LATVIJAS BANKA
EIROSISTĒMA

K. VALDEMĀRA IELA 2A, RĪGA, LV-1050, LATVIJA. TĀLRUNIS +371 67022300, E-PASTS INFO@BANK.LV, WWW.BANK.LV

Projekts (1. variants)

[Datums] Noteikumi Nr. [____]
Rīgā

Informācijas tehnoloģiju un drošības risku pārvaldības noteikumi

Izdoti saskaņā ar
Apdrošināšanas un pārapdrošināšanas likuma
53. panta sesto daļu, Finanšu instrumentu tirgus
likuma 4.[2] pantu, Ieguldījumu brokeru sabiedrību likuma
31. panta ceturto daļu un 45. panta sesto daļu, Ieguldījumu
pārvaldes sabiedrību likuma 13. panta piecpadsmito daļu,
Krājaizdevu sabiedrību likuma 27. panta otro daļu,
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 un Privāto pensiju
fondu likuma 20. panta trešo un sešpadsmito daļu

1. Vispārīgie jautājumi

1. Informācijas tehnoloģiju un drošības risku pārvaldības noteikumi (turpmāk – noteikumi) ir saistoši Latvijas Republikā reģistrētiem finanšu un kapitāla tirgus dalībniekiem (turpmāk – 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, alternatīvo ieguldījumu fondu pārvaldniekiem un kolektīvās finansēšanas pakalpojumu sniedzējiem.

2. Noteikumu mērķis ir līdz pieņemamam līmenim mazināt tirgus dalībnieku darbībai un klientiem sniegto pakalpojumu nodrošināšanai izmantojamo informācijas tehnoloģiju (turpmāk – 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. Ārpakalpojums – (Eiropas Banku iestādes 2019. gada 25. februāra "Pamatnostādņu par ārpakalpojumu izmantošanu" (EBA/GL/2019/02) izpratnē) 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 lietotājpieeju 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 pakalpojumus (saskaņā ar Maksājumu pakalpojumu un elektroniskās naudas likuma 2. panta otrās daļas 1., 2. un 4. punktu).

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 ārpakalpojumu 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 laikus tiek iepazīstināti darbinieki.

3.3. Informācijas drošības funkcija

26. Tirgus dalībnieks nodrošina informācijas drošības funkciju, lai veiktu 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 ārpakalpojumu 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 pārliecību 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 atpakaļnodošanu un klientu informācijas dzēšanu pie pakalpojuma sniedzēja. Tirgus dalībnieks nodrošina datu integritāti un kritisko IT pakalpojumu pieejamību situācijās, kad tiek pārtraukts ārpakalpojums, t. sk. laikus 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. laikus 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 tādu operacionālo un drošības risku novērtējumu, kuri saistīti ar tā sniegtajiem maksājumu pakalpojumiem.

4.2. Resursu uzskaite 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;
48.4. noteikt prasības auditācijas pierakstiem;
48.5. sadarboties ar tehnoloģisko resursu turētāju IT sistēmas funkcionalitātes un drošības jautājumos.

49. Tehnoloģisko resursu turētāja pienākumi ir vismaz šādi:
49.1. nodrošināt tehnoloģisko resursu fizisko un loģisko aizsardzību;
49.2. sadarboties ar informācijas resursu turētāju, lai īstenotu viņa prasības par informācijas resursu aizsardzību un piekļuvi tiem;
49.3. piedalīties risku analīzē, noteikt ar tehnoloģiskajiem resursiem saistītos apdraudējumus un novērtēt šo apdraudējumu īstenošanās varbūtību;
49.4. nodrošināt IT sistēmas atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un IT sistēmas funkcionēšana ir traucēta vai neiespējama;
49.5. sadarboties ar informācijas resursu turētāju IT sistēmas funkcionalitātes un drošības jautājumos.

4.3. Risku novērtējums un risku mazināšana

50. Tirgus dalībnieks identificē IT un drošības riskus, kas ietekmē klasificētos IT resursus. Šādu risku novērtējumu veic un dokumentē katru gadu vai īsākos starplaikos, ja nepieciešams. Šādu risku novērtējumu veic arī attiecībā uz visām būtiskām izmaiņām infrastruktūrā, procesos vai procedūrās, kas ietekmē IT resursus.

51. Tirgus dalībnieks nodrošina, ka tas pastāvīgi uzrauga apdraudējumus un ievainojamības, kas attiecas uz tā biznesa procesiem un IT resursiem, un regulāri pārskata risku scenārijus, kas tos ietekmē.

52. Tirgus dalībnieks plāno un īsteno drošības pasākumus, ja risku analīzē novērtētais risks ir nepieņemams. Drošības pasākumu mērķis ir samazināt atlikušo risku līdz pieņemamam līmenim. Tirgus dalībnieks drošības pasākumus nosaka, pamatojoties uz to izmaksu un iespējamo zaudējumu samērojamību, un plānotajiem drošības pasākumiem nosaka realizācijas prioritātes, termiņus un atbildīgos. Tirgus dalībnieks var paredzēt arī stingrākas drošības prasības, nekā noteikts šajos noteikumos, ja tas nav pretrunā ar citiem normatīvajiem aktiem.

5. Informācijas drošība

5.1. Informācijas drošības politika

53. Tirgus dalībnieka vadība apstiprina hierarhiski strukturētu dokumentu kopumu, t. sk. informācijas drošības politiku, kurā definē tirgus dalībnieka informācijas konfidencialitātes, integritātes un pieejamības aizsardzības un IT stratēģijas īstenošanas principus un noteikumus. Informācijas drošības politikas mērķis ir definēt tirgus dalībnieka vadības nostāju un atbalstu drošības stiprināšanai atbilstoši tirgus dalībnieka un tā klientu vajadzībām.

54. Balstoties uz informācijas drošības politiku, tirgus dalībnieks nosaka informācijas drošības pasākumus, lai mazinātu IT un drošības riskus, kuriem tas ir pakļauts. Minētie

pasākumi ietver šādus aspektus: organizācija un pārvaldība, loģiskā un fiziskā drošība, IT operāciju drošība, drošības uzraudzība, informācijas drošības pārskati un pārbaude, apmācība un izpratne par informācijas drošību. Politikā iekļauj arī informācijas drošības pārvaldības galveno lomu un atbildību aprakstu, kā arī nosaka prasības personālam un procesiem saistībā ar informācijas drošību.

55. Tirgus dalībnieks iepazīstina darbiniekus ar informācijas drošības politiku.

5.2. Lietotāja autentiskuma noteikšana

56. Lietotāja autentiskuma noteikšanas mērķis ir pārliecināties, ka klasificētus informācijas resursus un atbalsta sistēmas lieto pilnvarotais lietotāja konta īpašnieks.

57. Katram tirgus dalībnieka IT lietotājam un administratoram tiek piešķirts unikāls lietotāja kods (lietotājvārds). Kopīgi lietotu kontu izmantošanu maksimāli ierobežo un nodrošina, ka lietotājus var identificēt attiecībā uz visām darbībām, kas veiktas IT sistēmās.

58. Tirgus dalībnieks nosaka autentifikācijas līdzekļu (piemēram, paroļu, kodu kalkulatoru, privāto atslēgu, biometrisko līdzekļu u. c.) lietošanas kārtību, t. sk. paroļu politiku (paroles garumu, sarežģītību, derīguma termiņu, atkārtojamības ierobežojumu). Paroļu politikas prasības iespēju robežās īsteno tehnoloģiski.

59. Iekārtām, t. sk. infrastruktūras iekārtām, kas nodrošina sistēmu darbību, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles, un tās jānomaina ar drošības prasībām atbilstošām parolēm.

60. Tirgus dalībnieks nosaka neveiksmīgu autentifikācijas mēģinājumu skaitu, pēc kura konts (izņemot sistēmas vai infrastruktūras iekārtas administratora kontu) tiek bloķēts.

61. Autentifikācijas metodes ir samērīgas ar IT sistēmas, informācijas vai procesa kritiskumu un lietotāja privilēģijām. Lai nodrošinātu drošu saziņu un samazinātu risku, IT sistēmu administratoru attālinātai piekļuvei izmanto vismaz divu faktoru autentifikāciju un kriptogrāfijas līdzekļus, piemēram, virtuālo privāto tīklu (*virtual private network* – VPN).

62. Informācijas sistēmu paroles glabā un pārsūta šifrētā veidā. Ievadot paroli, tā nedrīkst būt salasāma uz ekrāna. Paroli nekavējoties nomaina, ja tā varētu būt vai ir nesankcionēti kļuvusi zināma citai personai.

63. Izveidojot, piegādājot un aktivizējot autentifikācijas līdzekli, tirgus dalībnieks nodrošina, ka tas ir pieejams vienīgi attiecīgā lietotāja konta īpašniekam.

5.3. Pieejas tiesību vadība

64. Jauna IT sistēmas lietotāja reģistrāciju, tiesību piešķiršanu, anulēšanu un bloķēšanu tirgus dalībnieks veic saskaņā ar dokumentētu pieprasījumu, kuru apstiprina informācijas resursu turētājs. Dokumentēšanas metode nodrošina iespēju veikt efektīvu aktuālo pieejas tiesību kontroli un novērtējumu.

65. Pieejas tiesības IT sistēmām tirgus dalībnieks nosaka saskaņā ar dokumentēti apstiprinātām lomām vai lietotāju profiliem. IT lietotājam piešķir pieeju tikai tai informācijai un funkcijām, kas ir nepieciešamas viņa pienākumu izpildei.

66. Veidojot IT administratoru kontus, ievēro mazāko privilēģiju (*least privilege*) principu, un papildus iebūvētam administratora kontam tirgus dalībnieks izveido individuālus kontus (nepieciešamības gadījumā vairākus) katram administratoram, lai ierobežotu administratora privilēģijas ikdienas darbību veikšanai un novērstu nepamatotu piekļuvi lielai datu kopai. Lietotāju veiktās darbības, izmantojot augstu privilēģiju kontus, pastiprināti kontrolē un uzrauga.

67. IT sistēmu administratoriem, izmantojot paaugstinātu privilēģiju lietotāju kontus, nodala pieeju kritisko sistēmu administrēšanas videi no publiskā tīkla, piemēram, interneta pārlūkošanas vides.

68. Veidojot kontus dažādu tehnoloģisku procesu veikšanai (turpmāk – sistēmkonts), piemēram, lietojumprogrammu elektroniskai piekļuvei datiem un IT sistēmām, sistēmkontam piešķirtās privilēģijas ierobežo līdz minimumam, kas nepieciešams pakalpojuma vai procesa nodrošināšanai.

69. IT lietotāja vai administratora darba pienākumu maiņas vai darba attiecību izbeigšanas gadījumā tirgus dalībnieks nekavējoties maina vai bloķē IT lietotāja vai administratora tiesības.

70. Piekļuves tiesības periodiski pārskata, lai pārliecinātos, ka lietotājiem nav pārmērīgu privilēģiju un ka piekļuves tiesības tiek atsauktas, kad tās vairs nav vajadzīgas.

5.4. Fiziskā drošība un vides kontrole

71. Tirgus dalībnieks risku pārvaldīšanas ietvaros veic IT fiziskās aizsardzības pasākumus, lai aizsargātu tirgus dalībnieka telpas no nevēlamu apkārtējās vides faktoru (ugunsgrēks, plūdi, temperatūras svārstības, gaisa mitrums u. c.), tehnisku faktoru (neatbilstoša elektroenerģijas padeve, elektromagnētiskā lauka iedarbība u. c.) un cilvēkfaktoru (tīši vai netīši bojājumi, zādzība u. c.) iedarbības.

72. IT infrastruktūras telpas izvieto ēkas vietās, kurās ir zemāki fiziskās drošības un apkārtējas vides riski.

73. Tirgus dalībnieks IT infrastruktūras iekārtas, t. sk. serverus, disku masīvus, datortīkla iekārtas u. c., ekspluatē ierobežotas pieejas telpās, kuru fiziskā aizsardzība nodrošina tikai pilnvarotu personu piekļuvi. Šo personu piekļuvi reģistrē.

74. Tirgus dalībnieks nodrošina IT infrastruktūras telpu mikroklimatu (mitrumu, temperatūru u. tml.) un elektroenerģijas padevi atbilstoši aparatūras ražotāju noteiktajām prasībām.

75. Tirgus dalībnieks aprīko IT infrastruktūras telpas ar apsardzes signalizāciju.

76. Trešās personas IT infrastruktūras telpās drīkst uzturēties tikai to personu klātbūtnē, kurām ir tiesības iekļūt IT infrastruktūras telpās.

77. Tirgus dalībnieks IT resursus administrējošā personāla darba vietas nodala ierobežotas pieejas telpās.

5.5. Datu nesēju fiziskā aizsardzība

78. Tirgus dalībnieks veic nepieciešamos drošības pasākumus datu nesēju, t. sk. demontēto disku iekārtu, papīra izdruku, zibatmiņas karšu u. tml., fiziskai aizsardzībai atkarībā no informācijas klasifikācijas.

79. Tirgus dalībnieks nosaka kārtību, kādā lieto, pārvieto, glabā un drošā veidā iznīcina datu nesējus. Ja datu nesēju, kas satur klasificētu informāciju, ir paredzēts iznīcināt, tad tirgus dalībnieks to dara tā, lai nebūtu iespējams veikt datu atjaunošanu.

80. Tirgus dalībnieks datu nesēju aizsardzības ietvaros veic datu izvadierīču fizisko aizsardzību, novēršot nesankcionētu informācijas resursu iegūšanu, piemēram, printeru iekārtu aizsardzību, saskarņu lietošanas ierobežošanu.

5.6. IT operāciju drošība

81. Tirgus dalībnieks veic pasākumus, lai mazinātu IT sistēmu un pakalpojumu potenciālo drošības risku rašanos un to ietekmi.

82. Tirgus dalībnieks risku kontroles ietvaros veic nepieciešamās un tehnoloģiski iespējamās izmaiņas IT resursu standarta konfigurācijā un, ja tas ir nepieciešams un tehnoloģiski iespējams, samazina funkcionalitāti līdz nepieciešamajam apjomam.

83. Tirgus dalībnieks veic potenciālo ievainojamību identificēšanu un novēršanu, uzstādot kritiskus drošības labojumus. Tirgus dalībnieks nodrošina programmatūras un aparātprogrammatūras (*firmware*) atjaunināšanu vai ievieš kompensējošas kontroles.

84. Tirgus dalībnieks identificē, kā izmaiņas tā operacionālajā vidē ietekmē esošo drošības līmeni un vai ir nepieciešami papildu pasākumi, lai mazinātu ar to saistītos IT un drošības riskus. Šīs izmaiņas ir kopējā izmaiņu pārvaldības procesa daļa un nodrošina, ka izmaiņas tiek pareizi plānotas, testētas, dokumentētas, apstiprinātas un ieviestas.

5.7. Datortīklu aizsardzība

85. Tirgus dalībnieks veic visu tīkla komponentu drošas bāzes konfigurācijas (*configuration baseline*) ieviešanu, datortīkla segmentēšanu, datu noplūdes novēršanas risinājumu (*data leakage prevention* – DLP) un tīkla plūsmas šifrēšanas ieviešanu (saskaņā ar datu klasifikāciju).

86. Tirgus dalībnieks iekšējo datortīklu nodala no ārējā datortīkla. Datu plūsmā starp iekšējo un ārējo datortīklu, kā arī starp datortīkla segmentiem atļauj tikai nepieciešamās datu plūsmas. Tirgus dalībnieks regulāri pārbauda visu ārējo savienojumu eksistenci un pārliecinās, ka pastāv tikai tie savienojumi, kuri atbilst tirgus dalībnieka darbības vajadzībām.

87. Tirgus dalībnieks risku kontroles ietvaros nodrošina nepieciešamos un iespējamos papildu datu plūsmas ierobežojumus (t. sk. lietojumprogrammu, vietņu ierobežošanu) starp iekšējo un ārējo datortīklu.

88. Tirgus dalībnieks izveido un uztur aktuālas datortīkla, t. sk. datortīkla segmentu, shēmas.

5.8. Personālo datoru un ierīču aizsardzība

89. Tirgus dalībnieks nosaka, kādus informācijas resursus drīkst glabāt un kā tie tiek aizsargāti galalietotāju iekārtās, t. sk. stacionārajā un portatīvajā datorā (turpmāk – personālais dators), mobilajā ierīcē.

90. Personālajā datorā tiek uzstādīta un lietota tikai tāda programmatūra un tādā konfigurācijā, kādu noteicis tirgus dalībnieks, kurš arī nosaka kārtību un veic pasākumus aizsardzībai pret kaitīgām programmām, izmantojot, piemēram, antivīrusu programmatūru, jaunas programmatūras ierobežojumu politiku.

91. Tirgus dalībnieks, pirms piešķir personālajam datoram vai iekārtai piekļuvi korporatīvajam tīklam, novērtē, vai personālā datora vai iekārtas parametri atbilst tirgus dalībnieka noteiktajiem drošības standartiem. Personālais dators tiek pieslēgts tikai tirgus dalībnieka noteiktajiem datortīkliem.

92. Personālā datora funkcionalitāti tirgus dalībnieks ierobežo līdz darba vajadzībām nepieciešamajam funkciju līmenim, t. sk. kontrolē datora portu izmantošanu un iekārtu pieslēgšanu, kā arī pieeju publiskā tīkla informācijai (*blacklisting, whitelisting*).

93. Tirgus dalībnieks nodrošina, ka, lietotājam atstājot personālo datoru bez uzraudzības, atsākt datora izmantošanu iespējams tikai tad, ja ir veikta lietotāja autentifikācija.

94. Izmantojot personālos datorus, kuriem ir pastiprināti fiziskās drošības apdraudējumi, t. sk. portatīvās ierīces, kuras lieto ārpus tirgus dalībnieka telpām, paaugstināti klasificētā informācija tiek pārraidīta un glabāta šifrētā veidā.

95. Tirgus dalībnieks veic visu tā rīcībā esošo personālo datoru, kurus paredzēts lietot ārpus tirgus dalībnieka telpām, uzskaiti, lai noteiktu, kura persona lieto attiecīgo iekārtu.

96. Ja tiek atļauta attālināta pieeja tirgus dalībnieka IT sistēmām, izmantojot mobilās ierīces, šo ierīču drošību aizsargā, lai incidenta gadījumā tiktu novērsta klientu vai tirgus dalībnieka sensitīvu datu nokļūšana trešo pušu rīcībā, piemēram, tiek aizsargāta pieeja ierīcei, dati ierīcē netiek glabāti.

5.9. IT drošības uzraudzība

97. Tirgus dalībnieks veido organizatorisko struktūru un ievieš procesus, lai atklātu tīkla plūsmas vai sistēmu darbības anomālijas un identificētu drošības draudus, kas varētu ietekmēt tā spēju sniegt pakalpojumus. Šīs pastāvīgās uzraudzības ietvaros tirgus dalībnieks veic nepieciešamos pasākumus, lai identificētu fizisko vai loģisko ielaušanos, kā arī atklātu IT un drošības incidentus. Pārraudzības pasākumi tiek piemēroti atbilstoši IT resursu klasifikācijai.

98. Tirgus dalībnieks pastāvīgi veic IT resursu pārraudzību:
98.1. laikus identificē gan iekšējo, gan ārējo apdraudējumu;
98.2. identificē sistēmu ievainojamību un veic tās novēršanu;
98.3. uzrauga neautorizētu iekārtu un programmatūras lietošanu un veic tās novēršanu;
98.4. uzrauga IT administratoru piekļuvi sistēmām un reģistrē veiktās darbības;
98.5. kontrolē ārpakalpojumu sniedzēju piekļuvi IT sistēmām;
98.6. pārrauga IT sistēmu, iekārtu un procesu pieejamību.

99. Drošības uzraudzības procesu izveido tādu, ka tas spēj palīdzēt tirgus dalībniekam izprast darbības (operācijas) vai drošības incidenta cēloni, noteikt tendences un atbalstīt iekšējo izmeklēšanu.

5.10. Informācijas drošības novērtēšana un pārbaudes

100. Tirgus dalībnieks izveido un ievieš informācijas drošības pārbaudes procesu, kas apstiprina informācijas drošības pasākumu stabilitāti un efektivitāti. Tirgus dalībnieks nodrošina, ka šajā procesā tiek iekļautas IT un drošības risku novērtēšanas pārbaudes, kā arī ņemti vērā draudi un ievainojamības, kas identificētas, izmantojot draudu uzraudzības risinājumus, kā arī IT un drošības risku novērtēšanas procesu. Pārbaudes veic regulāri un kritiskām IT sistēmām vismaz reizi gadā. Attiecībā uz maksājumu pakalpojumu sistēmām pārbaudes un testi ir daļa no visaptverošā novērtējuma (atbilstoši Maksājumu pakalpojumu un elektroniskās naudas likuma 104.[1] panta trešajai daļai) tiem drošības risku veidiem, kas ir saistīti ar tirgus dalībnieka sniegtajiem maksājumu pakalpojumiem.

101. Proporcionāli identificētajam risku līmenim pārbaudēs iekļauj ievainojamību skenēšanu un ielaušanās (*penetration*) testus, kā arī nepieciešamības gadījumā uz draudiem vērstus ielaušanās testus (*threat led penetration testing*), kurus veic drošā veidā.

102. Tirgus dalībnieks nodrošina, ka veicamie testi ir proporcionāli identificētajam riska līmenim un tos veic neatkarīgi pārbaudītāji, kuriem ir pietiekamas zināšanas, prasmes un kompetence informācijas drošības testēšanā.

103. Veicot būtiskas izmaiņas, piemēram, ieviešot jaunu ar internetu saistītu sistēmu vai veicot nozīmīgas izmaiņas infrastruktūrā, kā arī ja izmaiņas tiek veiktas būtiska drošības incidenta dēļ, tirgus dalībnieks veic drošības pārbaudi. Tas novērtē drošības pārbaudes rezultātus un bez nevajadzīgas kavēšanās ievieš nepieciešamos drošības pasākumus.

104. Pamatojoties uz novērotajiem drošības apdraudējumiem un veiktajām izmaiņām, tirgus dalībnieks drošības pārbaudēs un testos ietver zināmos un iespējamos uzbrukumu scenārijus.

5.11. Informācijas drošības apmācība un drošības apzināšanās veicināšana

105. Tirgus dalībnieks nodrošina, ka IT lietotāju zināšanu un izpratnes līmenis ir atbilstošs IT lietošanas vajadzībām, tā samazinot personāla kļūdas, krāpšanu, resursu ļaunprātīgu izmantošanu vai citu veidu zaudējumus.

106. Tirgus dalībnieks izstrādā apmācības programmu visiem darbiniekiem, tostarp drošības izpratnes programmu, lai nodrošinātu, ka darbinieki ir apmācīti veikt savus pienākumus saskaņā ar tirgus dalībnieka drošības politiku un attiecīgajām procedūrām, t. sk. klasificētas informācijas aizsardzības prasībām. Tirgus dalībnieks nodrošina, ka apmācība visiem darbiniekiem tiek veikta vismaz reizi gadā.

6. IT operāciju pārvaldība

107. Tirgus dalībnieks pārvalda savas IT operācijas, pamatojoties uz dokumentētiem un ieviestiem procesiem. Dokumentu kopumā nosaka, kā tirgus dalībnieks uztur, uzrauga un kontrolē savas IT sistēmas un pakalpojumus, tādējādi mazinot kļūdas un darbinieku aizstājamības risku.

108. Darbiniekiem, kas veic IT uzturēšanu, tirgus dalībnieks nosaka pienākumus un atbildību, nodrošina aizstājamību un kvalifikācijas uzturēšanu. Procesu kontroles nodrošināšanai veic pienākumu nodalīšanu.

109. Tirgus dalībnieks nodrošina, lai IT operācijas tiktu veiktas atbilstoši tā biznesa prasībām, un pēc iespējas uzlabo savu IT operāciju efektivitāti, t. sk. veic pasākumus, kas mazina iespējamās kļūdas, kuras rodas manuāli izpildītu uzdevumu rezultātā.

6.1. Konfigurācijas pārvaldība un kontrole

110. Tirgus dalībnieks nosaka kārtību, kādā pieprasa, autorizē, testē, maina un dokumentē IT resursus.

111. Tirgus dalībnieks uztur aktuālu IT resursu (ieskaitot IT sistēmas, tīkla ierīces, datubāzes utt.) uzskaiti. IT resursu uzskaite ir pietiekami detalizēta, lai varētu laikus identificēt IT aktīvus, to atrašanās vietu, drošības klasifikāciju un piederību (resursu turētāju). IT resursu uzskaitē ieteicams saglabāt arī resursu aktuālo konfigurāciju, kā arī saikni ar citiem resursiem un ārējiem pakalpojumiem, lai nodrošinātu konfigurācijas un izmaiņu pārvaldības procesu efektivitāti un laikus spētu reaģēt uz drošības un operatīvajiem incidentiem, tostarp kiberuzbrukumiem.

112. Tirgus dalībnieks uzrauga un pārvalda IT resursu dzīves ciklus, lai nodrošinātu, ka tie atbalsta biznesa un risku pārvaldības prasības. Tirgus dalībnieks uzrauga, kā tā IT aktīvus atbalsta un uztur ārējie piegādātāji vai iekšējie izstrādātāji un vai visi nepieciešamie ielāpi un jauninājumi, pamatojoties uz dokumentētiem procesiem, ir uzstādīti. Tirgus dalībnieks vērtē un mazina riskus, ko rada novecojuši vai neatbalstīti IT aktīvi.

113. Tirgus dalībnieks nodrošina veiktspējas pārbaudes un kapacitātes plānošanas un uzraudzības pasākumus, lai laikus novērstu IT sistēmu veiktspējas un kapacitātes trūkumu.

6.2. Auditācijas pierakstu pārvaldība

114. Lai identificētu lietotāju veiktās darbības un IT kļūdas, tirgus dalībnieks veido, glabā un analizē auditācijas pierakstus.

115. Auditācijas pierakstos tirgus dalībnieks iekļauj vismaz visu veiksmīgu un neveiksmīgu lietotāju pieslēgšanās gadījumu laiku un lietotāju kodus. Papildu auditācijas pierakstus veic par informācijas sistēmu parametru maiņu, t. sk. par darbībām ar lietotāju kontiem, ciktāl to var nodrošināt ar lietoto tehnoloģisko risinājumu. Pierakstos ietver darbību identificēšanai nepieciešamo informāciju tādā apmērā, kādā to var nodrošināt esošais tehnoloģiskais risinājums, t. sk. IP adresi, no kuras ir veikta darbība.

116. Tirgus dalībnieks lieto metodes un rīkus, kas ļauj efektīvi analizēt auditācijas pierakstus, lai atvieglotu anomāliju identificēšanu, laikus konstatētu incidentus un sekmētu to izmeklēšanu.

117. Tirgus dalībnieks nodrošina auditācijas pierakstu integritāti. Piekļuvi auditācijas pierakstiem aizsargā, lai novērstu to neatļautu modifikāciju vai dzēšanu.

118. Auditācijas pierakstus glabā tik ilgi, cik tas ir nepieciešams tirgus dalībnieka biznesa funkcijām vai atbalsta procesiem, kā arī ņemot vērā glabāšanas prasības, kas noteiktas ārējos normatīvajos aktos.

119. Tirgus dalībnieks vismaz 18 mēnešus glabā auditācijas pierakstus par tirgus dalībnieka klientu veiktajiem un atteiktajiem attālināto pakalpojumu pieslēgumiem, kas nodrošina klientu aktīvu, t. sk. naudas līdzekļu, pārvaldību. Auditācijas pierakstos reģistrē vismaz lietotāja veikto transakciju un citu darbību identificēšanai nepieciešamo informāciju, t. sk. avota IP adresi un laiku.

6.3. Datu rezerves kopēšana

120. Tirgus dalībnieks nosaka un ievieš datu un IT sistēmu rezerves kopēšanas un atjaunošanas procedūras sistēmu darbības atjaunošanai nepieciešamības gadījumā. Datu rezerves kopēšanas apjomu un biežumu nosaka atbilstoši biznesa atjaunošanas prasībām, datu un IT sistēmu kritiskajam svarīgumam un risku novērtējumam. Regulāri pārbauda, vai, izmantojot rezerves kopijas, ir iespējams atjaunot sistēmu darbību.

121. Tirgus dalībnieks nodrošina, ka datu un IT sistēmu rezerves kopijas tiek glabātas droši un pietiekami attālināti, lai tās netiktu pakļautas ražošanas vides riskiem. Rezerves kopijas aizsargā pret nesankcionētu lietošanu un bojāšanu.

6.4. Incidentu pārvaldība

122. Tirgus dalībnieks nosaka un ievieš incidentu un problēmu pārvaldības procesus, lai identificētu un novērstu IT un drošības incidentus un ļautu tirgus dalībniekam atjaunot un turpināt biznesa procesus.

123. Tirgus dalībnieks nosaka piemērotus kritērijus un sliekšņus, lai klasificētu notikumu kā IT vai drošības incidentu, kā arī nosaka agrīnās brīdināšanas indikatorus, kuri dotu iespēju incidentus atklāt vai novērst laikus. Lai mazinātu nelabvēlīgu notikumu ietekmi un ļautu laikus atjaunot pakalpojumus, tirgus dalībnieks veido konsekventu un integrētu IT un drošības incidentu pārvaldību un veicina, ka tiek novērsti incidentu cēloņi un ierobežota incidentu atkārtošanās.

124. Incidentu un problēmu pārvaldībai tirgus dalībnieks nosaka vismaz:
124.1. procedūras incidentu identificēšanai, ietekmes mazināšanai un seku likvidēšanai, pierādījumu saglabāšanai, reģistrēšanai un klasificēšanai atbilstoši ietekmei;
124.2. darbinieku lomas un atbildību dažādu incidentu scenāriju gadījumā (piemēram, kļūdas, darbības traucējumi, kiberuzbrukumi);
124.3. problēmu pārvaldības procedūru, lai identificētu, analizētu un novērstu viena vai vairāku incidentu pamatcēloni (*root cause*). Tirgus dalībnieks ņem vērā incidentu vadības procesā gūtās atziņas un attiecīgi uzlabo drošības pasākumus;
124.4. efektīvus iekšējās saziņas plānus, tostarp incidentu paziņojumus un eskalācijas procedūras, kas aptver arī ar drošības jautājumiem saistītu klientu sūdzību izskatīšanu un ziņojumus augstākajai vadībai par būtiskiem incidentiem, kas ietekmē kritiskos IT pakalpojumus;
124.5. ārējās komunikācijas plānus sadarbībai ar ieinteresētajām personām (klientiem, citiem tirgus dalībniekiem, uzraudzības iestādi), lai efektīvi reaģētu uz incidentu un tā izraisītajiem riskiem un sniegtu savlaicīgu informāciju.

125. Maksājumu pakalpojumu sniedzējs ziņo par būtiskiem maksājumu pakalpojumu incidentiem saskaņā ar Latvijas Bankas noteikumiem, kas regulē par ziņošanu par būtiskiem maksājumu pakalpojumu incidentiem.

7. IT projektu un izmaiņu pārvaldība

7.1. IT projektu vadība

126. Tirgus dalībnieks nosaka IT projektu vadības metodoloģiju, kas efektīvi atbalsta IT stratēģijas īstenošanu un mērķu sasniegšanu, kā arī ietver projekta risku novērtējumu, IT drošības prasību definēšanu, projekta plānu un laika grafiku, projekta vadības organizāciju un atbildīgās personas.

127. Tirgus dalībnieks uzrauga un mazina riskus, kas saistīti ar kopējā IT projektu portfeļa pārvaldību. Vērtēšanā ņem vērā arī riskus, kas var rasties dažādu projektu savstarpējas ietekmes un tirgus dalībnieka ierobežoto resursu dēļ.

7.2. IT sistēmu izstrāde un iegāde

128. Tirgus dalībnieks nosaka un ievieš procesu, kas regulē IT sistēmu iegādi, izstrādi un uzturēšanu. Šo procesu izstrādā, izmantojot uz risku izvērtējumu balstītu pieeju, un tajā ietver vismaz:
128.1. mērķu izvirzīšanu un projekta risku analīzi izstrādes un iegādes posmā;
128.2. tehnisko prasību noteikšanu, ieskaitot drošas programmēšanas vadlīnijas;
128.3. kvalitātes nodrošināšanas standartus;
128.4. IT sistēmu testēšanu, apstiprināšanu un laidienu pārvaldību (*release management*) neatkarīgi no tā, vai izstrādi veic pats tirgus dalībnieks vai ārējs pakalpojumu sniedzējs.

129. Tirgus dalībnieks nodrošina, lai pirms IT sistēmu izstrādes tehniskajā specifikācijā tiktu skaidri definētas funkcionālās un nefunkcionālās prasības (t. sk. informācijas drošības prasības). Ar definētajām prasībām saistītās kontroles tiek iestrādātas sistēmas arhitektūrā un uzturēšanas procesos. Drošības arhitektūra paredz vairāklīmeņu aizsardzību, kāda drošības līmeņa kompromitēšanas gadījumā saglabājot IT kopējo aizsargspēju.

130. Tirgus dalībnieks nodrošina, ka tiek ieviesti pasākumi, lai izstrādes laikā nepieļautu netīšu neautorizētu izmaiņu vai tīšu ļaunprātīgu manipulāciju veikšanu ar IT sistēmu. Tirgus dalībnieks īsteno pasākumus, lai aizsargātu iekšēji izstrādāto IT sistēmu pirmkodu integritāti.

131. Tirgus dalībnieks apstiprina IT sistēmu testēšanas, noteikto prasību un projektējumu pārbaudes un apstiprināšanas metodoloģiju.

132. Tirgus dalībnieks pirms IT sistēmu ieviešanas nodrošina saistīto IT pakalpojumu un IT drošības kontroļu pārbaudi ar mērķi laikus identificēt iespējamās drošības nepilnības, pārkāpumus un incidentus.

133. Tirgus dalībnieks nodrošina ražošanas (produkcijas) vides nodalīšanu no izstrādes, testēšanas vai citas vides, kas nav ražošanas vide. Tirgus dalībnieks nodrošina ražošanas datu integritāti un konfidencialitāti vidē, kurā nenotiek ražošana. Piekļuve ražošanas datiem visās vidēs ir tikai pilnvarotiem lietotājiem.

134. Tirgus dalībnieks veido un uztur nepieciešamo dokumentāciju. Tajā iekļauj nepieciešamo informācijas apjomu, lai varētu nodrošināt kvalitatīvu IT lietošanu, uzturēšanu un izmaiņu pārvaldīšanu, piemēram, tehniskās sistēmas dokumentāciju, IT administratora un lietotāju instrukcijas u. c.

135. Tirgus dalībnieka noteikto IT sistēmu izstrādes un iegādes procesu un risku vadību piemēro arī sistēmām, kuras izstrādā vai pārvalda biznesa funkciju galalietotāji ārpus uzņēmuma IT organizācijas, piemēram, pašu galalietotāju pārvaldītām vai veidotām lietojumprogrammām. Tirgus dalībnieks uztur šo lietojumprogrammu reģistru, ja tās atbalsta būtiskus biznesa procesus.

7.3. IT izmaiņu vadība

136. Tirgus dalībnieks veido un ievieš IT izmaiņu pārvaldības procesu, lai nodrošinātu, ka visas izmaiņas IT sistēmās tiek reģistrētas, novērtētas, izstrādātas, testētas, dokumentētas, apstiprinātas un ieviestas kontrolētā veidā.

137. Avārijas IT izmaiņu procesā tirgus dalībnieks nosaka personas, kuras ir tiesīgas pieņemt lēmumu par šādām izmaiņām, un veic pasākumus, lai preventīvi samazinātu nepieciešamību veikt avārijas izmaiņas.

8. Darbības nepārtrauktības pārvaldība

138. Tirgus dalībnieks izveido darbības nepārtrauktības pārvaldības procesu, lai maksimāli palielinātu spēju nodrošināt pakalpojumus un ierobežotu zaudējumus nopietnu darbības traucējumu gadījumā.

139. Tirgus dalībnieks ir atbildīgs par tā IT nepārtrauktības politikas noteikšanu un apstiprināšanu, kas ir daļa no tirgus dalībnieka vispārējās darbības nepārtrauktības politikas. Tirgus dalībnieks informē darbiniekus un nepieciešamības gadījumā arī ārpakalpojumu sniedzējus par IT nepārtrauktības politikā noteikto.

8.1. Biznesa ietekmes analīze

140. Darījumdarbības nepārtrauktības pārvaldības ietvaros tirgus dalībnieks veic biznesa ietekmes analīzi (turpmāk – BIA), vērtējot nozīmīgu incidentu vai ārkārtas situāciju ietekmi uz tirgus dalībnieka darbību. Veicot BIA, veic incidenta ietekmes kvantitatīvu vai kvalitatīvu novērtējumu, izmantojot iekšējos un ārējos datus un scenāriju analīzi. BIA ņem vērā arī identificēto un klasificēto biznesa procesu un resursu kritiskumu un to savstarpējo ietekmi saskaņā ar šo noteikumu 4. nodaļu.

141. Tirgus dalībnieks nodrošina, ka tā IT sistēmas, infrastruktūra un pakalpojumi tiek veidoti un uzturēti saskaņā ar BIA, piemēram, tiek izmantota kritisku IT infrastruktūras elementu rezervēšana vai dublēšana, lai novērstu dīkstāvi avārijas gadījumā.

8.2. Darbības nepārtrauktības plānošana

142. Balstoties uz BIA, tirgus dalībnieks veido darbības nepārtrauktības plānu (turpmāk – DNP) un ņem vērā arī riskus, kas nelabvēlīgi ietekmētu IT sistēmas un IT pakalpojumus. DNP apstiprina vadība, un tā mērķis ir aizsargāt un vajadzības gadījumā atjaunot tirgus dalībnieka biznesa procesus un resursu konfidencialitāti, integritāti un pieejamību.

143. Tirgus dalībnieks DNP vērtē iespējamo ietekmi un plāno darbības dažādu scenāriju gadījumos, ieskaitot ārkārtējus, bet iespējamus scenārijus, piemēram, kiberuzbrukumu, terorismu. Balstoties uz šiem scenārijiem, tirgus dalībnieks apraksta, kā tiek nodrošināta IT sistēmu un pakalpojumu nepārtrauktība, kā arī tirgus dalībnieka informācijas drošība.

144. Tirgus dalībnieks ievieš DNP, lai nodrošinātu, ka tas var pienācīgi reaģēt uz iespējamiem dīkstāves scenārijiem atjaunošanas laika mērķa (RTO – maksimālais laiks,

kurā sistēma vai process jāatjauno pēc negadījuma) un atjaunošanas punkta mērķa (RPO – maksimālais laika periods, par kuru var zaudēt datus negadījuma rezultātā) ietvaros.

8.3. Darbības atjaunošanas plāni

145. Balstoties uz BIA un identificētajiem scenārijiem, tirgus dalībnieks izstrādā reaģēšanas un atjaunošanas plānus. Šajos plānos nosaka, kādos apstākļos plāns tiek aktivizēts un kādas darbības jāveic, lai nodrošinātu vismaz kritiski svarīgo IT sistēmu un pakalpojumu atjaunošanu un pieejamību. Atjaunošanas plāni ir vērsti uz to, lai sasniegtu tirgus dalībnieka noteiktos operāciju atjaunošanas mērķus.

146. Atjaunošanas plānos ņem vērā gan īstermiņa, gan ilgtermiņa atjaunošanas iespējas un tajos vismaz:
146.1. koncentrējas uz kritiski svarīgo IT pakalpojumu, biznesa funkciju, atbalsta procesu, informācijas resursu un to savstarpēji saistīto darbību atjaunošanu, lai samazinātu nelabvēlīgo ietekmi uz tirgus dalībnieka darbību, tostarp uz maksājumu sistēmām un maksājumu pakalpojumu lietotājiem, un lai nodrošinātu nenokārtoto maksājumu darījumu izpildi;
146.2. dokumentē un nosaka atbildīgos darbiniekus, kuriem jābūt viegli pieejamiem ārkārtas gadījumos, iekļaujot skaidru lomu un atbildības sadalījumu;
146.3. nosaka, ka tie jāatjaunina, ņemot vērā incidentos un pārbaudēs gūto pieredzi, atklātos jaunos riskus un draudus, kā arī mainītos atjaunošanas mērķus un prioritātes.

147. Atjaunošanas plānos apsver alternatīvas rīcības iespējas, ja risku, izmaksu, loģistikas vai neparedzētu apstākļu dēļ atjaunošana paredzētajā termiņā var nebūt iespējama.

148. Atjaunošanas plānu ietvaros tirgus dalībnieks apsver un īsteno nepārtrauktības pasākumus, lai mazinātu ārpakalpojumu sniedzēju, kuru pakalpojumi ir nozīmīgi tirgus dalībnieka IT pakalpojumu nepārtrauktībai, dīkstāves.

8.4. DNP pārbaude

149. Tirgus dalībnieks, pamatojoties uz savu riska profilu, regulāri, t. i., vismaz reizi gadā, veic DNP pārbaudi un pārliecinās, ka tā kritisko biznesa procesu (ieskaitot tos, kurus nodrošina ārpakalpojumu sniedzēji), kā arī resursu pieejamība (ņemot vērā arī to savstarpējo atkarību) tiek nodrošināta.

150. Tirgus dalībnieks regulāri, t. i., vismaz reizi gadā, pamatojoties uz pārbaudes rezultātiem un pieejamo informāciju par draudiem, kā arī ņemot vērā pieredzi, kas gūta no incidentiem, atjaunina DNP. Tajā iekļauj arī visas izmaiņas atjaunošanas mērķos (t. sk. RTO un RPO), kā arī izmaiņas biznesa procesos un resursos.

151. Tirgus dalībnieks dokumentē DNP testu rezultātus un visus trūkumus, kas tiek identificēti testos, analizē, risina un ziņo par tiem vadībai.

8.5. Krīzes komunikācija

152. Tirgus dalībnieks ārkārtas situācijā, kā arī DNP īstenošanas laikā veic efektīvus krīzes komunikācijas pasākumus, lai visas attiecīgās iekšējās un ārējās atbildīgās personas, tostarp ārpakalpojumu sniedzēji, tiktu laikus un pietiekami informētas. Tirgus dalībnieks klientiem sniedz maksimāli plašu un detalizētu informāciju par incidentu, neietverot ierobežotas pieejamības informāciju, lai mazinātu baumu un viltus ziņu izplatīšanos incidenta laikā.

9. Maksājumu pakalpojumu lietotāju attiecību pārvaldība

153. Maksājumu pakalpojumu sniedzējs, lai uzlabotu maksājumu pakalpojumu lietotāju izpratni par maksājumu pakalpojumu drošību, informē tos par riskiem, kas saistīti ar maksājumu pakalpojumu izmantošanu, un sniedz nepieciešamo atbalstu un norādījumus.

154. Maksājumu pakalpojumu sniedzējs piedāvāto informāciju un norādījumus atjaunina, ņemot vērā aktuālos draudus un ievainojamības. Visas drošības informācijas izmaiņas paziņo maksājumu pakalpojumu lietotājam.

155. Ja produkta funkcionalitāte atļauj, maksājumu pakalpojumu sniedzējs ļauj maksājumu pakalpojumu lietotājam atteikt (atspējot) maksājumu funkcijas, kas saistītas ar maksājumu pakalpojumu sniedzēja piedāvātajiem maksājumu pakalpojumiem.

156. Maksājumu pakalpojumu sniedzējs nosaka maksājumu limitus. Maksājumu pakalpojumu sniedzējs var vienoties ar maksājumu pakalpojumu lietotāju par tā riska profilam atbilstošu maksājumu limitu katram maksājuma instrumentam. Maksājumu pakalpojumu lietotājam tiek nodrošināta iespēja mainīt šos ierobežojumus, nepārsniedzot maksimālo saskaņoto robežu, par kuru ir notikusi vienošanās.

157. Maksājumu pakalpojumu sniedzējs nodrošina maksājumu pakalpojumu lietotājam iespēju saņemt brīdinājumus par ierosinātiem maksājumu darījumiem vai neveiksmīgiem mēģinājumiem sākt maksājumu darījumus, ļaujot atklāt krāpniecisku vai ļaunprātīgu kontu izmantošanu.

158. Maksājumu pakalpojumu sniedzējs informē maksājumu pakalpojumu lietotāju par atjauninājumiem drošības procedūrās, kas ietekmē maksājumu pakalpojumu lietotāju attiecībā uz maksājumu pakalpojumu sniegšanu.

10. Noslēguma jautājumi

159. Noteikumi ir spēkā līdz 2025. gada 16. janvārim.

160. Atzīt par spēku zaudējušiem Finanšu un kapitāla tirgus komisijas 2020. gada 8. septembra noteikumus Nr. 150 "Informācijas tehnoloģiju un drošības risku pārvaldības normatīvie noteikumi".

ŠIS DOKUMENTS IR ELEKTRONISKI PARAKSTĪTS AR DROŠU ELEKTRONISKO PARAKSTU UN SATUR LAIKA ZĪMOGU

Latvijas Bankas prezidents M. Kazāks