahaldus -fondihaldus -muu varahaldus
Erakliendimaaklerlus *(Retail brokerage)*	-maaklerlus ja nõuandmine fondipaberite ja finantsinstrumentide nagu rendi-, valuuta- ja toorainega seotud instrumentide, aktsiate, teisesteväärtpaberite ja väärtpaberilaenude alal massiturule ja eraklientidele