



Laidiens: 04.10.2018., Nr. 196

Oficiālās publikācijas Nr.: 2018/196.34

Finanšu un kapitāla tirgus komisijas normatīvie noteikumi Nr. 158

Rīgā 2018. gada 26. septembrī

(Finanšu un kapitāla tirgus komisijas padomes
sēdes protokols Nr. 44 5. p.)

Informācijas sistēmu drošības normatīvie noteikumi

Izdoti saskaņā ar Finanšu un kapitāla tirgus komisijas likuma 7. panta pirmās daļas 1. punktu, 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 123.⁵ panta otro daļu, 124. panta 1.¹ daļu un likuma "Par privātajiem pensiju fondiem" 28. panta sesto daļu

I. Vispārīgie jautājumi

1. "Informācijas sistēmu drošības normatīvie noteikumi" (tālāk tekstā – noteikumi) ir saistoši Latvijā reģistrētiem finanšu un kapitāla tirgus dalībniekiem (tālāk tekstā – tirgus dalībnieks): kredītiestādēm, krājaizdevu sabiedrībām, maksājumu iestādēm, elektroniskās naudas iestādēm, apdrošināšanas sabiedrībām, apdrošināšanas starpniekiem, privātajiem pensiju fondiem, regulētā tirgus organizētājiem, vērtspapīru centrālajam depozitārijam, ieguldījumu brokeru sabiedrībām, ieguldījumu pārvaldes sabiedrībām un alternatīvo ieguldījumu fondu pārvaldniekiem.

2. Noteikumu mērķis ir ierobežot tirgus dalībnieku darbībai un klientiem sniegto pakalpojumu nodrošināšanai izmantojamo informācijas sistēmu (tālāk tekstā arī – IS) riskus, kopumā tiecoties uz piesardzīgu informācijas sistēmu risku pārvaldības līmeni (risku apetīti), kā arī noteikt vienoti strukturētas prasības tirgus dalībnieku IS drošības risku pārvaldībai.

3. Tirgus dalībnieks, ieviešot drošības pasākumus, ievēro proporcionalitātes principu un risku pārvaldībā balstītu pieeju, ņemot vērā darbības jomu, darbinieku skaitu, sniegto pakalpojumu veidu, kā arī to sarežģītību un kopējo informācijas tehnoloģiju (tālāk tekstā – IT) izmantošanas līmeni.

II. Termins

4. Auditācijas pieraksti – analīzei pieejami pieraksti, kuros reģistrēti dati par noteiktiem notikumiem IS (piekļuve, datu ievade, maiņa, dzēšana, izvade u.c.).

5. Drošības pasākumi – tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina IS risku līdz pieļaujamajam līmenim.

6. Ievainojamība – IS nepilnība, kas ļauj kādam noteiktam apdraudējumam īstenoties un ietekmēt IS drošību.
7. Informācijas sistēma – datu ievades, uzglabāšanas un apstrādes sistēma, kas nodrošina noteikto funkciju izpildi un paredz lietotājiem tajā glabātajiem datiem vai informācijai.
8. Informācijas konfidencialitāte – piekļuves nodrošināšana informācijai tikai pilnvarotām personām vai procesiem.
9. Informācijas integritāte – informācijas un tās apstrādes metožu precizitāte, pareizība un pilnīgums.
10. Informācijas pieejamība – iespēja pilnvarotām personām lietot IS noteiktā laikā un vietā.
11. Informācijas resursi – informācijas vienības, kurās ietilpst datu faili, kas satur IS glabājamo, apstrādājamo un IS lietotājiem pieejamo informāciju, kā arī visi IS ievades un izvades dokumenti neatkarīgi no datu nesēja veida.
12. Informācijas resursu turētājs – persona, kas ir atbildīga par informācijas resursiem un rīkojas ar tiem tirgus dalībnieka uzdevumā.
13. Stingrā autentifikācija – autentifikācija, kas sastāv no diviem vai vairākiem elementiem, ko klasificē kā zināšanas (to, ko zina tikai maksājumu pakalpojumu izmantotājs, piemēram, parole, PIN), valdījumu (to, kas ir tikai maksājumu pakalpojumu izmantotāja valdījumā, piemēram, kodu kalkulators, mobilā ierīce) un neatņemamas īpašības (maksājumu pakalpojumu izmantotājam raksturīgas īpašības, piemēram, pirkstu nospiedums), un kas ir savstarpēji neatkarīgi, proti, viena elementa uzticamības zaudēšanas gadījumā cita elementa uzticamība netiek apdraudēta, un kas ir izstrādāti tā, lai nodrošinātu autentifikācijas datu konfidencialitātes aizsardzību.
14. IS drošība – IS konfidencialitātes, integritātes un pieejamības prasību nodrošināšana.
15. IS drošības incidents – notikums vai vairāki saistīti notikumi, kurus tirgus dalībnieks nav plānojis un kuri negatīvi ietekmē vai, iespējams, ietekmēs IS drošību.
16. IS lietotājs – persona, kura piešķirto pilnvaru robežās lieto IS.
17. Risks – ar IS funkcionēšanu saistīta organizācijas varbūtēja nespēja pilnvērtīgi un kvalitatīvi veikt kādu savu saistību vai funkciju izpildi, ko nosaka kā nevēlamā notikuma iespējamības un tā seku kombināciju.
18. Tehnoloģiskie resursi – IS sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, palīgprogrammas, sistēmfaili, datori, datortīkli, aparatūra un citas iekārtas, kas nodrošina IS darbību.
19. Tehnoloģisko resursu turētājs – persona, kas ir atbildīga par tehnoloģiskajiem resursiem un rīkojas ar tiem tirgus dalībnieka uzdevumā.

III. Informācijas sistēmu drošības organizēšana

20. Vadības atbildība un atbalsts

20.1. Tirgus dalībnieka vadība ir atbildīga par IS drošības politikas un IT stratēģijas noteikšanu un īstenošanu, darbinieku pienākumu un atbildības noteikšanu, kontroles organizēšanu, kā arī adekvātu resursu piešķiršanu IS drošības un IS audita funkciju pilnvērtīgai nodrošināšanai.

20.2. IS drošības politikas mērķis ir definēt tirgus dalībnieka vadības nostāju un atbalstu IS drošības nodrošināšanai atbilstoši tirgus dalībnieka un tā klientu vajadzībām.

21. Normatīvi

21.1. Tirgus dalībnieks apstiprina hierarhiski strukturētu dokumentu kopumu, kas nosaka IS pārvaldību, t.sk. IS drošības pārvaldību. Definējot IS drošības pārvaldību, nosaka IS drošības mērķus, lomas, atbildību un IS drošības pasākumu piemērošanas kārtību.

21.2. Tirgus dalībnieks dokumentē vismaz tos IS pārvaldības procesus, kuru neizpilde var radīt IS drošības riskus.

21.3. Tirgus dalībnieks nodrošina normatīvu aktualizāciju un pieejamību darbiniekiem.

21.4. Tirgus dalībnieks nosaka darbinieku atbildību par normatīvu neievērošanu.

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

22. IS drošības jeb IS risku pārvaldības funkcija (tālāk tekstā – IS drošības funkcija)

22.1. Tirgus dalībnieks nodrošina IS drošības funkciju, lai realizētu risku kontroli un IS drošības pasākumu īstenošanu.

22.2. IS drošības funkcijas ietvaros tirgus dalībnieks nodrošina vismaz:

22.2.1. IS drošības normatīvu izstrādi un aktualizēšanu;

22.2.2. IS klasifikācijas un risku vadības procesa koordināciju un apdraudējumu identifikāciju;

22.2.3. vadības informēšanu par drošības līmeņa atbilstību prasībām un būtiskiem IS drošības incidentiem;

22.2.4. noteikto drošības pasākumu uzraudzību;

22.2.5. darbinieku apmācību un informēšanu IS drošības jomā;

22.2.6. IS drošības incidentu pārvaldību;

22.2.7. dalību IS darbības atjaunošanas un nepārtrauktības plānošanā.

22.3. Tirgus dalībnieks nodrošina IS drošības funkcijas neatkarību no IS izstrādes un uzturēšanas funkcijām un pienākumu nepastarpināti informēt tirgus dalībnieka vadību par būtiskiem IS 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.

23. IS audita funkcija

23.1. Tirgus dalībnieks nodrošina IS audita funkciju, lai nodrošinātu IS drošības pasākumu īstenošanas neatkarīgu pārbaudi.

23.2. Audita funkciju var nodrošināt arī ārpalpojuma sniedzējs.

24. Ārpakalpojumu vadība

24.1. Tirgus dalībnieks var izmantot trešās personas – ārpalpojuma sniedzēja – pakalpojumus. Tirgus dalībnieks veic visu izmantoto ārpalpojumu uzskaiti.

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

24.3. Pirms lēmuma pieņemšanas par ārpalpojumu iegādi tirgus dalībnieks izvērtē piegādātājus un, ņemot vērā prasības pakalpojuma kvalitātei un drošībai, tostarp pieejamībai, izvērtē riskus, kā arī nosaka pakalpojuma izbeigšanas stratēģiju.

24.4. Tirgus dalībnieks izveido un regulāri atjaunina visu izmantoto ārpakalpojumu sarakstu un veic ārpakalpojumu uzraudzību, kontrolējot to atbilstību drošības un darbības mērķiem. Tirgus dalībnieks līgumā ar ārpakalpojumu sniedzēju ietver prasības ārpakalpojuma kontrolei, piemēram, skaidru pakalpojuma aprakstu, drošības prasības, konfidencialitātes saistības, tiesības saņemt pakalpojuma uzraudzībai nepieciešamo informāciju, prasību ārpakalpojumu sniedzējam nekavējoties ziņot par incidentiem, tiesības pārtraukt līgumu.

24.5. Izmantojot ārpakalpojumus, t.sk. mākoņskaitļošanu, tirgus dalībniekam ir pienākums saglabāt nepieciešamo kontroli pār informācijas resursiem, kas satur informāciju par tirgus dalībnieka klientiem. Tirgus dalībnieka klasificētas IS drošā veidā ir fiziski vai loģiski jānošķir no ārpakalpojuma sniedzēja citu klientu IS. Jāsagatavo un regulāri jāaktualizē pakalpojuma pārtraukšanas plāns, paredzot datu, programmatūras un tehnisko resursu atpakaļ nodošanu un klientu informācijas dzēšanu pie pakalpojuma sniedzēja.

24.6. Tirgus dalībnieks veic ārpakalpojumu kvalitātes uzraudzību un drošības kontroli, t.sk. saņem pārskatus par pakalpojuma kvalitāti un incidentiem.

24.7. Tirgus dalībniekam, ja tas sniedz ārpakalpojumu trešajai pusei, izmantojot savas IS, 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.

IV. Informācijas sistēmu resursu pārvaldība

25. Resursu piederība

25.1. Tirgus dalībnieks rakstveidā norīko IS resursu (informācijas un tehnoloģisko resursu) turētājus visiem informācijas un tehnoloģiskajiem resursiem.

25.2. Informācijas resursu turētāja pienākumi ir šādi:

25.2.1. klasificēt viņa turējumā esošos informācijas resursus;

25.2.2. piedalīties viņa turējumā esošo informācijas resursu un saistīto IS risku analīzē un to apstiprināt;

25.2.3. apstiprināt pieejas tiesības IS;

25.2.4. apstiprināt IS izmaiņu veikšanu un ieviešanu;

25.2.5. noteikt prasības auditācijas pierakstu veidošanai;

25.2.6. sadarboties ar IS tehnoloģisko resursu turētāju IS funkcionalitātes un drošības jautājumos.

25.3. Tirgus dalībnieks nodrošina informācijas resursu turētāju apmācību to pienākumu izpildē.

25.4. Tehnoloģisko resursu turētāja pienākumi ir šādi:

25.4.1. nodrošināt tehnoloģisko resursu fizisko un loģisko aizsardzību;

25.4.2. sadarboties ar informācijas resursu turētāju, lai īstenotu viņa prasības par informācijas resursu aizsardzību un piekļuvi tiem;

25.4.3. piedalīties risku analīzē, noteikt ar tehnoloģiskajiem resursiem saistītos IS apdraudējumus un novērtēt šo apdraudējumu īstenošanās varbūtību;

25.4.4. nodrošināt IS atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un IS funkcionēšana traucēta vai neiespējama;

25.4.5. sadarboties ar IS informācijas resursu turētāju IS funkcionalitātes un drošības jautājumos.

25.5. Resursu turētājs minētos pienākumus var uzdot pildīt resursu aizbildņiem – personām, kuras norīkojis resursu turētājs un kuras ikdienā ir atbildīgas par attiecīgajiem IS resursiem vai to daļu.

26. IS un IT klasifikācija

26.1. Tirgus dalībnieks izveido un regulāri atjaunina IS vai IT pakalpojumu sarakstu un veic to klasifikāciju.

26.2. Klasifikācijas mērķis ir novērtēt IS un/vai IT pakalpojumu nozīmību un nodrošināt to aizsardzību atbilstoši pakalpojuma nozīmībai un piemērojamajiem operacionālajiem un drošības riskiem. Tirgus dalībnieks veic klasificēšanu, nosakot konfidencialitātes, vērtības un pieejamības līmeni.

26.3. Tirgus dalībnieks regulāri pārvērtē IS un/vai IT pakalpojumu klasifikāciju.

26.4. Tirgus dalībnieks atbilstoši informācijas klasifikācijas līmenim nosaka klasificētas informācijas lietošanas un aizsardzības prasības.

V. Risku analīze un pārvaldība

27. Tirgus dalībnieks pastāvīgi uzrauga apdraudējumus un ievainojamības un regulāri pārskata tos riska scenārijus, kas ietekmē IS un/vai IT pakalpojumus. IS risku pārvaldība ir integrēta uzņēmuma kopējā risku pārvaldības ietvarā.

28. Risku analīzes un pārvaldības mērķi ir:

28.1. noteikt pieļaujamo jeb akceptējamo risku lielumu (risku limitu jeb apetīti);

28.2. novērtēt IS apdraudējuma un ievainojamības īstenošanās varbūtību atbilstoši dažādiem riska scenārijiem;

28.3. novērtēt iespējamo kaitējumu vai ietekmi uz tirgus dalībnieku, klientu vai citu personu, ja nav nodrošināta IS drošība;

28.4. noteikt papildu drošības pasākumus, ja risks ir nepieņemams;

28.5. akceptēt pēc drošības pasākumu īstenošanas atlikušo risku (atbilstību noteiktajam risku limitam).

29. Risku analīze ir regulārs process. Tirgus dalībnieks to veic visā IS dzīves ciklā, t.sk., sākot IS projektu, veicot nozīmīgas IS izmaiņas, pārvērtējot IS klasifikāciju, parādoties jauniem būtiskiem apdraudējumiem, īstenojoties nozīmīgiem incidentiem vai pieaugot to kopējam skaitam.

30. Tirgus dalībnieks risku analīzi veic, lietojot tā apstiprināto metodiku, kas nosaka arī risku analīzes regularitāti. Tirgus dalībnieks lieto tādu risku analīzes metodiku, kas ļauj efektīvi realizēt šo noteikumu 28. punktā noteiktos mērķus.

31. Tirgus dalībnieks plāno un īsteno drošības pasākumus, ja risku analīzē novērtētais risks ir nepieņemams, un plānotajiem drošības pasākumiem nosaka realizācijas prioritātes, termiņus un atbildīgos.

32. Drošības pasākumu mērķis ir samazināt atlikušo risku līdz pieņemamam līmenim. Tirgus dalībnieks drošības pasākumus nosaka, pamatojoties uz to izmaksu un iespējamo zaudējumu samērojamību.