



Laidiens: 18.09.2020., Nr. 181

Oficiālās publikācijas Nr.: 2020/181.41

Finanšu un kapitāla tirgus komisijas normatīvie noteikumi Nr. 150

Rīgā 2020. gada 8. septembrī

(Finanšu un kapitāla tirgus komisijas padomes
sēdes protokols Nr. 37 2. p.)

Informācijas tehnoloģiju un drošības risku pārvaldības normatīvie noteikumi

*Izdoti saskaņā ar Kredītiestāžu likuma
34.¹ panta otro daļu un 50. panta trešo daļu,
Maksājumu pakalpojumu un elektroniskās naudas likuma
45. panta pirmo daļu un 104.¹ panta piekto daļu,
Finanšu instrumentu tirgus likuma
4.² pantu un 124. panta 1.¹ daļu,
Privāto pensiju fondu likuma
20. panta trešo daļu un sešpadsmito daļu,
Apdrošināšanas un pārapdrošināšanas likuma
53. panta sesto daļu,
Ieguldījumu pārvaldes sabiedrību likuma
13. panta piecpadsmito daļu,
Krājaizdevu sabiedrību likuma
27. panta otro daļu,
Finanšu un kapitāla tirgus komisijas likuma
7. panta pirmās daļas 1. punktu*

1. Vispārīgie jautājumi

1. "Informācijas tehnoloģiju un drošības risku pārvaldības normatīvie noteikumi" (tālāk tekstā – noteikumi) ir saistoši Latvijas Republikā reģistrētiem vai licencētiem finanšu un kapitāla tirgus dalībniekiem (tālāk tekstā – tirgus dalībnieks): kredītiestādēm, krājaizdevu sabiedrībām, maksājumu iestādēm, elektroniskās naudas iestādēm, apdrošināšanas un pārapdrošināšanas sabiedrībām, apdrošināšanas un pārapdrošināšanas starpniekiem, privātajiem pensiju fondiem, regulētā tirgus organizētājiem, centrālajiem vērtspapīru depozitārijiem, ieguldījumu brokeru sabiedrībām, ieguldījumu pārvaldes sabiedrībām un alternatīvo ieguldījumu fondu pārvaldniekiem.
2. Noteikumu mērķis ir līdz pieņemamam līmenim mazināt tirgus dalībnieku darbībai un klientiem sniegto pakalpojumu nodrošināšanai izmantojamo informācijas tehnoloģiju (tālāk tekstā – IT) riskus un uzlabot IT un drošības pārvaldību, kopumā tiecoties uz piesardzīgu risku pārvaldības līmeni (risku apetīti), kā arī noteikt vienotas strukturētas tirgus dalībnieku IT un drošības pārvaldības prasības.
3. Tirgus dalībnieks, ieviešot drošības pasākumus, ievēro proporcionalitātes principu un uz risku izvērtējumu balstītu pieeju, ņemot vērā konkrētā tirgus dalībnieka lielumu, darbības jomu, sarežģītību, riska pakāpi un

pakalpojumus, kurus tas sniedz vai plāno sniegt. Apdrošināšanas un pārapdrošināšanas starpnieki un reģistrētie alternatīvo ieguldījumu fondu pārvaldnieki ievieš tās šo noteikumu prasības, kuras par nepieciešamām atzītas konkrētā tirgus dalībnieka aktuālajā IT risku analīzē.

2. Termini

4. Auditācijas pieraksti – analīzei pieejami pieraksti, kuros reģistrēti dati par konkrētiem IT notikumiem (piekļuve, datu ievade, maiņa, dzēšana, izvade u.c.).
5. Ārpakalpojums¹ – jebkura veida vienošanās starp tirgus dalībnieku un pakalpojuma sniedzēju, saskaņā ar kuru šis pakalpojuma sniedzējs nodrošina procesu, sniedz pakalpojumu vai veic citu darbību, ko citādi darītu pats tirgus dalībnieks.
6. Drošības pasākumi – tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina IT risku līdz pieļaujamajam līmenim.
7. IT sistēma – datu ievades, uzglabāšanas un apstrādes sistēma, kas nodrošina noteikto funkciju izpildi un paredz lietotājiem tajā glabātajiem datiem vai informācijai.
8. Informācijas resursi – informācijas vienības, kurās ietilpst datu faili, kas satur IT sistēmā glabājamo, apstrādājamo un lietotājiem pieejamo informāciju, kā arī visi IT sistēmas ievades un izvades dokumenti neatkarīgi no datu nesēja veida.
9. Informācijas resursu turētājs – persona, kas ir atbildīga par informācijas resursiem un rīkojas ar tiem tirgus dalībnieka uzdevumā.
10. Tehnoloģiskie resursi – IT sistēmas sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, palīgprogrammas, sistēmfaili, datori, datortīkli, aparatūra un citas iekārtas, kas nodrošina IT sistēmu darbību.
11. IT resursi – informācijas un tehnoloģiskie resursi.
12. Tehnoloģisko resursu turētājs – persona, kas ir atbildīga par tehnoloģiskajiem resursiem un rīkojas ar tiem tirgus dalībnieka uzdevumā.
13. Konfidencialitāte – piekļuve informācijai vai procesam tikai pilnvarotām personām vai procesiem.
14. Integritāte – informācijas un tās apstrādes metožu precizitāte, pareizība un pilnīgums.
15. Pieejamība – iespēja pilnvarotām personām lietot IT sistēmu noteiktā laikā un vietā.
16. Drošības incidents – kaitīgs notikums vai nodarījums vai vairāki saistīti notikumi, kuru rezultātā tiek apdraudēta IT integritāte, pieejamība vai konfidencialitāte.
17. IT incidents – notikums vai vairāki saistīti notikumi, kurus tirgus dalībnieks nav plānojis un kuri negatīvi ietekmē IT pakalpojumus.
18. Ievainojamība – IT nepilnība, kas ļauj kādam noteiktam apdraudējumam īstenoties un ietekmēt IT drošību.
19. Lietotājs – persona, kura piešķirto pilnvaru robežās lieto IT sistēmu.
20. Maksājumu pakalpojumu sniedzējs – kredītiestāde, maksājumu iestāde vai elektroniskās naudas iestāde, kas sniedz maksājumu pakalpojumus².

3. Pārvaldība un stratēģija

3.1. Vadības atbildība un atbalsts

21. Tirgus dalībnieka vadība nodrošina, ka tirgus dalībniekam ir atbilstoša iekšējā pārvaldība un organizācija. Vadība skaidri nosaka lomas un atbildību attiecībā uz IT funkcijām, informācijas drošības riska pārvaldību un darbības nepārtrauktību, tostarp vadības struktūru un tās komiteju lomu un atbildību.

22. Tirgus dalībnieka vadība izveido efektīvu operacionālo risku, tostarp IT un drošības risku, pārvaldības sistēmu. Šī sistēma koncentrējas uz pasākumiem risku mazināšanai un ir integrēta kopējos tirgus dalībnieka risku pārvaldības procesos.

23. Tirgus dalībnieka vadība nodrošina, ka tirgus dalībnieka IT budžets, kā arī personāls un tā prasmes ir pietiekamas, lai nodrošinātu tā IT vajadzības, risku pārvaldības procesus un IT stratēģijas īstenošanu. Vadība ir atbildīga par adekvātu resursu piešķiršanu informācijas drošības un IT audita funkciju pilnvērtīgai nodrošināšanai.

3.2. IT stratēģija

24. Tirgus dalībnieka vadība ir atbildīga par tirgus dalībnieka IT stratēģijas noteikšanu saskaņā ar tā kopējo biznesa stratēģiju un nosaka vismaz:

24.1. IT attīstības virzienus, mērķus un prioritātes, lai efektīvi atbalstītu un īstenotu tā biznesa stratēģiju, ietverot organizatoriskās struktūras izmaiņas, IT sistēmu attīstību un atkarību no ārpalpojumu sniedzējiem;

24.2. IT stratēģiskās arhitektūras attīstību;

24.3. informācijas drošības mērķus, koncentrējoties uz IT sistēmām un pakalpojumiem, personālu un procesiem.

25. Tirgus dalībnieks izveido procesus, lai uzraudzītu un mērītu IT stratēģijas īstenošanas efektivitāti, un nodrošina, ka tā IT stratēģija tiek pieņemta, īstenota un ar to savlaicīgi tiek iepazīstināti darbinieki.

3.3. Informācijas drošības funkcija

26. Tirgus dalībnieks nodrošina informācijas drošības funkciju, lai realizētu informācijas drošības risku kontroli un īstenotu nepieciešamos drošības pasākumus.

27. Informācijas drošības funkcijas ietvaros tirgus dalībnieks nodrošina vismaz:

27.1. informācijas drošības politikas izstrādi, uzturēšanu un ieviešanas kontroli;

27.2. vadības informēšanu par drošības līmeņa atbilstību prasībām un būtiskiem IT drošības incidentiem;

27.3. noteikto drošības pasākumu uzraudzību, t.sk. attiecībā uz ārpalpojumu sniedzējiem;

27.4. dalību infrastruktūras vai procesu būtisku izmaiņu pārvaldībā, ja tās ietekmē drošību;

27.5. darbinieku apmācību un informēšanu IT drošības jomā;

27.6. dalību incidentu pārvaldībā;

27.7. dalību darbības atjaunošanas un nepārtrauktības plānošanā.

28. Tirgus dalībnieks nodrošina informācijas drošības funkcijas neatkarību un objektivitāti, pienācīgi nodalot to no IT izstrādes un uzturēšanas procesiem, un nosaka pienākumu nepastarpināti informēt tirgus dalībnieka vadību par būtiskiem IT drošības notikumiem. Ja par IS drošību atbildīgais darbinieks savus pienākumus veic darbu apvienošanas kārtībā, tad ievēro pienākumu nodalīšanas principu – darbu izpildītājs nedrīkst pats sevi kontrolēt.

3.4. Audita funkcija

29. Audita funkcija, ievērojot uz risku izvērtējumu balstītu pieeju, patstāvīgi pārskata un sniedz tirgus dalībnieka vadībai objektīvu pārlicību par tirgus dalībnieka IT un drošības pārvaldību un atbilstību tā politikai un procedūrām, kā arī ārējām prasībām.

30. Auditus veic saskaņā ar plānu, kuru nosaka atbilstoši tirgus dalībniekam raksturīgajiem IT un drošības riskiem, un to dara auditori, kuriem ir nepieciešamās zināšanas, prasmes un pieredze un kuri var sniegt neatkarīgu vērtējumu tirgus dalībnieka vadībai par IT un drošības pārvaldības efektivitāti.

31. Tirgus dalībnieks nosaka pārraudzības procesu, kas nodrošina IT audita konstatējumu kontroli un novēršanu.

3.5. Ārpakalpojumu vadība

32. Ārpakalpojuma saņemšana neatbrīvo tirgus dalībnieku no normatīvajos aktos vai līgumā ar tā klientiem noteiktās atbildības – tas ir atbildīgs par ārpakalpojuma sniedzēja veikumu tādā pašā mērā kā par savu. IT drošības līmenis, ja IT attīsta vai uztur ārpakalpojuma sniedzējs, nedrīkst būt zemāks par tirgus dalībnieka noteikto.

33. Pirms lēmuma par ārpakalpojumu iegādi pieņemšanas tirgus dalībnieks izvērtē piegādātājus un, ņemot vērā pakalpojuma kvalitātes un drošības, tostarp pieejamības, prasības, vērtē riskus, kā arī nosaka pakalpojuma izbeigšanas stratēģiju.

34. Tirgus dalībnieks līgumā ar ārpakalpojuma sniedzēju ietver ārpakalpojuma kontroles prasības, t.sk. saņemtā ārpakalpojuma aprakstu, prasības attiecībā uz ārpakalpojuma apjomu, kvalitāti un drošību, konfidencialitātes saistības, tiesības saņemt visu pakalpojuma uzraudzībai nepieciešamo informāciju, prasību ārpakalpojuma sniedzējam nekavējoties ziņot par incidentiem, kā arī tiesības pārtraukt ārpakalpojuma līgumu. Ja ārpakalpojuma sniedzējs atsevišķus pakalpojuma elementus deleģē citam pakalpojumu sniedzējam, tad apakšuzņēmējs ievēro visas drošības prasības, kas noteiktas ārpakalpojuma sniedzējam. Ārpakalpojuma sniedzējs ir pilnībā atbildīgs par apakšuzņēmējiem deleģēto pakalpojumu uzraudzību.

35. Izmantojot ārpakalpojumus, t.sk. mākoņskaitļošanu, tirgus dalībniekam ir pienākums saglabāt nepieciešamo kontroli pār informācijas resursiem, kas satur informāciju par tirgus dalībnieka klientiem, t.sk. noteikt prasības attiecībā uz datu centru izvietojumu, datu šifrēšanu un drošības uzraudzību. Tirgus dalībnieka klasificētus informācijas resursus drošā veidā nošķir no citu klientu informācijas resursiem.

36. Tirgus dalībnieks sagatavo un regulāri aktualizē pakalpojuma pārtraukšanas plānu, paredzot datu un programmatūras atpakaļ nodošanu un klientu informācijas dzēšanu pie pakalpojuma sniedzēja. Tirgus dalībnieks nodrošina datu integritāti un kritisko IT pakalpojumu pieejamību situācijās, kad tiek pārtraukts ārpakalpojums, t.sk. savlaicīgi veido datu rezerves kopijas alternatīvā, ar ārpakalpojuma sniedzēju nesaistītā vietā.

37. Tirgus dalībnieks izveido un regulāri atjaunina visu izmantoto ārpakalpojumu, t.sk. uzņēmuma grupas ietvaros izmantoto ārpakalpojumu, sarakstu un veic to uzraudzību atbilstoši prasībām. Tirgus dalībnieks nodrošina, ka tam ir visas nepieciešamās prasmes un resursi, kas vajadzīgi ārpakalpojumā deleģēto darbību pienācīgai uzraudzīšanai.

38. Tirgus dalībniekam, ja tas sniedz ārpakalpojumu trešajai pusei, izmantojot savas informācijas sistēmas, tostarp autentifikācijas ārpakalpojumu, ir pienākums kontrolēt risinājuma ieviešanu trešās puses uzņēmumā. Tirgus dalībnieks informē sadarbības partnerus par riskiem, kas saistīti ar šādu pakalpojumu izmantošanu. Drošības prasību neizpildes gadījumā tirgus dalībniekam ir pienākums pārtraukt sadarbību.

4. Risku pārvaldība

4.1. Organizācija un mērķi

39. Tirgus dalībnieka vadība ir atbildīga par efektīvas IT un drošības risku pārvaldības sistēmas (ietvara) izveidi, kas ir daļa no tirgus dalībnieka vispārējās risku pārvaldības sistēmas. Tā ietver risku identificēšanu, analīzi, novērtējumu, vadību, ziņojumu un pārskatu gatavošanu un uzraudzību pieņemto limitu jeb risku apetītes ietvaros.

40. Tirgus dalībnieka risku pārvaldības funkcijai piešķir atbildību arī par IT un drošības risku pārvaldību un pārraudzību. Vadība nodrošina šīs funkcijas neatkarību, nodalot to no IT operāciju procesiem, nosaka svarīgākās lomas un atbildību, kā arī pārskatu sniegšanas kārtību.

41. IT un drošības risku pārvaldības sistēmā ietver procesus, kas ieviesti, lai:

41.1. noteiktu gatavību uzņemties IT un drošības riskus saskaņā ar tirgus dalībnieka kopējo akceptējamo risku lielumu jeb risku apetīti;

41.2. identificētu un novērtētu IT un drošības riskus, ņemot vērā to iespējamību un ietekmi;

41.3. noteiktu risku mazināšanas pasākumus, tostarp papildu kontroles, lai mazinātu IT un drošības riskus;

41.4. pārraudzītu incidentus un risku mazināšanas pasākumu efektivitāti;

41.5. ziņotu vadībai par IT un drošības riskiem un kontroles pasākumiem;

41.6. savlaicīgi identificētu un novērtētu, vai pastāv kādi IT un drošības riski, kas saistīti ar jebkādām būtiskām izmaiņām IT sistēmās, pakalpojumos, procesos, procedūrās vai pēc nozīmīgiem operacionālajiem vai drošības incidentiem.

42. Tirgus dalībnieks nodrošina, ka IT un drošības risku pārvaldības sistēma tiek dokumentēta un informācija tiek pastāvīgi uzlabota, pamatojoties uz gūtajām atziņām, kas uzkrātas sistēmas izmantošanas un uzraudzības gaitā.

43. Saskaņā ar Maksājumu pakalpojumu un elektroniskās naudas likuma 104.1 panta prasībām maksājumu pakalpojumu sniedzējam ir pienākums izveidot un sniegt uzraudzības iestādei operacionālo un drošības risku, kas saistīti ar tā sniegtajiem maksājumu pakalpojumiem, novērtējumu.

4.2. Resursu uzskaitē un klasifikācija

44. Tirgus dalībnieks izveido un uztur IT resursu, biznesa funkciju vai IT pakalpojumu sarakstu, novērtē to nozīmīgumu un nosaka to savstarpējo atkarību (*mapping*), kas saistīta ar IT un drošības riskiem.

45. Identificētos IT resursus klasificē. Veicot klasifikāciju, ņem vērā resursu konfidencialitātes, integritātes un pieejamības prasības. Klasifikācijas mērķis ir nodrošināt IT resursu aizsardzību atbilstoši to klasifikācijai. IT resursu klasifikāciju pārskata vismaz reizi divos gados vai veicot būtiskas izmaiņas.

46. Tirgus dalībnieks izveido un uztur aktuālu informācijas plūsmas shēmu.

47. Tirgus dalībnieks rakstveidā norīko IT resursu (informācijas un tehnoloģisko resursu) turētājus visiem informācijas un tehnoloģiskajiem resursiem.

48. Informācijas resursu turētāja pienākumi ir vismaz šādi:

48.1. klasificēt viņa turējumā esošos informācijas resursus;

48.2. piedalīties viņa turējumā esošo resursu IT risku analīzē un to apstiprināt;

48.3. apstiprināt pieejas tiesības resursiem un IT sistēmas izmaiņu ieviešanu;