LATVIJAS BANKA
EIROSISTĒMA

Vadlīnijas finanšu krāpšanas riska uzraudzībai, pārvaldībai un ierobežošanai

Saturs

1. Vispārīgie jautājumi

1.1. Latvijas Banka ir izstrādājusi kredītiestādēm, maksājumu iestādēm, elektroniskās naudas iestādēm un visu šo subjektu dalībvalstu filiālēm Latvijas Republikā (turpmāk – Iestāde) vadlīnijas finanšu krāpšanas riska (turpmāk – krāpšanas risks) uzraudzībai, pārvaldībai un ierobežošanai. Vadlīnijās sniegtos skaidrojumus katra Iestāde piemēro tiktāl, cik tie atbilst Iestādes darbības specifikai, sniegtajiem pakalpojumiem un piedāvātajiem produktiem, kā arī ievērojot Iestādes darbībai piemītošo risku.

1.2. Vadlīnijas izdotas saskaņā ar Maksājumu pakalpojumu un elektroniskās naudas likuma 48. panta trešo daļu, Kredītiestāžu likuma 50. panta otro daļu, kā arī Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likuma 46. panta pirmās daļas 2. punktu.

1.3. Vadlīnijas sagatavotas atbilstoši spēkā esošajiem normatīvajiem aktiem un labās prakses piemēriem to izstrādes un aktualizēšanas laikā.

1.4. Vadlīnijas izdotas, lai sniegtu skaidrojumus attiecībā uz organizatoriskajām prasībām krāpšanas riska iekšējai pārvaldībai, tā pārvaldības nosacījumiem, sūdzību izskatīšanas procesa efektivitāti un maksājumu rīkojumu noraidīšanas kārtību, tostarp maksājumu apturēšanu, un ieteikumus attiecībā uz prasībām par informācijas pieejamību un apmaiņu starp finanšu krāpšanas apkarošanā iesaistītajām iestādēm. Vadlīnijas ietver principu "ievēro vai paskaidro", ņemot vērā Iestāžu atšķirīgos darbības modeļus un piederību dažādām finanšu institūciju grupām, tostarp pārrobežu finanšu grupām.

1.5. Vadlīniju saturs veidots saskaņā ar krāpšanas riska pārvaldības un ierobežošanas pamatprincipiem. Vadlīnijās ietverti skaidrojumi par veicamo pasākumu tvērumu un apjomu atkarībā no riska, kā arī papildus sniegti skaidrojumi par atsevišķiem krāpšanas riska pārvaldības un ierobežošanas pasākumiem, kuru piemērošanā nepieciešama vienota izpratne par pamatprincipiem.

1.6. Vadlīniju mērķis ir stiprināt krāpšanas riska ierobežošanas principus, kā arī izstrādāt vienotu pieeju krāpšanas riska pārvaldībai, izmantojot uz risku balstītu pieeju. Uz risku balstīta pieeja nozīmē, ka Iestāde krāpšanas risku identificē, novērtē, izprot un piemēro tā pārvaldības pasākumus atbilstoši riskam, kādam tā ir pakļauta, ar mērķi šo risku efektīvi pārvaldīt.

1.7. Vadlīnijas nekalpo kā zaudējumu atlīdzināšanas prasījuma pamats strīdos starp Iestādi un Iestādes klientu. Zaudējumu atlīdzināšanu nosaka ārējie normatīvie akti.

1.8. Krāpšanas riska pārvaldības pasākumus nosaka atbilstoši riska novērtējumam – Iestādes darbībai piemītošajam riskam un krāpšanas gadījumam individuāli piemītošajam riskam. Šis princips ar piemēriem skaidrots attiecīgajās vadlīniju nodaļās. Tomēr, ievērojot, ka katrai Iestādei ir atšķirīgi piedāvātie

produkti un pakalpojumi, tās darbībai piemītošais risks, kā arī krāpšanas gadījumiem piemītošais risks, vienas Iestādes piemērotie pasākumi var atšķirties no citas Iestādes piemērotajiem pasākumiem.

1.9. Vadlīniju saturs tiks pilnveidots un papildināts atbilstoši praksē konstatētajām problēmām un labās prakses piemēriem. Izmantojot piemērus kā skaidrojošu informāciju, tos nevar piemērot visiem gadījumiem vienādi bez izvērtējuma, jo situācijas var būt atšķirīgas. Faktiskie apstākļi, lai arī sākotnēji var šķist līdzīgi apstākļiem, kas minēti piemēros, tomēr var atšķirties, izvērtējot tieši faktisko apstākļu detaļas, kā rezultātā var būt situācija, ka Iestādei nepieciešams izmantot no piemērā minētajiem atšķirīgus vai papildu pasākumus.

2. Organizatoriskās prasības krāpšanas riska iekšējai pārvaldībai

2.1. Spēcīga Iestādes iekšējā pārvaldība un efektīvi iekšējie procesi ir būtiski, lai pasargātu Iestādi un tās klientus no ārējās finanšu krāpšanas. Ieviešot sistēmisku pieeju un vienotu ietvaru krāpšanas riska uzraudzībai, pārvaldībai un ierobežošanai, skaidri definējot iekšējās pārvaldības funkciju veicēju lomas un pienākumus un nosakot vadības atbildību, kā arī ieviešot efektīvus pārraudzības mehānismus, veicinot integrējošu kultūru un izmantojot tehnoloģiju sniegtās iespējas un datu analīzi, Iestāde var efektīvāk mazināt krāpšanas risku un pasargāt savus aktīvus un reputāciju.

2.2. Nosakot ārējos un iekšējos faktorus, kas ir svarīgi Iestādes mērķu sasniegšanai un ietekmē tās spēju veiksmīgi īstenot krāpšanas riska uzraudzību, pārvaldību un ierobežošanu, Iestāde identificē atbilstošās ieinteresētās puses un to prasības attiecībā uz sagaidāmo attīstību un rezultātiem finanšu krāpšanas ierobežošanas un novēršanas procesā. Iestādes vadības atbildība, loma un sagaidāmās riska kultūras demonstrēšana, izmantojot lejupejošo pieeju (*tone from the top*), ir izšķiroša, lai nodrošinātu atbilstošus iekšējās kontroles mehānismus un efektīvus procesus krāpšanas riska identificēšanai, pārvaldībai, uzraudzībai un ziņošanai par to.

2.3. Lai izveidotu un uzturētu efektīvus procesus un kontroles krāpšanas riska novēršanas jomā, Iestāde definē un dokumentē skaidras lomas un pienākumu sadalījumu:
2.3.1. Iestādes vadība ir pilnībā atbildīga par krāpšanas riska izvērtēšanu, tā novēršanas pasākumu īstenošanu, kas ir būtiska kopējās riska pārvaldības sistēmas daļa, pamatotas riska apetītes noteikšanu un atlikušā riska uzņemšanos. Tāpat Iestādes vadības atbildība ir veicināt izpratni un panākt, lai visi iesaistītie darbinieki skaidri izprot Iestādes krāpšanas riska novēršanas kopējo ietvaru un ar to saistītos procesus, kā arī savu lomu un pienākumus šajos procesos;

2.3.2. Iestādes vadība nosaka, kura Iestādes struktūrvienība vai kuri darbinieki ir tieši atbildīgi par krāpšanas riska novēršanas procesu nodrošināšanu.

2.4. Iestāde izstrādā un ievieš krāpšanas riska pārvaldības ietvaru, kura procesu aprakstā iekļauj ciešu sadarbību un regulāru informācijas apmaiņu starp finanšu krāpšanas novēršanas procesā iesaistītajām struktūrvienībām un iekšējās kontroles funkcijām (otro un trešo aizsardzības līniju), kā arī nepieciešamības gadījumā ar ārējiem auditoriem. Iestādes krāpšanas riska pārvaldības ietvars, kas iekļauj politikas, procedūras un riska ierobežošanas un kontroles pasākumus, ir skaidri definēts, dokumentēts un tiek regulāri (ieteicams – reizi gadā) pārskatīts un atjaunināts.

2.5. Lai efektīvi pārvaldītu krāpšanas risku, Iestāde nosaka tās darbinieku kategorijas (grupas), kurām jānodrošina regulāras apmācības krāpšanas riska un tā novēršanas (pārvaldīšanas) jomā. Ņemot vērā darbinieku amata pienākumiem, atbildībai un pilnvarojuma līmenim nepieciešamās zināšanas un kvalifikāciju, Iestāde nodrošina, ka minētie darbinieki:
2.5.1. ir informēti par krāpšanas riska veidiem un to novēršanas metodēm;
2.5.2. pārzina normatīvo regulējumu, kas attiecas uz krāpšanas riska pārvaldību, tostarp attiecīgās nozares specifiskos noteikumus un standartus;
2.5.3. regulāri iegūst specifiskas zināšanas par krāpšanas riska identificēšanu, novērtēšanu un mazināšanu;
2.5.4. attīsta nepieciešamo pieredzi praktiskajā darbā ar krāpšanas riska pārvaldības sistēmām un procedūrām;
2.5.5. veic regulāru kompetences paaugstināšanu, lai nodrošinātu izpratni par jaunākajām tendencēm un labāko praksi krāpšanas riska pārvaldībā;
2.5.6. piedalās apmācībās, kas palīdz uzlabot izpratni un prasmes saistībā ar krāpšanas riska pārvaldību.

2.6. Iestādes vienojas un uztur drošu un uzticamu informācijas apmaiņas sistēmu, kurā īsteno tādas informācijas savstarpēju apmaiņu, kas saistīta ar finanšu krāpšanu, lai uzlabotu darījumu uzraudzības iespējas. Aktuālās informācijas apmaiņu nodrošina nekavējoties (reāllaikā). Iestādes, apmainoties ar datiem, kas saistīti ar finanšu krāpšanu, neaprobežojas tikai ar maksājuma saņēmēja unikālajiem identifikatoriem vai starptautisko bankas konta numuru (IBAN), bet iespēju robežās iekļauj arī citus datus. Informācijas apmaiņai jābūt orientētai uz valsts (iekšzemes) līmeni, taču tas neliedz Iestādēm brīvprātīgi veikt datu apmaiņu starp valstīm pārrobežu kontekstā, ja tas ir nepieciešams un atbilst normatīvo aktu prasībām.

2.7. Iestāde nosaka kārtību un atbildīgās personas, lai nekavējoties ziņotu informācijas tehnoloģiju drošības incidentu novēršanas institūcijai CERT.LV par krāpšanas incidentu digitālajā vidē, t. sk. sniedz Iestādes rīcībā esošo informāciju par attiecīgajā krāpšanas gadījumā izmantoto domēna vārdu vai tīmekļvietni. Pamatojoties uz informācijas aktualitāti, Iestāde izvērtē nepieciešamību ziņot nekavējoties.

2.8. Lai nodrošinātu efektīvu krāpšanas riska pārvaldību, Iestāde definē, dokumentē un regulāri (vismaz reizi gadā) pārskata krāpšanas riska pārvaldības stratēģiju, riska tolerances līmeni un riska līmeņa kvantitatīvos vai kvalitatīvos rādītājus. Lai identificētu potenciālo risku vai riska līmeņa izmaiņas, Iestāde nosaka un regulāri pārbauda galvenos riska rādītājus (*key risk indicators*; KRI). Krāpšanas riska pārvaldības procesa efektivitātes noteikšanai Iestāde nosaka un regulāri pārbauda procesa snieguma rādītājus (*key performance indicators*; KPI). Visus rādītājus regulāri (vismaz reizi gadā) pārskata. Kalibrējot rādītājus un nosakot to būtiskuma sliekšņus, Iestāde nodrošina iespēju identificēt nepieciešamību veikt papildu pasākumus darbības procesa izmaiņu vai uzlabojumu ieviešanai. Iestāde izveido procesu pienācīgai rādītāju pārraudzībai, kontrolei (monitoringam), informācijas nodošanai un izvērtēšanai vadības augstākajā līmenī.

2.9. Pamatojoties uz finanšu krāpšanas atklāšanas un novēršanas jomā ieviestajiem riska pārvaldības snieguma rādītājiem, Iestādes vadība regulāri (ne retāk kā reizi gadā) pārskata un izvērtē finanšu krāpšanas novēršanai nepieciešamā personāla un tehnisko resursu pietiekamību, kā arī plāno un nodrošina tam nepieciešamo finansējumu, tostarp, ņemot vērā riska pārvaldības snieguma rādītājus.

2.10. Iestāde regulāri (vismaz reizi gadā) veic pašnovērtējumu par finanšu krāpšanas atklāšanas un novēršanas procesa efektivitāti, ņemot vērā iekšējos un ārējos faktorus, kas var ietekmēt krāpšanas gadījumu statistikas rādītājus, t. sk. finanšu krāpšanas statistiku, kas apkopota atbilstoši Latvijas Bankas 2022. gada 13. jūnija noteikumu Nr. 208 "Statistisko datu par klientu maksājumiem sagatavošanas un iesniegšanas noteikumi" prasībām, novērtējot arī personāla un informācijas tehnoloģiju resursu pietiekamību un to, cik efektīvi krāpšanas riska pārvaldība atbilst organizatoriskajām prasībām, riska pārvaldības procedūrām un krāpšanas novēršanas mērķiem. Iestādes iekšējās pārvaldības vai darbības atbilstības uzraudzības funkcija un vadības struktūras (augstākā vadība) tiek informētas par pašnovērtējuma rezultātiem un identificēto trūkumu novēršanas pasākumiem.

2.11. Iestādes augstākā vadība periodiski pārskata izvēlēto pieeju krāpšanas riska uzraudzībai, pārvaldībai un ierobežošanai un tās ietvaru, lai nodrošinātu tā pastāvīgu piemērotību, efektivitāti un atbilstību Iestādes stratēģiskajai virzībai. Iestādes vadība ņem vērā vismaz:
2.11.1. izmaiņas ārējos un iekšējos aspektos, kas ietekmē Iestādes spēju sasniegt krāpšanas riska uzraudzībā, pārvaldībā un ierobežošanā plānotos rezultātus;
2.11.2. informāciju par krāpšanas riska uzraudzības, pārvaldības un ierobežošanas procesa sniegumu;
2.11.3. ziņojumu rezultātus no iepriekšējiem vadības pārskatiem (*management review*) krāpšanas riska jomā;
2.11.4. iekšējā un ārējā audita un atbilstības pārbaužu rezultātus, tostarp informācijas tehnoloģiju pārvaldības un drošības jomā;

2.11.5. tendences, kas izriet no finanšu krāpšanas ierobežošanas un novēršanas rezultātiem, resursu pietiekamības, monitoringa un mērījumu rezultātiem, darbības efektivitātes riska mazināšanai ieviestajām kontrolēm, kā arī jaunām krāpnieku darbības metodēm, shēmām u. tml.

2.12. Vadības pārskatos norādītie rezultāti ietver lēmumus un darbības, kas nosaka:
2.12.1. norādījumus par jebkādām veicamajām izmaiņām kontekstā ar izvēlēto pieeju krāpšanas riska uzraudzībai, pārvaldībai un ierobežošanai un tās ietvaru;
2.12.2. procesu un tehnoloģisko risinājumu uzlabošanas un pilnveides iespējas;
2.12.3. vajadzības attiecībā uz resursiem.

2.13. Ņemot vērā, ka pieaug pastāvošie un rodas arvien jauni krāpšanas draudi, ko veicina arī mākslīgā intelekta izmantošana ļaunprātīgos nolūkos, un finanšu krāpnieki izstrādā jaunas krāpšanas shēmas, Iestāde īsteno atbilstošus tehnoloģiskos un organizatoriskos pasākumus, lai spētu palielināt maksājumu darījumu uzraudzības procesa efektivitāti un novērsto finanšu krāpšanas gadījumu īpatsvaru, īpaši veicinot iespējamās finanšu krāpšanas savlaicīgu atklāšanu, piemēram, situācijās, kad klients vēl nav paspējis konstatēt savu autentifikācijas datu nonākšanu krāpnieku rokās vai identitātes datu vai maksājumu instrumentu zādzību. Tāpēc maksājumu darījumu uzraudzības kontekstā Iestāde nosaka atbilstošas riska aplēses par maksājumu darījumiem vai izmanto līdzvērtīgus alternatīvus risinājumus maksājumu darījumu grupēšanai konkrētos riska līmeņos un izvēlas katram līmenim atbilstošas kontroles procedūras un riska mazināšanas pasākumus, piemēram, sākot no stingrās klienta autentifikācijas (*strong customer authentication*; SCA) izmantošanas maksājumu darījumu apstiprināšanai vai maksājuma veikšanas tikai pēc klienta personīgi sniegta apstiprinājuma saņemšanas līdz pat darījuma apturēšanai vai atteikšanai.

2.14. Iestāde iespēju robežās izmanto tādus tehnoloģiskos risinājumus finanšu krāpšanas ierobežošanai un novēršanai, kas ne tikai pamato ieguldītos līdzekļus un resursus, bet arī nodrošina ieinteresēto pušu prasību izpildi attiecībā uz sagaidāmajiem rezultātiem, piemēram, klientu uzticību Iestādei un Latvijas Bankas gaidām finanšu tirgus drošības jomā. Šajā nolūkā Iestāde identificē iespējamās darbības, kuru efektivitāti būtu iespējams izmērīt un uzraudzīt tehnoloģiskā risinājuma darbības kontekstā, paredzot, ka veiktos mērījumus ir iespējams atkārtot, savukārt to rezultātus salīdzināt un pārbaudīt.

2.15. Iestādes risku kontroles funkcija regulāri veic padziļinātu, neatkarīgu un visaptverošu krāpšanas riska mērīšanu, novērtēšanu un uzraudzību, kā arī krāpšanas riska novēršanas procesu vai pasākumu efektivitātes analīzi un par rezultātiem ziņo Iestādes vadībai.

2.16. Iestāde nosaka prasības sistemātiskai un regulārai uz risku balstītai (pamatotai) iekšējā audita iesaistei finanšu krāpšanas atklāšanas un novēršanas procesa uzraudzībā:
2.16.1. paredz obligātu finanšu krāpšanas jomas iekļaušanu iekšējā audita darba plānos, ņemot vērā krāpšanas riska uzraudzības un pārskatīšanas rezultātus,

ziņojumu rezultātus par krāpšanas riska uzraudzības, pārvaldības un ierobežošanas procesu sniegumu, plānotās izmaiņas regulējumā un Iestādes procesos, kā arī iepriekšējo auditu rezultātus;
2.16.2. nosaka katra veicamā audita kritērijus un apjomu un piesaista auditorus ar atbilstošu kompetenci plānoto auditu īstenošanai;
2.16.3. nodrošina audita rezultātu iesniegšanu Iestādes vadībai un savlaicīgu korektīvo pasākumu noteikšanu un to ieviešanas uzraudzību krāpšanas riska jomā.

3. Krāpšanas riska pārvaldība

3.1. Lai nodrošinātu, ka tiek sasniegti mērķi un sagaidāmie rezultāti un novērsta vai mazināta identificēto risku nevēlamā ietekme, Iestāde ņem vērā šo vadlīniju 2. nodaļā noteiktās prasības un vismaz reizi gadā, izmantojot savu izvēlēto metodoloģiju krāpšanas riska novērtējuma veikšanai, veic aktuālā krāpšanas riska novērtēšanu. Šai metodoloģijai jāietver prasības dokumentēta krāpšanas riska novērtējuma veikšanai un riska novērtējuma sagatavošanai (skaidrojums par novērtējuma mērķi, tvērumu un veikšanas kārtību), kā arī jāparedz kārtība, kā krāpšanas riska novērtējuma rezultāti tiek nodoti izskatīšanai vadības augstākajā līmenī.
3.2. Krāpšanas riska novērtējumu Iestāde veic sistemātiski, iteratīvi, sadarbojoties ar jomas ekspertiem un pamatojoties uz viņu zināšanām un viedokli, izmantojot atbilstošāko pieejamo informāciju un nodrošinot, ka:
3.2.1. veiktais krāpšanas riska novērtējums tiek dokumentēts un iegūtie rezultāti ir ticami un savstarpēji salīdzināmi;
3.2.2. visi aktuālie riski tiek identificēti un aprakstīti, pamatojoties uz ticamu informāciju un argumentāciju, ka minētie riski varētu ierobežot Iestādes iespējas vai neļaut tai sasniegt noteiktos mērķus krāpšanas riska uzraudzībā, pārvaldībā un ierobežošanā. Jāņem vērā, ka identificēto risku izcelsmes avoti var nebūt Iestādes pārraudzības jomā;
3.2.3. identificētā krāpšanas riska analīze tiek veikta, izmantojot kvalitatīvās vai kvantitatīvās metodes vai šo metožu kombinācijas, lai veicinātu, ka iegūtie rezultāti sniedz priekšstatu par lēmumiem, kas pamato izdarītās izvēles, kuras izriet no attiecīgo risku līmeņiem. Krāpšanas riska novērtējumā iekļauj informāciju par krāpšanas riska vispārējo līmeni, tā izmaiņām un galvenajiem faktoriem, kas to ietekmē, tostarp informāciju par konstatētajām jaunajām krāpšanas tipoloģijām, kā arī par Iestādes spēju efektīvi pārvaldīt no jauna identificētos riska veidus un izmaiņas riska līmenī. Iestāde regulāri seko līdzi statistikas datiem, kas ir pieejami saskaņā ar Eiropas Banku iestādes vadlīnijām attiecībā uz ziņošanu par krāpšanu saskaņā ar Direktīvu (ES) 2015/2366 (PSD2), novērtējot Iestādes kopējo krāpšanas riska līmeni attiecībā uz galvenajiem maksājumu instrumentiem pret maksimāli pieļaujamo līmeni, kas ir noteikts Eiropas Savienībā;

3.2.4. iegūtais krāpšanas riska novērtējums obligāti ietver riska analīzes rezultātu salīdzināšanu ar noteiktajiem riska akceptēšanas kritērijiem, lai konstatētu situācijas, kurās nepieciešamas vēl kādas papildu darbības attiecībā uz atlikušo risku, ņemot vērā plašāku kontekstu un faktiskās sekas attiecībā uz Iestādes krāpšanas riska pārvaldībā ieinteresētajām pusēm;
3.2.5. krāpšanas riska novērtējuma rezultāti tiek reģistrēti un paziņoti Iestādes vadībai.

3.3. Balstoties uz krāpšanas riska novērtējuma rezultātiem, kā arī ņemot vērā finanšu krāpšanas atklāšanas un novēršanas procesa efektivitātes novērtējuma (pašnovērtējuma) rezultātus, Iestāde nosaka vai atjaunina krāpšanas ierobežošanas mērķus un plānotās aktivitātes to sasniegšanai, nosakot to, cik bieži jāseko līdzi to izpildes statusam, un par šo darbību izpildi atbildīgās personas:
3.3.1. iestāde izstrādā krāpšanas riska pārvaldības plānu, lai nodrošinātu, ka izvēlētās pārvaldības iespējas tiks īstenotas, lai krāpšanas riska pārvaldībā iesaistītās puses saprastu noteiktos pasākumus un varētu sekot līdzi šā plāna īstenošanai;
3.3.2. krāpšanas riska pārvaldības plānā skaidri norāda kārtību, kādā tiek īstenota riska pārvaldība un kādā tā tiek integrēta Iestādes pārvaldības plānos un procesos, vienojoties ar attiecīgajām ieinteresētajām pusēm.

3.4. Saskaņā ar labo praksi krāpšanas riska pārvaldībā Iestādei ieteicams ieviest atbilstošākās izvēles iespējas, plānojot potenciālo ieguvumu līdzsvarošanu ar krāpšanas ierobežošanas mērķu sasniegšanu un īstenošanas izmaksām, tostarp pūlēm, kas ieguldītas tādu nepilnību novēršanā, kuras nav iespējams pilnībā novērst. Šīs iespējas ne vienmēr ir savstarpēji izslēdzošas vai piemērotas visos apstākļos. Tāpēc Iestādes vadībai un citām ieinteresētajām pusēm jāapzinās atlikušā riska veids un tā apjoms pēc riska novērtēšanas un atlikušais risks ir jādokumentē un jāpakļauj uzraudzībai, pārskatīšanai un, ja nepieciešams, turpmākai novērtēšanai. Savukārt, ja riska pārvaldības iespējas nav pieejamas vai ja tās pietiekami nemaina riska lielumu, tad attiecīgais risks jāreģistrē un tā lielums pastāvīgi jāpārskata.

3.5. Iestāde ņem vērā, ka pat rūpīgi izstrādāta un īstenota riska pārvaldība var nedot gaidītos rezultātus un radīt neparedzētas sekas, tāpēc ir nepieciešama pastāvīga reģistrēto risku uzraudzība un pārskatīšana, lai savlaicīgi konstatētu, ka esošie riska pārvaldības pasākumi ir kļuvuši neefektīvi. Turklāt arī šie plānotie riska pārvaldības pasākumi var radīt jaunus riskus, kas arī ir attiecīgi jāpārvalda. Tāpēc pastāvīgai riska pārvaldības procesa un tā rezultātu uzraudzībai un periodiskai pārskatīšanai jābūt plānotai riska pārvaldības procesa daļai, skaidri definējot atbildību un visos procesa posmos, t. sk. plānošanā, informācijas vākšanu un analīzi, rezultātu reģistrēšanu un atgriezeniskās saites sniegšanu.

3.6. Iestāde nodrošina, ka finanšu krāpšanas novēršanas jomā ieviesto procesu un kontroļu darbības efektivitāte tiek sistemātiski novērtēta un iegūtie novērtējuma rezultāti tiek dokumentēti un saglabāti. Iestāde analizē un novērtē atbilstošus

datus un informāciju, kas izriet no monitoringa un mērījumu rezultātiem. Šajā nolūkā Iestāde nosaka:
3.6.1. izmērāmus parametrus, kas tiks periodiski uzraudzīti un mērīti, un krāpšanas monitoringa, mērīšanas, analīzes un novērtēšanas metodes, kas nodrošina derīgu rezultātu iegūšanu;
3.6.2. periodu krāpšanas monitoringa un mērījumu veikšanai un iegūto krāpšanas monitoringa un mērījumu rezultātu analīzei un novērtēšanai;
3.6.3. atbildīgos par krāpšanas monitoringa novērtējuma veikšanu un dokumentācijas uzturēšanu.

3.7. Iestāde izmanto krāpšanas monitoringa analīzes rezultātus, lai novērtētu:
3.7.1. izvēlētās pieejas un ietvara krāpšanas riska uzraudzībai, pārvaldībai un ierobežošanai plānošanas efektivitāti, t. sk. cilvēku un tehnisko resursu pietiekamību;
3.7.2. finanšu krāpšanas novēršanas procesu un kontroļu darbības efektivitāti;
3.7.3. to darbību efektivitāti, kas tiek veiktas, lai novērstu krāpšanas risku;
3.7.4. nepieciešamību pēc uzlabojumiem krāpšanas riska uzraudzībā, pārvaldībā un ierobežošanā.

3.8. Iestāde finanšu krāpšanas novēršanā izmanto iespējami atbilstošākos un mūsdienīgākos tehnoloģiskos risinājumus, kas spēj nodrošināt:
3.8.1. līdztekus jau zināmajiem krāpšanas novēršanas scenārijiem iespējas operatīvi pievienot jaunus identificētos krāpšanas novēršanas scenārijus, kā arī iespējas iekļaut papildu uzraudzības scenārijos maksājumu darījumu rādītājus;
3.8.2. vēsturisko lietojuma datu izmantošanu, lai identificētu klientam neraksturīgu uzvedību, veicot darbības internetbankā vai mobilajā lietotnē;
3.8.3. mijiedarbību starp dažādiem krāpšanas riska līmeņiem un uz risku balstītiem faktoriem (piemēram, mobilās lietotnes uzstādīšana citā ierīcē, norēķinu kartes digitalizācija u. tml.) un iespējas grupēt darījumus pēc attiecīgā riska līmeņa, īstenojot krāpšanas riska uzraudzību, pārvaldību un ierobežošanu.

3.9. Iestāde nodrošina, ka maksājumu darījumu uzraudzības procesā, konstatējot jaunu maksājumu instrumentu reģistrāciju, piemēram, maksājumu kartes pievienošanu viedierīces digitālajam makam, un lietojumu, kā arī augsta un paaugstināta riska gadījumus, ņemot vērā pieejamos datus, tiek ņemta vērā mijiedarbība starp dažādiem riska līmeņiem un uz risku balstītiem faktoriem. Ja piemērojams un tehniski izpildāms, šos principus piemēro arī e-komercijā veiktajiem darījumiem, tostarp ar tirgotājiem ārpus Eiropas Savienības. Maksājumu darījumu uzraudzības procesā kopumā un īpaši šādos gadījumos, pamatojoties uz maksājuma izpildes specifiku, pēc noklusējuma būtu jānodrošina stingrās klienta autentifikācijas lietojums, ņemot vērā noteiktus faktorus, piemēram:
3.9.1. veicot autentificēšanos internetbankā, tiek izmantota ierīce, par kuras tehnoloģiskajiem parametriem un iepriekšējo lietojumu Iestādei nav informācijas. Šādos gadījumos kombinācijā ar citiem risku paaugstinošiem faktoriem Iestādei ieteicams piemērot paaugstinātu riska līmeni notiekošajiem darījumiem, t. sk. pirkumiem e-komercijas ietvaros, tostarp maksājumiem starp

klienta kontiem, īpaši, ja notiek naudas līdzekļu pārskaitīšana uz debetkartei vai kredītkartei piesaistītu kontu un tai sekojoši e-komercijas darījumi;
3.9.2. tiek konstatēta jauna maksājuma instrumenta, tāda kā mobilā lietotne, iestatīšana vai klienta maksājumu karte tiek pievienota digitālajam makam iestādē iepriekš neidentificētā klienta ierīcē. Šādos gadījumos Iestādei ieteicams paredzēt un īstenot procedūru klienta jaunās ierīces reģistrācijai, piemēram, nosūtot brīdinājumu uz klienta iepriekš reģistrēto ierīci, lai nodrošinātu papildu ierīces apstiprināšanu darbam ar lietotni vai piekrišanu klienta kartes digitalizēšanai tikai pēc apstiprinājuma saņemšanas no klienta esošās ierīces, vai piemērojot citus līdzvērtīgus risinājumus, kas nepārprotami informē klientu par jaunas ierīces reģistrēšanu;
3.9.3. tiek konstatēta tādu maksājumu darījumu īstenošana, kas rada aizdomas par iespējami notiekošu krāpšanu, piemēram, netipiski liels maksājumu rīkojumu skaits ar kredīta vai debeta līdzekļiem attiecīgajā maksājumu kontā, īpaši gadījumos, kad iesniegto maksājumu rīkojumu kopējā vērtība ir līdzvērtīga konta atlikumam, ja maksājumu rīkojumi tiek iniciēti klientam neierastā laikā vai ar klientam neraksturīgi lielām summām, kad tiek konstatēta naudas līdzekļu ātra izņemšana, tostarp ārvalstu valūtā un kriptoaktīvu iegādei, maksājuma rīkojumā tiek identificētas tādas detaļas un maksājuma īstenošanas pazīmes kā klientam neraksturīga valoda, nesamērīgi ātrs teksta ievades ātrums, kas ir pazīme par šādu rīkojumu ģenerēšanu ar automatizētiem tehnoloģiskiem rīkiem, u. tml.;
3.9.4. maksājumu rīkojumi tiek sagatavoti no klientam neraksturīgas ģeogrāfiskās atrašanās vietas, tostarp īsā laika periodā Iestādē tiek saņemti maksājumu rīkojumi no tādām ģeogrāfiskās atrašanās vietām, kas atrodas fiziski tālu cita no citas;
3.9.5. tiek konstatēta tādu informācijas tehnoloģiju rīku un IP adrešu, kā arī tehnoloģisko līdzekļu izmantošana, kuri jau ir tikuši izmantoti iepriekšējos pārkāpumos un par kuriem informācija ir pašas Iestādes vai citu uzticamu informācijas avotu rīcībā;
3.9.6. pieejama detalizēta informācija par iepriekš konstatētajiem krāpšanas gadījumiem, piemēram, krāpšanā izmantotiem maksājumu kontiem un to parametriem vai krāpšanas gadījumos un shēmās iesaistītajām pusēm, kura ir pašas Iestādes vai citu uzticamu informācijas avotu rīcībā;
3.9.7. tiek konstatētas anomālijas attiecībā uz piekļuvei izmantoto ierīču tīkla parametriem, vienlaicīgs maksājumu instrumentu lietojums no dažādām IP adresēm, kā arī dažādu apakštīklu IP adrešu izmantošana īsā laika posmā, tostarp virtuālā privātā tīkla (*virtual private network*; VPN) un starpniekserveru izmantošanas pazīmes u. tml.;
3.9.8. tiek identificētas ļaunprogrammatūras klātbūtnes pazīmes jebkurā klienta autentifikācijas procedūras posmā;
3.9.9. tiek veikti darījumi starp maksātāju un tādu maksājuma saņēmēju, kas varētu tikt uzskatīts par uzticamu, taču darījuma veikšanas brīdī informācija par to neatrodas Iestādes uzticamo darījumu partneru sarakstā;
3.9.10. gadījumi, kad notiek ziņošana par aizdomām par krāpšanu u. c.

3.10. Iestāde darījumu uzraudzības ietvaros iespēju robežās, ņemot vērā Iestādes tehnoloģisko risinājumu iespējas, nodrošina arī ienākošo maksājumu monitoringu attiecībā uz nestandarta ienākošajiem maksājumiem, piemēram, ātro kredītu izmantošanu, maksājumiem ar neatbilstošiem rekvizītiem un mēģinājumiem naudas līdzekļus pārskaitīt tālāk.

4. Sūdzību izskatīšanas procesa efektivitāte

4.1. Iestāde finanšu krāpšanas sūdzību izskatīšanas kārtību nosaka un sūdzību izskatīšanu organizē saskaņā ar Latvijas Bankas 2024. gada 2. decembra noteikumiem Nr. 358 "Finanšu tirgus dalībnieku saņemto sūdzību pārvaldības kārtība".

4.2. Saņemot informāciju par finanšu krāpšanas gadījumu, kurā klients apstrīd veikto darījumu (t. sk. situācijā, kad informācija ir saņemta ar zvanu centra starpniecību), Iestāde veic situācijas analīzi:
4.2.1. Iestāde stingri uzrauga un analizē visas sūdzības, ko tā saņem par iespējamu finanšu krāpšanu, tostarp gadījumos, kad ir aizdomas par krāpšanu;
4.2.2. Iestāde veic saņemto sūdzību analīzi, kas var palīdzēt tai izstrādāt potenciālo krāpnieku profilus, to darbībai raksturīgās tipoloģijas un šādu darbību identificēšanas kritērijus, kas uzlabos uzraudzības procesu;
4.2.3. lai palielinātu ieviesto krāpšanas novēršanas pasākumu efektivitāti, Iestāde pastāvīgi uzrauga saņemto sūdzību statistisku, salīdzinot to ar kopējo pieejamo klientu bāzi, kā arī pieejamo informāciju par sūdzību, kas iesniegtas saistībā ar pārrobežu maksājumiem, apjomu un seko līdzi riska līmeņa izmaiņām, balstoties uz katrai pozīcijai noteiktajiem galvenajiem riska indikatoriem.

4.3. Izskatot informāciju par finanšu krāpšanu, kurā klients apstrīd veikto darījumu, Iestāde:
4.3.1. lai pilnībā izvērtētu krāpšanas apstākļus, rūpīgi izvērtē tai pieejamo informāciju un nepieciešamības gadījumā pieprasa klientam papildu informāciju;
4.3.2. noskaidro veiktās krāpšanas apstākļus un klienta rīcību.

4.4. Sniedzot atbildes uz sūdzībām par finanšu krāpšanu, Iestāde papildus vispārējai atbilžu uz sūdzībām sagatavošanas kārtībai ievēro šādus principus:
4.4.1. atbilde tiek sniegta detalizēti par konkrētā klienta gadījumu;
4.4.2. atbilde tiek sniegta, nepieļaujot pārrakstīšanās kļūdas notikumu gaitas aprakstā;
4.4.3. nav pieļaujama vispārīga atbilde ar standarta frāzēm, t. sk. tikai līguma punktu citēšana bez skaidrojuma, kā tieši ir notikusi krāpšana un kur klients pieļāvis rupju neuzmanību, ko tas būtu varējis nepieļaut;
4.4.4. kompensācijas (zaudējumu segšanas) atteikuma gadījumā tiek sniegts atteikuma pamatojums. Ja atteikuma pamatojums ir klienta rupja neuzmanība, Iestāde sniedz detalizētu rupjas neuzmanības apstākļu izvērtējumu;

4.4.5. atbilde tiek sniegta vienkāršā un saprotamā valodā (iespējami īsiem, konkrētiem teikumiem).

4.5. Pēc uzraudzības iestādes pieprasījuma sniedzot paskaidrojumu saistībā ar sūdzību par finanšu krāpšanu, Iestāde sniedz:
4.5.1. skaidrojumu par tās veiktajām darbībām saistībā ar sūdzībā norādīto, t. sk. par līdzekļu atgūšanu;
4.5.2. detalizētu krāpšanas gadījuma tehnisko informāciju;
4.5.3. pierādījumus un secinājumus par klienta maksājuma autorizāciju;
4.5.4. ja attiecināms uz konkrētās sūdzības faktiskajiem apstākļiem – izvērtējumu par to, vai maksājums veikts, klientam rīkojoties prettiesiski ar ļaunu nolūku vai rupjas neuzmanības dēļ;
4.5.5. ja attiecināms uz konkrētās sūdzības faktiskajiem apstākļiem – situācijā, kad klients konkrētajā gadījumā iesaistīts kā naudas mūlis, klienta izpētes lietu, kas ietver informāciju un to pamatojošo dokumentāciju par klienta identifikāciju, klienta sākotnējo izpēti, riska līmeni (tā izmaiņām), klienta kārtējo izpēti un darījumu uzraudzību.

5. Maksājumu rīkojumu noraidīšana (maksājumu apturēšana un atsaukšana)

5.1. Papildus vispārējai darījumu uzraudzības kārtībai Iestāde darījumu uzraudzībā un noraidīšanā ievēro šādus nosacījumus:
5.1.1. ja Iestāde pirms darījuma veikšanas konstatē, ka maksājumam vai zibmaksājumam ir augsts risks, tā atsaka pieņemt izpildei šādu maksājumu un paziņo par to klientam, tostarp norāda vispārīgu atteikuma iemeslu;
5.1.2. Iestāde, ņemot vērā klientu grupas paradumus un riska profilu, tostarp šo vadlīniju 3.9. punktā minētos riska faktorus, nosaka dažādus sākotnējos limitus, uzsākot maksājumu pakalpojumu nodrošināšanu klientam, regulāri pārskata piemērotos limitus, koriģējot tos sadarbības laikā, kā arī piedāvā klientam iespēju noteikt tam piemērotu limitu zem vai virs tās noteiktajām noklusējuma vērtībām, paredzot limita maiņas iespēju tikai pēc individuālas saziņas ar Iestādes darbinieku, izņemot gadījumus, kad maksājumu limits tiek palielināts līdz Iestādes noteiktajam apmēram un tādēļ saziņa ar Iestādes darbinieku nav obligāta vai maksājumu limits tiek palielināts nebūtiskā apmērā. Gadījumos, kad maksājumu limita palielināšanā netiek iesaistīts Iestādes darbinieks, Iestāde nodrošina, ka maksājumu limita palielināšanā tiek veikta stingrā klienta autentifikācija;
5.1.3. Iestāde darījumu uzraudzību piemēro visiem elektronisko maksājumu kanāliem, kuros tās klients izmanto konkrētu maksājuma instrumentu, piemēram, bankomātiem, ļaujot integrēti uzraudzīt darījumus, kas apstrādāti saistībā ar šo maksājuma instrumentu;
5.1.4. izsniedzot klientam jaunu maksājumu karti, Iestāde noskaidro, vai klientam ir nepieciešamība izmantot karti maksājumiem ārpus valsts robežām un e-

komercijā, izvairoties no situācijām, kurās no jauna izsniegtas maksājumu kartes pēc noklusējuma tiek konfigurētas šāda veida maksājumiem bez klienta vajadzību noskaidrošanas, ņemot vērā Iestādes tehnoloģisko risinājumu iespējas.

5.2. Maksājuma uzdevuma atsaukšana pēc tā izpildes:
5.2.1. ja pēc maksājuma izpildes Iestādei rodas pamatotas aizdomas par finanšu krāpšanas gadījumu, Iestāde sazinās ar klientu, lai saņemtu klienta piekrišanu informēt maksājuma saņēmēju iestādi par iespējamo krāpšanas gadījumu un par maksājuma atsaukumu. Vienlaikus Iestāde informē klientu par veiktajām darbībām, to termiņiem un iespējamām sekām maksājuma atsaukuma vai tā neiespējamības gadījumā. Iestāde neveic saziņu ar klientu gadījumos, kad Iestādei ir pamatotas aizdomas, ka klienta maksājumu konts tiek izmantots izkrāptu finanšu līdzekļu pārvietošanai, tostarp gadījumos, kad klients varētu būt naudas mūlis;
5.2.2. ja maksājums, kas atzīts par finanšu krāpšanas gadījumu, veikts, izmantojot maksājuma instrumentu (maksājumu karti, digitālo maku, kam piesaistīta karte), Iestāde sazinās ar klientu par iespējamo krāpšanas gadījumu un informē to par maksājuma atsaukuma procedūru un rezervētā maksājuma statusu.

5.3. Iestāde nodrošina, ka klientiem ir ērti pieejama vienkāršā valodā sniegta informācija par maksājumu kartes darījuma rezervācijas statusa nozīmi un šī informācija ir saprotama personām, kurām nav speciālu zināšanu tieslietās vai finanšu pakalpojumu jomā.

6. Maksājumu autorizācijas un rupjas neuzmanības izvērtēšana

6.1. Iestāde izstrādā iekšējo kārtību, kādā tiek pieņemts lēmums par klientam finanšu krāpšanas gadījumā radušos zaudējumu segšanu. Lēmums par zaudējumu kompensāciju ir pamatots ar izvērtējumu par konkrētā klienta rīcību krāpnieciskajā darījumā, t. sk. par tā rīcību attiecībā uz darījuma autorizāciju un iespējām krāpšanu identificēt pirms darījuma veikšanas.

6.2. Izvērtējot klienta iesniegumu par zaudējumu, kas radušies finanšu krāpšanas rezultātā, kompensēšanu, Iestāde savā izvērtējumā (lēmumā) neaprobežojas tikai ar vispārīga skaidrojuma, ka darījums ir bijis autorizēts, tostarp, izmantojot stingro klienta autentifikāciju, sniegšanu. Iestāde savā izvērtējumā (lēmumā) norāda arī:
6.2.1. darījuma faktiskos apstākļus, tostarp darījuma veidu (kartes darījums, kredītpārvedums) un Iestādei zināmo informāciju par darījumā iesaistītajām pusēm;
6.2.2. informāciju par darījumā izmantotajām autentifikācijām (personas identitātes noskaidrošanai) un autorizācijām (darījuma veikšanas apstiprināšanai), tostarp stingro klienta autentifikāciju un autentifikācijas un autorizācijas veikšanā izmantotajām ierīcēm;

6.2.3. to Iestādei pašai zināmo vai no klienta iesnieguma izrietošo apstākļu vispārīgu skaidrojumu, kuru dēļ konstatējama klienta rupja neuzmanība, tostarp standartlīgumos noteikto pienākumu neizpilde, kā rezultātā ir noticis krāpšanas gadījums;
6.2.4. ja attiecināms uz konkrētās lietas apstākļiem, proti, klients noliedz, ka viņš būtu autorizējis darījumu ar stingro klienta autentifikāciju, – faktisko apstākļu skaidrojumu, t. sk. klienta veiktās darbības, kas ļāvušas trešajām pusēm iegūt pieeju klienta autentifikācijas vai autorizācijas rīkiem vai uzstādīt internetbankas lietotni trešo pušu ierīcēs un liecina par rupju neuzmanību, tostarp standartlīgumos noteikto pienākumu neizpildi, kā rezultātā ir noticis krāpšanas gadījums.

6.3. Izvērtējot klienta rīcību saistībā ar darījuma autorizāciju, Iestāde vērtē, vai klienta rīcībā ir konstatējamas rupjas neuzmanības pazīmes, piemēram:
6.3.1. klients veic stingro autentifikāciju, neiepazīstoties ar veicamo darbību (PIN1 gadījumā atļauja pievienoties internetbankai; PIN2 gadījumā atļauja veikt maksājumu), – ar nosacījumu, ka pirms PIN2 ievades Iestāde nodrošina, ka tiek sniegta nepārprotama informācija par maksājuma veikšanu konkrētam saņēmējam noteiktas summas apmērā;
6.3.2. klients nav ņēmis vērā Iestādes sniegto informāciju, kas adresēta klientam un sniegta pa individuāliem kanāliem, par konkrētām aktualitātēm krāpšanas jomā;
6.3.3. klients nodrošina vieglu pieeju maksājumu kartes PIN kodam, glabājot to līdzās maksājumu kartei vai uzrakstot to uz maksājumu kartes;
6.3.4. klients nav informējis Iestādi par citiem jau notikušiem aizdomīgiem darījumiem ar konkrēto maksājuma instrumentu vai kontu;
6.3.5. klients atkārtoti kļūst par krāpšanas upuri identiskā vai līdzīgā finanšu krāpšanas gadījumā;
6.3.6. klients saziņā ar trešajām pusēm nodod tām informāciju par maksājumu instrumentiem, pašus maksājumu instrumentus vai informāciju, kas ļauj trešajām pusēm pārņemt klienta digitālo identitāti vai piekļuvi internetbankai, tostarp internetbankas lietotnes uzstādīšanai trešo pušu viedierīcēs.

7. Prasības attiecībā uz informācijas pieejamību

7.1. Iestāde nodrošina, ka klientam ir viegli pieejama detalizēta informācija par sūdzību izskatīšanas procesu, darījumu apstrīdēšanas kārtību, kā arī par klienta rīcību, ja tam ir aizdomas par krāpnieciskām darbībām, norādot šiem procesiem paredzētos saziņas kanālus un procesa gaitu, skaidri aprakstot to, kāda informācija klientam ir jāsniedz attiecīgajā gadījumā, un iespējamos procesa rezultātus, kā arī norādot uz tālākajām darbībām, ja klienta sūdzību vai pieteikumu nav iespējams atrisināt. Iestāde mudina klientus nekavējoties ziņot

par pamanītajām aizdomīgām darbībām, t. sk. neautorizētajiem darījumiem, negaidītām izmaiņām kontā vai pikšķerēšanas mēģinājumiem.

7.2. Iestāde veic šādus finanšu pratības veicināšanas pasākumus:
7.2.1. izmantojot savus informācijas izplatīšanas rīkus (tīmekļvietnes, sociālos medijus u. c.) vai novirzot uz citiem publiski pieejamiem un uzticamiem informācijas avotiem, Iestāde aktīvi informē klientus par dažādām konstatētajām krāpšanas metodēm, neuzticamu vai nepatiesu tīmekļvietņu adresēm un pazīmēm, kā arī par rīcību, lai aizsargātos pret iespējamu krāpšanu. Informācijai ir jābūt savlaicīgai, un tā regulāri jāatjaunina;
7.2.2. Iestāde lietotājdraudzīgā un saprotamā valodā informē klientus, kā droši izmantot maksājumu instrumentus un maksājumu pakalpojumus elektroniskajā vidē un kā aizsargāt savu maksājumu instrumentu personalizētos drošības datus pirms sniegto maksājumu pakalpojumu izmantošanas sākšanas. Īpaši svarīgi ir atbilstošā veidā (ar piemēriem) norādīt, kādas darbības līgumattiecībās tiktu uzskatītas par piekrišanu maksājumam (ne tikai sniedzot informāciju savā tīmekļvietnē, bet arī izmantojot citus iedarbīgus informācijas veidus un kanālus);
7.2.3. Iestāde sniedz klientiem palīdzību saistībā ar jebkādiem pakalpojuma drošības aspektiem, paziņošanu par novirzēm un aizdomām par krāpšanu, tostarp nodrošina iespēju klientiem nekavējoties sazināties ar apmācītiem darbiniekiem. Vajadzības gadījumā Iestāde seko līdzi konkrētajam gadījumam. Šim pakalpojumam vajadzētu būt pieejamam vismaz Iestādes darba laikā.