Pamatnostādnes

EBA/GL/2019/04

2019. gada 28. novembris

EBI pamatnostādnes par IKT un drošības risku pārvaldību

Atbilstības nodrošināšanas un ziņošanas pienākumi

Pamatnostādņu statuss

1. Šis dokuments ietver pamatnostādnes, kas izdotas saskaņā ar Regulas (ES) Nr. 1093/2010 16. pantu [1]. Kompetentajām iestādēm un finanšu iestādēm saskaņā ar Regulas (ES) Nr. 1093/2010 16. panta 3. punktu jādara viss iespējamais, lai ievērotu šīs pamatnostādnes.

2. Pamatnostādnēs izklāstīts EBI viedoklis par attiecīgām uzraudzības praksēm Eiropas finanšu uzraudzības sistēmā jeb par to, kā Eiropas Savienības tiesību akti ir jāpiemēro konkrētā jomā. Kompetentajām iestādēm, kas minētas Regulas (ES) Nr. 1093/2010 4. panta 2. punktā, uz kurām attiecas šīs pamatnostādnes, tās jāievēro, iekļaujot tās attiecīgi savā praksē (piemēram, veicot grozījumus savā tiesiskajā regulējumā vai uzraudzības procesos), tostarp gadījumos, ja pamatnostādnes ir paredzētas galvenokārt iestādēm.

Ziņošanas prasības

3. Saskaņā ar Regulas (ES) Nr. 1093/2010 16. panta 3. punktu kompetentajām iestādēm līdz ([dd.mm.yyyy]) jāpaziņo EBI, vai tās ievēro vai paredz ievērot šīs pamatnostādnes, vai arī jānorāda to neievērošanas iemesli. Ja attiecīgajā termiņā šāds ziņojums netiek saņemts, EBI uzskata, ka kompetentās iestādes neievēro šīs pamatnostādnes. Paziņojumi jāiesniedz, nosūtot EBI tīmekļa vietnē pieejamo veidlapu uz e-pasta adresi compliance@eba.europa.eu ar norādi "EBA/GL/2019/04". Ziņojumi ir jāsaņem no personām, kuras ir attiecīgi pilnvarotas kompetento iestāžu vārdā ziņot par atbilstību. Par jebkurām izmaiņām atbilstības statusā arī ir jāziņo EBI.

4. Paziņojumus publicēs EBI tīmekļa vietnē saskaņā ar 16. panta 3. punktu.

[1] Eiropas Parlamenta un Padomes Regula (ES) Nr. 1093/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK (OV L 331, 15.12.2010., 12. lpp.).

Priekšmets, piemērošanas joma un definīcijas

Priekšmets

5. Šīs pamatnostādnes pamatojas uz Direktīvas 2013/36/ES (Kapitāla prasību direktīva, CRD) 74. panta noteikumiem par iekšējo pārvaldību, un tās izriet no pilnvarojuma izstrādāt pamatnostādnes, kas noteikts Direktīvas (ES) 2015/2366 (Otrā maksājumu pakalpojumu direktīva, PSD2) 95. panta 3. punktā.

6. Šajās pamatnostādnēs ir precizēti riska pārvaldības pasākumi, kas finanšu iestādēm (kā noteikts 9. punktā turpmāk) jāveic saskaņā ar Kapitāla prasību direktīvas 74. pantu, lai pārvaldītu savus IKT un drošības riskus attiecībā uz visām darbībām, un tas, ka maksājumu pakalpojumu sniedzējiem (MPS, kā definēts 9. punktā turpmāk) saskaņā ar Otrā maksājumu pakalpojumu direktīvas 95. panta 1. punktu jāpārvalda operacionālie un drošības riski (kas saprotami kā "IKT un drošības riski"), kuri saistīti ar viņu nodrošinātajiem maksājumu pakalpojumiem. Pamatnostādnēs ir iekļautas prasības attiecībā uz informācijas drošību, tostarp kiberdrošību, ciktāl informācija tiek glabāta IKT sistēmās.

Piemērošanas joma

7. Šīs pamatnostādnes piemēro attiecībā uz IKT un drošības risku pārvaldību finanšu iestādēs (kā noteikts 9. punktā). Šajās pamatnostādnēs termins "IKT" un "drošības riski" attiecas uz PSD2 95. pantā minētajiem operacionālajiem un drošības riskiem attiecībā uz maksājumu pakalpojumu nodrošināšanu.

8. Maksājumu pakalpojumu sniedzējiem (kā definēts 9. punktā) šīs pamatnostādnes piemēro maksājumu pakalpojumu nodrošināšanai saskaņā ar PSD2 95. panta darbības jomu un pilnvarojumu. Iestādēm (kā definēts 9. punktā) šīs pamatnostādnes attiecas uz visām darbībām, ko tās nodrošina.

Adresāti

9. Šīs pamatnostādnes ir adresētas finanšu iestādēm un šo pamatnostādņu vajadzībām attiecas uz (1) MPS, kā definēts PSD2 4. panta 11. punktā, un (2) uz iestādēm, ar kurām saprot kredītiestādes un ieguldījumu brokeru sabiedrības, kā definēts Regulas 575/2013 4. panta 1. punkta 3. apakšpunktā. Šīs pamatnostādnes attiecas arī uz kompetentajām iestādēm, kā noteikts Regulas (ES) Nr. 575/2013 4. panta 1. punkta 40. apakšpunktā, tostarp Eiropas Centrālo banku saistībā ar jautājumiem, kas attiecas uz Regulā (ES) Nr. 1024/2013 tai uzticētajiem uzdevumiem, un PSD2 minētajām kompetentajām iestādēm, kā norādīts Regulas (ES) Nr.1093/2010 4. panta 2. punkta i) apakšpunktā.

Definīcijas

10. Ja vien nav norādīts citādi, Direktīvā 2013/36/ES (CRD), Regulā (ES) Nr. 575/2013 (CRR) un Direktīvā 2015/2366/ES (PSD2) izmantotajiem un definētajiem terminiem pamatnostādnēs ir viena un tā pati nozīme. Šajās pamatnostādnēs papildus tiek piemērotas šādas definīcijas:

IKT un drošības risks	Zaudējumu risks, kas rodas saistībā ar konfidencialitātes pārkāpumu, sistēmu un datu integritātes zudumu, sistēmu un datu neatbilstību vai nepieejamību, kā arī gadījumā, kad, mainoties vides vai darījumdarbības prasībām (t. i., ātrumam), saprātīgā laikposmā un ar saprātīgām izmaksām nav bijis iespējams mainīt informācijas tehnoloģiju (IT) [2]. Tas ietver drošības riskus, ko izraisa neatbilstīgi vai nepilnvērtīgi iekšējie procesi vai ārējie notikumi, tostarp kiberuzbrukumi vai neatbilstīga fiziskā drošība.
Vadības struktūra	(a) Attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām šā termina nozīme atbilst Direktīvas 2013/36/ES 3. panta 1. punkta 7. apakšpunktā sniegtajai definīcijai. (b) Attiecībā uz maksājumu iestādēm vai elektroniskās naudas iestādēm, šis termins nozīmē direktorus vai personas, kas ir atbildīgas par maksājumu iestāžu vai elektroniskās naudas iestāžu vadību, un attiecīgos gadījumos — personas, kas ir atbildīgas par maksājumu iestāžu vai elektroniskās naudas iestāžu maksājumu pakalpojumu darbību vadību. (c) Attiecībā uz Direktīvas (ES) 2015/2366 1. panta 1. punkta c), e) un f) apakšpunktā minētajiem MPS šim terminam ir tāda nozīme, kāda tam piešķirta piemērojamajos ES un valsts tiesību aktos.
Operacionālais vai drošības incidents	Vienreizējs notikums vai vairāki saistīti notikumi, kurus finanšu iestāde nav plānojusi un kuri negatīvi ietekmē vai, iespējams, ietekmēs pakalpojumu integritāti, pieejamību, konfidencialitāti un/vai autentiskumu.
Augstākā vadība	(a) Attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām šā termina nozīme atbilst Direktīvas 2013/36/ES 3. panta 1. punkta 9. apakšpunktā sniegtajai definīcijai. (b) Attiecībā uz maksājumu iestādēm vai elektroniskās naudas iestādēm šis termins nozīmē tās fiziskās personas, kuras iestādē veic izpildfunkcijas un ir atbildīgas un pārskatatbildīgas vadības struktūrai par iestādes ikdienas pārvaldību. (c) Attiecībā uz Direktīvas (ES) 2015/2366 1. panta 1. punkta c), e) un f) apakšpunktā minētajiem MPS šim terminam ir tāda

[2] Definīcija no EBI 2014. gada 19. decembra pamatnostādnēm par kopējām procedūrām un metodoloģiju, ko izmanto uzraudzības pārskatīšanas un novērtēšanas procesā (EBA/GL/2014/13), kas grozītas ar EBA/GL/2018/03.

	nozīme, kāda tam piešķirta piemērojamajos ES un valsts tiesību aktos.
Vēlme uzņemties risku	Tāda riska kopējais līmenis un veidi, ko MPS un iestādes saskaņā ar to darbības modeli vēlas uzņemties savas riska spējas darījumdarbības jomā, lai sasniegtu savus stratēģiskos mērķus.
Revīzijas funkcija	(a) Kredītiestādēm un ieguldījumu brokeru sabiedrībām revīzijas funkcija ir tāda, kā minēts 22. iedaļā EBI pamatnostādnēs par iekšējo pārvaldību (EBA/GL/2017/11). (b) Attiecībā uz MPS, kas nav kredītiestādes, revīzijas funkcijai jābūt neatkarīgai MPS ietvaros vai neatkarīgai no tām, un tā var būt iekšējā un/vai ārējā revīzijas funkcija.
IKT projekti	Jebkurš projekts vai tā daļa, kurā IKT sistēmas un pakalpojumi tiek mainīti, aizstāti, atcelti vai ieviesti. IKT projekti var būt daļa no plašākām IKT vai darījumdarbības pārveides programmām.
Trešā persona	Organizācija, kas ir noslēgusi darījumdarbības attiecības vai līgumus ar darījumdarbības subjektu, lai tas nodrošinātu produktu vai pakalpojumu[3].
Informācijas aktīvs	Materiālas vai nemateriālas informācijas kopums, kuru ir vērts aizsargāt.
IKT aktīvs	Programmatūras vai aparatūras aktīvs, kas atrodams darījumdarbības vidē.
IKT sistēmas[4]	IKT struktūra, kas ietilpst finanšu iestādes darbības atbalsta mehānismā vai savienojošajā tīklā.
IKT pakalpojumi[5]	Pakalpojumi, kurus IKT sistēmas nodrošina vienam vai vairākiem iekšējiem vai ārējiem lietotājiem. Piemēram, datu ierakstīšanas, datu uzglabāšanas, datu apstrādes un ziņošanas pakalpojumi, kā arī uzraudzības, darījumdarbības un lēmumu pieņemšanas atbalsta pakalpojumi.

[3] Definīcija no G7 pamatelementiem trešo personu kiberdrošības riska pārvaldībai finanšu nozarē.
[4] Definīcija no pamatnostādnēm par kopējām procedūrām un metodoloģiju, ko izmanto uzraudzības pārskatīšanas un novērtēšanas procesā (SREP) (EBA/GL/2017/05).
[5] ibid.

Īstenošana

Piemērošanas datums

11. Šīs pamatnostādnes piemēro no 2020. gada 30. jūnija.

Atcelšana

12. Ar šīm pamatnostādnēm pamatnostādnes par drošības pasākumiem attiecībā uz operacionālajiem un drošības riskiem (EBA/GL/2017/17), kas izdotas 2017. gadā, tiks atceltas dienā, kad sāks piemērot šīs pamatnostādnes.

Pamatnostādnes par IKT un drošības risku pārvaldību

1.1. Proporcionalitāte

1. Visām finanšu iestādēm ir jāievēro šajās pamatnostādnēs izklāstītie noteikumi tādā veidā, kas samērīguma ziņā ir atbilstošs un ņemtu vērā finanšu iestāžu lielumu, iekšējo organizāciju, kā arī to pakalpojumu un produktu būtību, apjomu, sarežģītību un riska profilu, kurus finanšu iestādes nodrošina vai plāno piedāvāt.

1.2. Pārvaldība un stratēģija

1.2.1. Pārvaldība

2. Vadības struktūrai ir jānodrošina, ka finanšu iestādēm ir atbilstoša iekšējā pārvaldība un to IKT un drošības riskiem piemērota iekšējās kontroles sistēma. Vadības struktūrai ir jānosaka skaidras lomas un atbildība attiecībā uz IKT funkcijām, informācijas drošības riska pārvaldību un darbības nepārtrauktību, tostarp vadības struktūras un tās komiteju lomas un atbildība.
3. Vadības struktūrai ir jānodrošina, ka finanšu iestāžu darbinieku skaits un prasmes ir piemērotas, lai pastāvīgi atbalstītu to IKT operacionālās vajadzības un IKT un drošības riska pārvaldības procesus, kā arī nodrošinātu to IKT stratēģijas īstenošanu. Vadības struktūrai ir jānodrošina, ka piešķirtais budžets ir piemērots, lai izpildītu iepriekš minēto. Turklāt finanšu iestādēm ir jānodrošina, lai visi darbinieki, tostarp personas, kas pilda pamatfunkcijas, katru gadu vai, ja vajadzīgs, biežāk, saņemtu atbilstošu apmācību par IKT un drošības riskiem, tostarp par informācijas drošību (skatīt arī 1.4.7. iedaļu).

4. Vadības struktūrai ir vispārēja atbildība par finanšu iestāžu IKT stratēģijas noteikšanu, apstiprināšanu un pārraudzību kā daļu no to vispārējās darījumdarbības stratēģijas, kā arī par drošības risku un efektīvas IKT riska pārvaldības sistēmas izveidi.

1.2.2. Stratēģija

5. IKT stratēģijai vajadzētu būt saskaņotai ar finanšu iestāžu vispārējo darījumdarbības stratēģiju un ir jānosaka šādi jautājumi:

   a) kā ir jāattīstās finanšu iestāžu IKT, lai efektīvi atbalstītu un piedalītos to darījumdarbības stratēģijā, ietverot organizatoriskās struktūras attīstību, IKT sistēmas izmaiņas un būtiskos atkarības faktorus no trešām personām;
   b) plānotā stratēģija un IKT arhitektūras attīstība, ietverot būtiskos atkarības faktorus no trešām personām;
   c) skaidri informācijas drošības mērķi, koncentrējoties uz IKT sistēmām un IKT pakalpojumiem, personālu un procesiem.

6. Finanšu iestādēm ir jāizveido rīcības plānu kopumi, kuros ietverti pasākumi, kas jāveic, lai sasniegtu IKT stratēģijas mērķi. Par tiem jāpaziņo visam attiecīgajam personālam (tostarp līgumslēdzējiem un trešo personu – pakalpojumu sniedzējiem gadījumos, ja tas ir piemērojams un attiecināms). Rīcības plāni ir periodiski jāpārskata, lai nodrošinātu to atbilstību un piemērotību. Finanšu iestādēm ir arī jāizveido procesi, kas vajadzīgi, lai uzraudzītu un izmērītu to IKT stratēģijas īstenošanas efektivitāti.

1.2.3. Trešo personu – pakalpojumu sniedzēju izmantošana

7. Neskarot EBI pamatnostādnes par ārpakalpojumu izmantošanu (EBA/GL/2019/02) un PSD2 19. pantu, finanšu iestādēm ir jānodrošina riska mazināšanas pasākumu efektivitāte, kā noteikts to riska pārvaldības sistēmā, ietverot pasākumus, kas noteikti šajās pamatnostādnēs, ja maksājumu pakalpojumu un/vai IKT pakalpojumu un jebkuras darbības IKT sistēmu operacionālās funkcijas tiek nodotas ārpakalpojumiem, tostarp darījumdarbības subjektu grupas vienībām, vai arī ja tiek izmantotas trešās personas.

8. Lai nodrošinātu IKT pakalpojumu un IKT sistēmu nepārtrauktību, finanšu iestādēm ir jānodrošina, ka līgumos un pakalpojumu līmeņa vienošanās (gan parastos apstākļos, gan pakalpojumu pārtraukšanas gadījumā — skatīt arī 1.7.2. iedaļu) ar pakalpojumu sniedzējiem (ārpakalpojumu sniedzējiem, darījumdarbības subjektu grupas vienībām vai trešo personu pakalpojumu sniedzējiem) tiktu ietverta šāda informācija:

   a) atbilstoši un samērīgi ar informācijas drošību saistīti mērķi un pasākumi, tostarp tādas prasības kā minimālās kiberdrošības prasības; finanšu iestādes datu aprites cikla specifikācijas; jebkuras prasības attiecībā uz datu šifrēšanu, tīkla drošību un drošības uzraudzības procesiem un datu centru izvietojums;
   b) operacionālo un drošības incidentu apstrādes procedūras, tostarp eskalācija un ziņošana.

9. Finanšu iestādēm ir jāuzrauga šo pakalpojumu sniedzēju atbilstības līmenis un jāpārliecinās, ka tas ir atbilstīgs finanšu iestāžu drošības mērķiem, pasākumiem un darbības mērķiem.

1.3. IKT un drošības risku pārvaldības sistēma

1.3.1. Organizācija un mērķi

10. Finanšu iestādēm ir jāidentificē un jāpārvalda savi IKT un drošības riski. IKT funkcijai(-ām), kas atbild par IKT sistēmām, procesiem un drošības operācijām, vajadzētu būt piemērotiem procesiem un kontroles pasākumiem, lai nodrošinātu, ka visi riski tiek identificēti, analizēti, izmērīti, uzraudzīti, pārvaldīti, ziņoti un tiek turēti finanšu iestādes vēlmes uzņemties risku noteiktajās robežās vai ka projekti un sistēmas, ko tie piegādā, un to veiktās darbības atbilst ārējām un iekšējām prasībām.

11. Finanšu iestādēm kontroles funkcijai ir jāpiešķir atbildība par IKT un drošības risku pārvaldību un pārraudzību, ievērojot EBI pamatnostādņu par iekšējo pārvaldību (EBA/GL/2017/11) 19. iedaļas prasības. Finanšu iestādēm ir jānodrošina šīs kontroles funkcijas neatkarība un objektivitāte, pienācīgi nodalot to no IKT operāciju procesiem. Šai kontroles funkcijai vajadzētu būt tieši pakļautai vadības struktūrai un būt atbildīgai par IKT un drošības riska pārvaldības sistēmas stingras ievērošanas uzraudzību un kontroli. Tai ir jānodrošina, ka IKT un drošības riski tiek identificēti, izmērīti, novērtēti, pārvaldīti, uzraudzīti un paziņoti. Finanšu iestādēm ir jānodrošina, ka šī kontroles funkcija nav atbildīga par nekādu iekšējo revīziju.

    Iekšējā audita funkcijai, ievērojot uz risku balstītu pieeju, vajadzētu spēt patstāvīgi pārskatīt un sniegt objektīvu pārliecību par visām ar IKT un ar drošību saistīto finanšu iestādes darbību un vienību atbilstību finanšu iestādes politikai un procedūrām, kā arī ārējam prasībām, ievērojot EBI pamatnostādņu par iekšējo pārvaldību (EBA/GL/2017/11) 22. iedaļas prasības.

12. Lai IKT un drošības riska pārvaldības sistēma būtu efektīva, finanšu iestādēm ir jānosaka un jāsadala svarīgākās lomas un atbildība, kā arī attiecīgā pārskatu sniegšanas kārtība. Šī sistēma ir pilnībā jāintegrē un jāpieskaņo finanšu iestāžu vispārējiem riska pārvaldības procesiem.

13. IKT un drošības riska pārvaldības sistēmā ir jāietver procesi, kas ieviesti, lai:

    a) noteiktu vēlmi uzņemties IKT un drošības riskus saskaņā ar finanšu iestādes vēlmi uzņemties risku;
    b) identificētu un novērtētu IKT un drošības riskus, kuriem finanšu iestāde ir pakļauta;
    c) noteiktu risku mazināšanas pasākumus, tostarp kontroles pasākumus, lai mazinātu IKT un drošības riskus;
    d) pārraudzītu šo pasākumu efektivitāti, kā arī paziņoto incidentu skaitu, MPS gadījumā ietverot incidentus, par kuriem paziņots saskaņā ar PSD2 96. pantu un kuri ietekmē ar IKT saistītas darbības, un vajadzības gadījumā rīkotos, lai koriģētu šos pasākumus;
    e) ziņotu vadības struktūrai par IKT un drošības riskiem un kontroles pasākumiem;
    f) identificētu un novērtētu, vai pastāv kādi IKT un drošības riski, kas saistīti ar jebkādām būtiskām izmaiņām IKT sistēmā vai IKT pakalpojumos, procesos vai procedūrās, un/vai pēc nozīmīgiem operacionālajiem vai drošības incidentiem.

14. Finanšu iestādēm ir jānodrošina, ka IKT un drošības risku pārvaldības sistēma tiek dokumentēta un informācija tiek pastāvīgi uzlabota, pamatojoties uz gūtajām atziņām, kas uzkrātas sistēmas īstenošanas un uzraudzības gaitā. Vadības struktūrai vismaz reizi gadā ir jāapstiprina un jāpārskata IKT un drošības riska pārvaldības sistēma.

1.3.2. Funkciju, procesu un aktīvu identifikācija

15. Finanšu iestādēm ir jāidentificē, jāizveido un jāuztur atjaunināta to darījumdarbības funkciju, lomu un atbalsta procesu kartēšana, lai katrai no tām identificētu nozīmīgumu un to savstarpējās atkarības faktorus, kas saistīti ar IKT un drošības riskiem.

16. Turklāt finanšu iestādēm ir jāidentificē, jāizveido un jāuztur atjaunināta to aktīvu kartēšana, kas atbalsta to darījumdarbības funkcijas un atbalsta procesus, piemēram, IKT sistēmas, personālu, darbuzņēmējus, trešās personas un atkarības faktorus no citām iekšējām un ārējām sistēmām un procesiem, lai varētu vismaz pārvaldīt informācijas aktīvus, kas atbalsta viņu kritiski svarīgās darījumdarbības funkcijas un procesus.

1.3.3. Klasifikācija un riska novērtējums

17. Finanšu iestādēm ir jāklasificē noteiktās darījumdarbības funkcijas, atbalsta procesi un informācijas aktīvi, kas minēti 15. un 16. punktā, pēc to kritiskā svarīguma.

18. Lai noteiktu šo identificēto darījumdarbības funkciju, atbalsta procesu un informācijas aktīvu kritisko svarīgumu, finanšu iestādēm ir jāņem vērā vismaz konfidencialitātes, integritātes un pieejamības prasības. Ir skaidri jānosaka pārskatatbildība un atbildība par informācijas aktīviem.

19. Veicot riska novērtējumu, finanšu iestādēm ir jāpārbauda informācijas aktīvu un saistošās dokumentācijas klasifikācijas piemērotība.

20. Finanšu iestādēm ir jāidentificē IKT un drošības riski, kas ietekmē identificētās un klasificētās darījumdarbības funkcijas, atbalstot procesus un informācijas aktīvus atbilstoši to kritiskajam svarīgumam. Šāds riska novērtējums ir jāveic un jādokumentē katru gadu vai īsākos starplaikos, ja vajadzīgs. Šādi riska novērtējumi jāveic arī attiecībā uz visām būtiskām izmaiņām infrastruktūrā, procesos vai procedūrās, kas ietekmē darījumdarbības funkcijas, atbalsta procesus vai informācijas aktīvus, un tāpēc kārtējais finanšu iestāžu riska novērtējums ir jāatjaunina.

21. Finanšu iestādēm ir jānodrošina, ka tās pastāvīgi uzrauga apdraudējumu un ievainojamības faktorus, kuri attiecas uz to darījumdarbības procesiem, atbalsta funkcijām un informācijas aktīviem, un regulāri jāpārskata riska scenāriji, kas tos ietekmē.

1.3.4. Riska mazināšana

22. Pamatojoties uz riska novērtējumiem, finanšu iestādēm ir jānosaka, kādi pasākumi ir vajadzīgi identificēto IKT un drošības risku mazināšanai līdz pieņemamam līmenim un vai ir vajadzīgas izmaiņas esošajos darījumdarbības procesos, kontroles pasākumos, IKT sistēmās un IKT pakalpojumos. Finanšu iestādei ir jāapsver laiks, kas vajadzīgs šo izmaiņu īstenošanai, un laiks, lai veiktu atbilstošus risku mazinošus pagaidu pasākumus, lai samazinātu IKT un drošības riskus,

kas ļautu saglabāt atbilstību finanšu iestādes noteiktajām IKT un drošības vēlmes uzņemties risku robežām.

23. Finanšu iestādēm ir jānosaka un jāīsteno pasākumi identificēto IKT un drošības risku mazināšanai un informācijas aktīvu aizsardzībai atbilstoši to klasifikācijai.

1.3.5. Ziņošana

24. Finanšu iestādēm ir skaidri un savlaicīgi jāziņo vadības struktūrai par riska novērtējuma rezultātiem. Šāda ziņošana neskar MPS pienākumu sniegt kompetentajām iestādēm atjauninātu un visaptverošu riska novērtējumu, kā noteikts Direktīvas (ES) 2015/2366 95. panta 2. punktā.

1.3.6. Revīzija

25. Revidentiem, kuriem ir pietiekamas zināšanas, prasmes un zināšanas par IKT un drošības riskiem un maksājumiem (attiecībā uz MPS), finanšu iestādes pārvaldība, sistēmas un procesi ir periodiski jāpārbauda attiecībā uz IKT un drošības riskiem, lai vadības struktūrai sniegtu neatkarīgu apliecinājumu par to efektivitāti. Revidentiem jābūt neatkarīgiem finanšu iestādes ietvaros vai neatkarīgiem no tās. Šādu revīziju biežumam un mērķim vajadzētu būt samērīgiem ar attiecīgajiem IKT un drošības riskiem.

26. Finanšu iestādes vadības struktūrai ir jāapstiprina revīzijas plāns, ietverot visas IKT revīzijas un visas būtiskās izmaiņas tajā. Revīzijas plānam un tā izpildei, ietverot revīzijas biežumu, ir jāatspoguļo finanšu iestādei raksturīgajiem IKT un drošības riskiem un jābūt samērīgiem ar tiem, un tas ir regulāri jāatjaunina.

27. Ir jāizveido oficiāls pārraudzības process, kas ietver noteikumus par kritiski svarīgo IKT revīzijas konstatējumu savlaicīgu pārbaudi un novēršanu.

1.4. Informācijas drošība

1.4.1. Informācijas drošības politika

28. Finanšu iestādēm ir jāizstrādā un jādokumentē informācijas drošības politika, kurā ir jānosaka augsta līmeņa principi un noteikumi, lai aizsargātu finanšu iestāžu un to klientu datu un informācijas konfidencialitāti, integritāti un pieejamību. MPS šī politika ir noteikta drošības politikas dokumentā, kas jāpieņem saskaņā ar Direktīvas (ES) 2015/2366 5. panta 1. punkta j) apakšpunktu. Informācijas drošības politikai jāatbilst finanšu iestādes informācijas drošības mērķiem un jāpamatojas uz attiecīgajiem riska novērtēšanas procesa rezultātiem. Šī politika ir jāapstiprina vadības struktūrai.

29. Šajā politikā ir jāiekļauj informācijas drošības pārvaldības galveno lomu un atbildības apraksts, un tajā ir jāizklāsta prasības darbiniekiem un darbuzņēmējiem, procesiem un tehnoloģijām attiecībā uz informācijas drošību, nosakot, ka visu līmeņu darbiniekiem un darbuzņēmējiem ir pienākums nodrošināt finanšu iestāžu informācijas drošību. Politikai ir jānodrošina konfidencialitāte, integritāte un pieejamība attiecībā uz finanšu iestāžu kritiski svarīgajiem

loģiskajiem un fiziskajiem aktīviem, resursiem un sensitīvajiem datiem, kas var būt neaktīvi dati, pārsūtīšanas procesā vai aktīvā lietojumā esoši dati. Informācijas drošības politika ir jāpaziņo visiem finanšu iestādes darbiniekiem un darbuzņēmējiem.

30. Pamatojoties uz informācijas drošības politiku, finanšu iestādēm ir jāizveido un jāīsteno drošības pasākumi, lai mazinātu IKT un drošības riskus, kuriem tās ir pakļautas. Minētajiem pasākumiem jāietver šādi aspekti:

    a) organizācija un pārvaldība saskaņā ar 10. un 11. punktu;
    b) loģiskā drošība (1.4.2. iedaļa);
    c) fiziskā drošība (1.4.3. iedaļa);
    d) IKT operāciju drošība (1.4.4. iedaļa);
    e) drošības uzraudzība (1.4.5. iedaļa);
    f) informācijas drošības pārskati, novērtējums un pārbaude (1.4.6. iedaļa);
    g) apmācība un izpratne par informācijas drošību (1.4.7. iedaļa).

1.4.2. Loģiskā drošība

31. Finanšu iestādēm ir jānosaka, jādokumentē un jāīsteno procedūras loģiskai piekļuves kontrolei (identitātes un piekļuves pārvaldībai). Šīs procedūras ir jāīsteno, jāpiemēro, jāuzrauga un periodiski jāpārskata. Procedūrās ir jāiekļauj arī kontroles pasākumi noviržu uzraudzībai. Šajās procedūrās ir jāīsteno vismaz šādi elementi, ja termins "lietotājs" ietver arī tehniskos lietotājus:

    (a) **Nepieciešamība zināt, mazākā privilēģija un pienākumu nošķiršana:** finanšu iestādēm ir jāpārvalda piekļuves tiesības informācijas aktīviem un to atbalsta sistēmām, pamatojoties uz "nepieciešamību zināt", ietverot attālinātu piekļuvi. Lietotājiem ir jāpiešķir minimālās piekļuves tiesības, kas ir nepārprotami nepieciešamas viņu pienākumu veikšanai ("mazāko privilēģiju" princips), t. i, lai novērstu nepamatotu piekļuvi lielai datu kopai vai novērstu piekļuves tiesību kombināciju piešķiršanu, ko var izmantot, lai apiet kontroles pasākumus ("pienākumu nošķiršanas" princips).
    (b) **Lietotāju pārskatatbildība:** finanšu iestādēm cik vien iespējams jāierobežo vispārēju lietotāju kontu un kopīgi lietotu kontu izmantošana un jānodrošina, ka lietotājus var identificēt attiecībā uz darbībām, kas tiek veiktas IKT sistēmās.
    (c) **Privileģētas piekļuves tiesības:** finanšu iestādēm jāīsteno stingri kontroles pasākumi attiecībā uz privileģētu piekļuvi sistēmai, stingri ierobežojot un cieši uzraugot kontus ar paaugstinātām piekļuves tiesībām sistēmai (piemēram, administratora kontus). Lai nodrošinātu drošu saziņu un samazinātu risku, attālinātā administratīvā piekļuve kritiski svarīgām IKT sistēmām ir jāpiešķir tikai, pamatojoties uz "nepieciešamību zināt", un, ja tiek izmantoti spēcīgi autentifikācijas risinājumi.
    (d) **Lietotāju darbību reģistrēšana:** jāreģistrē un jāuzrauga vismaz visas privileģēto lietotāju veiktās darbības. Piekļuves žurnāli jāglabā, lai novērstu neatļautu datu modifikāciju vai dzēšanu, un to glabāšanas ilgumam vajadzētu būt atbilstīgam konstatēto darbības funkciju, atbalsta procesu un informācijas aktīvu kritiskumam saskaņā ar 1.3.3. iedaļu, neskarot ES un valsts tiesību aktos noteiktās saglabāšanas prasības. Finanšu iestādei

jāizmanto šī informācija, lai sekmētu maksājumu pakalpojumu nodrošināšanā konstatēto netipisku darbību identifikāciju un izmeklēšanu.

(e) **Piekļuves pārvaldība:** piekļuves tiesības jāpiešķir, jāatsauc vai jāmaina savlaicīgi saskaņā ar iepriekš noteiktām apstiprinājuma darbplūsmām, kurās iesaistīts piekļuves mērķa informācijas darījumdarbības īpašnieks (informācijas aktīva īpašnieks). Darba attiecību pārtraukšanas gadījumā piekļuves tiesības nekavējoties jāatceļ.

(f) **Piekļuves atkārtota apstiprināšana:** piekļuves tiesības periodiski jāpārskata, lai pārliecinātos, ka lietotājiem nav pārmērīgu privilēģiju un ka piekļuves tiesības tiek atsauktas, kad tās vairs nav vajadzīgas.

(g) **Autentifikācijas metodes:** finanšu iestādēm jāīsteno autentifikācijas metodes, kas ir pietiekami spēcīgas, lai atbilstoši un efektīvi nodrošinātu atbilstību piekļuves kontroles politikai un procedūrām. Autentifikācijas metodēm vajadzētu būt samērīgām ar IKT sistēmu, informācijas vai piekļuves procesa kritisko svarīgumu. Tam vismaz jāietver sarežģītas paroles vai spēcīgākas autentifikācijas metodes (piemēram, tādu kā divu faktoru autentifikācija), pamatojoties uz attiecīgu risku.

32. Lietojumprogrammu elektroniskā piekļuve datiem un sistēmām jāierobežo līdz minimālajam līmenim, kas nepieciešams attiecīgā pakalpojuma nodrošināšanai.

1.4.3. Fiziskā drošība

33. Finanšu iestādēm ir jānosaka, jādokumentē un jāīsteno finanšu iestāžu fiziskās drošības pasākumi, lai aizsargātu savas telpas, datu centrus un sensitīvās zonas no neatļautas piekļuves un no apkārtējās vides apdraudējuma.

34. Fizisku piekļuvi IKT sistēmām jāatļauj tikai atļauju saņēmušām personām. Atļauja jāpiešķir saskaņā ar personas uzdevumiem un pienākumiem, un — tikai personām, kas ir atbilstīgi apmācītas un uzraudzītas. Fiziskā pieeja ir regulāri jāpārskata, lai nodrošinātu, ka nevajadzīgas piekļuves tiesības tiek nekavējoties atsauktas, kad tās vairs nav vajadzīgas.

35. Pienācīgiem pasākumiem aizsardzībai pret vides apdraudējumiem vajadzētu būt samērīgiem ar ēku nozīmi un šajās ēkās izvietoto operāciju vai IKT sistēmu kritisko svarīgumu.

1.4.4. IKT operāciju drošība

36. Finanšu iestādēm jāīsteno procedūras, lai novērstu drošības problēmu rašanos IKT sistēmās un IKT pakalpojumos, un pēc iespējas jāsamazina to ietekme uz IKT pakalpojumu nodrošināšanu. Šajās procedūrās ir jāietver šādi pasākumi:

a) potenciālo ievainojamību identificēšana, kuras ir jānovērtē un jānovērš, nodrošinot mūsdienīgas programmatūras un aparatūras, tostarp programmatūras, ko finanšu iestādes nodrošina saviem iekšējiem un ārējiem lietotājiem, paredzot kritiski svarīgus drošības “programmatūras ielāpus” vai ieviešot kompensējošus kontroles pasākumus;

b) visu tīkla komponentu drošas konfigurācijas bāzes līniju īstenošana;

c) tīkla segmentēšanas, datu zudumu novēršanas sistēmu un tīkla plūsmas šifrēšanas īstenošana (saskaņā ar datu klasifikāciju);

d) beigupunktu, tostarp serveru, darbstaciju un mobilo ierīču, aizsardzības īstenošana; finanšu iestādēm jānovērtē, vai parametri atbilst drošības standartiem, kurus tās noteikušas, pirms tām piešķir piekļuvi korporatīvajam tīklam;
e) pasākumi, kas nodrošina, ka tiek ieviesti mehānismi programmatūras, aparatūras un datu integritātes pārbaudei;
f) datu, kas ir neaktīvi dati, datu pārsūtīšanas procesā vai aktīvā lietojumā esošu datu šifrēšana (saskaņā ar datu klasifikāciju).

37. Turklāt finanšu iestādēm ir pastāvīgi jānosaka, vai izmaiņas esošajā darbības vidē ietekmē esošos drošības pasākumus, vai jāpieņem papildu pasākumi, lai atbilstoši mazinātu saistītos riskus. Šīm izmaiņām ir jāiekļaujas finanšu iestāžu formālo izmaiņu vadības procesā, kam ir jānodrošina, ka izmaiņas tiek pareizi plānotas, pārbaudītas, dokumentētas, atļautas un ieviestas.

1.4.5. Drošības uzraudzība

38. Finanšu iestādēm ir jāizveido un jāīsteno politika un procedūras, lai atklātu novirzes, kas var ietekmēt finanšu iestāžu informācijas drošību, un atbilstoši reaģētu uz šiem notikumiem. Šīs pastāvīgās uzraudzības ietvaros finanšu iestādēm ir jāīsteno atbilstīgas un efektīvas iespējas, kas ļautu konstatēt un paziņot par fizisku vai loģisku ielaušanos, kā arī pārkāpumiem attiecībā uz konfidencialitāti, integritāti un informācijas aktīvu pieejamību. Pastāvīgas uzraudzības un noteikšanas procesos ir jāietver šādi aspekti:

a) būtiski iekšējie un ārējie faktori, tostarp darījumdarbības un IKT administratīvās funkcijas;
b) darījumi, lai atklātu trešo personu vai citu subjektu piekļuves ļaunprātīgu izmantošanu un piekļuves iekšēju ļaunprātīgu izmantošanu;
c) iespējamie iekšējie un ārējie apdraudējumi.

39. Finanšu iestādēm ir jāizstrādā un jāīsteno procesi un organizatoriskās struktūras, lai noteiktu un pastāvīgi uzraudzītu drošības apdraudējumus, kas varētu būtiski ietekmēt to spējas nodrošināt pakalpojumus. Finanšu iestādēm ir aktīvi jāuzrauga tehnoloģiskā attīstība, lai nodrošinātu to, ka tie ir informēti par drošības riskiem. Finanšu iestādēm ir jāīsteno noteikšanas pasākumi, piemēram, lai konstatētu iespējamo informācijas noplūdi, ļaunprātīgu kodu un citus drošības apdraudējumus un publiski zināmas ievainojamības attiecībā uz programmatūru un aparatūru, kā arī ir jāpārliecinās par atbilstīgiem jauniem drošības atjauninājumiem.

40. Drošības uzraudzības procesam vajadzētu arī palīdzēt finanšu iestādei izprast operacionālo vai drošības incidentu būtību, noteikt tendences un atbalstīt organizācijas izmeklēšanu.

1.4.6. Informācijas drošības pārskati, novērtējums un pārbaude

41. Finanšu iestādēm ir jāveic dažādi informācijas drošības pārskati, novērtējumi un pārbaudes, lai nodrošinātu savu IKT sistēmu un IKT pakalpojumu ievainojamības aspektu identificēšanu. Piemēram, finanšu iestādes var veikt atbilstības analīzi, izmantojot salīdzinājumu ar informācijas drošības standartiem, atbilstības pārskatus, informācijas sistēmu iekšējās un ārējās revīzijas vai fiziskās drošības pārskatus. Turklāt iestādei vajadzētu apsvērt izmantot

paraugprakses piemērus, piemēram, avota koda pārskatus, ievainojamības novērtējumus, iespiešanās testus un "sarkanās komandas" pārbaudes.

42. Finanšu iestādēm ir jāizveido un jāievieš informācijas drošības testēšanas sistēma, kas apstiprinātu to informācijas drošības pasākumu stabilitāti un efektivitāti, un ir jānodrošina, ka šajā sistēmā tiek ņemti vērā apdraudējumi un ievainojamības faktori, kas identificēti, izmantojot apdraudējumu uzraudzību un IKT un drošības risku novērtēšanas procesu.

43. Informācijas drošības pārbaužu sistēmai ir jānodrošina, ka pārbaudes:

    a) veic neatkarīgi testētāji ar pietiekamām zināšanām, prasmēm un kompetenci informācijas drošības pasākumu pārbaudē un kuri nav iesaistīti informācijas drošības pasākumu izstrādē;
    b) ietver ievainojamības skenēšanu un iespiešanās testus (tostarp apdraudējumu iniciētu iespiešanās testēšanu, ja tas ir vajadzīgs un ir lietderīgi), kas ir proporcionāli ar darījumdarbības procesiem un sistēmām noteiktajam riska līmenim.

44. Finanšu iestādēm ir jāveic pastāvīgas un atkārtotas drošības pasākumu pārbaudes. Visām kritiski svarīgajām IKT sistēmām (17. punkts) šīs pārbaudes ir jāveic vismaz reizi gadā, un attiecībā uz MPS tās būs daļa no visaptveroša novērtējuma drošības riska veidiem, kas saistīti ar viņu nodrošinātajiem maksājumu pakalpojumiem, kā paredzēts saskaņā ar PSD2 95. panta 2. punktu. Sistēmas, kas nav kritiski svarīgas, ir jāpārbauda regulāri, izmantojot uz risku balstītu pieeju, bet ne retāk kā reizi trīs gados.

45. Finanšu iestādēm ir jānodrošina, ka drošības pasākumu pārbaudes tiek veiktas gadījumos, kad notiek izmaiņas infrastruktūrā, procesos vai procedūrās un ja izmaiņas tiek veiktas nopietnu operacionālo vai drošības incidentu dēļ, vai arī tādēļ, ka tirgū tiek laistas jaunas vai būtiski mainītas, ar internetu saistītas kritiski svarīgas lietojumprogrammas.

46. Finanšu iestādēm ir jāuzrauga un jāizvērtē drošības pārbaužu rezultāti un attiecīgi jāatjaunina savi drošības pasākumi atbilstošā veidā un bez nepamatotas kavēšanās attiecībā uz kritiski svarīgām IKT sistēmām.

47. Attiecībā uz MPS pārbaužu sistēmā ir jāietver arī drošības pasākumi, kas attiecas uz (1) maksājumu termināliem un ierīcēm, ko izmanto maksājumu pakalpojumu nodrošināšanai, (2) maksājumu termināliem un ierīcēm, ko izmanto maksājumu pakalpojumu lietotāju (MPL) autentifikācijai, un (3) ierīcēm un programmatūru, ar ko MPS nodrošina MPL, lai izveidotu/saņemtu autentifikācijas kodu.

48. Pamatojoties uz novērotajiem drošības apdraudējumiem un veiktajām izmaiņām, ir jāveic testēšana nolūkā ietvert būtisku un zināmu iespējamo uzbrukumu scenārijus.

1.4.7. Informācijas drošības apmācība un informētība

49. Finanšu iestādēm ir jāizstrādā apmācības programma visiem darbiniekiem un darbuzņēmējiem, tostarp periodiskas drošības izpratnes programmas, lai nodrošinātu, ka viņi ir apmācīti veikt savus pienākumus un atbildīgos uzdevumus saskaņā ar attiecīgo drošības politiku un attiecīgajām procedūrām, lai mazinātu cilvēku kļūdas, zādzības, krāpšanu, ļaunprātīgu izmantošanu vai zaudējumus, un jautājumos, kā novērst ar drošību saistītos riskus. Finanšu

iestādēm ir jānodrošina, ka apmācības programmā ir paredzēts sniegt apmācību visiem darbiniekiem un darbuzņēmējiem vismaz reizi gadā.

1.5. IKT operāciju pārvaldība

50. Finanšu iestādēm ir jāpārvalda savas IKT operācijas, pamatojoties uz dokumentētiem un ieviestiem procesiem un procedūrām (kas attiecībā uz MPS ietver drošības politikas dokumentu saskaņā ar PSD2 5. panta 1. punkta j) apakšpunktu), ko apstiprinājusi vadības struktūra. Šajā dokumentu kopumā ir jānosaka, kā finanšu iestādes darbojas, uzrauga un kontrolē savas IKT sistēmas un pakalpojumus, ietverot kritiski svarīgo IKT operāciju dokumentēšanu, un tiem ir jānodrošina, ka finanšu iestādes uztur atjauninātu IKT aktīvu uzskaiti.

51. Finanšu iestādēm ir jānodrošina, lai to IKT operācijas tiktu veiktas atbilstoši to darījumdarbības prasībām. Finanšu iestādēm ir jāuztur un pēc iespējas jāuzlabo savu IKT operāciju efektivitāte, ietverot, bet ne tikai, nepieciešamību apsvērt, kā samazināt iespējamās kļūdas, kas rodas manuālo uzdevumu izpildes rezultātā.

52. Finanšu iestādēm ir jāievieš reģistrēšanas un uzraudzības procedūras kritiski svarīgām IKT operācijām, kas ļautu atklāt, analizēt un labot kļūdas.

53. Finanšu iestādēm ir jāuztur atjaunināta savu IKT aktīvu uzskaite (ietverot IKT sistēmas, tīkla ierīces, datubāzes utt.). IKT aktīvu uzskaitē vajadzētu saglabāt IKT aktīvu konfigurāciju un dažādu IKT aktīvu saites un savstarpējo atkarību, lai nodrošinātu pareizu konfigurācijas un izmaiņu pārvaldības procesu.

54. IKT aktīvu uzskaitei vajadzētu būt pietiekami detalizētai, lai varētu ātri identificēt IKT aktīvu, tā atrašanās vietu, drošības klasifikāciju un īpašumtiesības. Aktīvu savstarpējā atkarība ir jādokumentē, lai palīdzētu reaģēt uz drošības un operatīvajiem incidentiem, tostarp kiberuzbrukumiem.

55. Finanšu iestādēm ir jāuzrauga un jāpārvalda IKT aktīvu aprites cikli, lai nodrošinātu, ka tie arvien ir atbilstīgi un atbalsta darījumdarbības un risku pārvaldības prasības. Finanšu iestādēm ir jāuzrauga, vai to IKT aktīvus atbalsta ārējie vai iekšējie pārdevēji un izstrādātāji un vai visi attiecīgie programmatūras ielāpi un jauninājumi tiek piemēroti, pamatojoties uz dokumentētiem procesiem. Ir jānovērtē un jāsamazina riski, ko rada novecojuši vai neatbalstīti IKT aktīvi.

56. Finanšu iestādēm ir jāīsteno veiktspējas un jaudas plānošanas un uzraudzības procesi, lai savlaicīgi novērstu, atklātu un reaģētu uz svarīgiem IKT sistēmu veiktspējas jautājumiem un IKT jaudas trūkumu.

57. Finanšu iestādēm ir jānosaka un jāievieš datu un IKT sistēmu dublēšanas un atjaunošanas procedūras, lai nodrošinātu, ka datus var atgūt pēc vajadzības. Dublējumu apjoms un biežums ir jānosaka atbilstoši darījumdarbības atjaunošanas prasībām un datu un IKT sistēmu kritiskajam svarīgumam un jānovērtē saskaņā ar veikto riska novērtējumu. Ir periodiski jāveic dublēšanas un atjaunošanas procedūru pārbaude.

58. Finanšu iestādēm ir jānodrošina, ka datu un IKT sistēmu dublējumi tiek glabāti droši un pietiekami tālu no primārās vietas, lai tie netiktu pakļauti tiem pašiem riskiem.

3.5.1 IKT incidentu un problēmu pārvaldība

59. Finanšu iestādēm ir jāizveido un jāīsteno incidentu un problēmu pārvaldības process, lai uzraudzītu un reģistrētu operatīvos un drošības IKT incidentus un kas dotu iespēju finanšu iestādēm savlaicīgi turpināt vai atsākt kritiski svarīgās darījumdarbības funkcijas un procesus gadījumos, kad rodas traucējumi. Finanšu iestādēm ir jānosaka piemēroti kritēriji un robežvērtības, lai notikumus klasificētu kā operacionālo vai drošības incidentus, kā noteikts šo pamatnostādņu iedaļā "Definīcijas", kā arī agrīnas brīdināšanas rādītāji, kam jābrīdina, lai dotu iespēju agrīni atklāt šos incidentus. Šādi MPS kritēriji un sliekšņi neskar būtisku incidentu klasifikāciju saskaņā ar PSD2 96. pantu un pamatnostādnēm paziņošanai par būtiskiem incidentiem saskaņā ar PSD2 (EBA/GL/2017/10).

60. Lai samazinātu nelabvēlīgu notikumu ietekmi un ļautu savlaicīgi atgūt datus, finanšu iestādēm ir jāizveido piemēroti procesi un organizatoriskās struktūras, kas nodrošinātu konsekventu un integrētu operacionālo un drošības incidentu uzraudzību, pārvaldību un kontroli un pārliecinātos, ka cēloņi tiek identificēti un likvidēti nolūkā novērst atkārtotu incidentu rašanos. Incidentu un problēmu pārvaldības procesā vajadzētu noteikt:

    a) procedūras, lai identificētu, izsekotu, reģistrētu, klasificētu un klasificētu incidentus pēc to prioritātēm, pamatojoties uz darījumdarbības kritisko svarīgumu;
    b) lomas un atbildību dažādiem incidentu scenārijiem (piemēram, kļūdas, darbības traucējumi, kiberuzbrukumi);
    c) problēmu pārvaldības procedūras, lai identificētu, analizētu un atrisinātu viena vai vairāku incidentu pamatcēloni — finanšu iestādei ir jāanalizē operacionālie vai drošības incidenti, kas varētu ietekmēt finanšu iestādi un kuri ir identificēti vai notikuši organizācijā un/vai ārpus tās, un ir jāapsver nozīmīgākā pieredze, kas gūta šajās analīzēs, un attiecīgi jāatjaunina drošības pasākumi;
    d) efektīvus iekšējās saziņas plānus, ietverot paziņojumus par incidentiem un eskalācijas procedūras — arī attiecībā uz klientu sūdzībām, kas saistītas ar drošību, lai nodrošinātu, ka:
        i) par incidentiem, kas, iespējams, ļoti nelabvēlīgi ietekmē kritiski svarīgās IKT sistēmas un IKT pakalpojumus, tiek ziņots attiecīgajai augstākajai vadībai un IKT augstākajai vadībai;
        ii) vadības struktūra tiek *ad hoc* informēta nopietnu incidentu gadījumā un vismaz tiek informēta par ietekmi, reaģēšanu un papildu kontroles pasākumiem, kas jānosaka incidentu rezultātā;
    e) procedūras reaģēšanai uz incidentiem, lai mazinātu ar incidentiem saistīto ietekmi un nodrošinātu, ka pakalpojums laikus kļūst pieejams un ir drošs;
    f) īpašus ārējās saziņas plānus kritiski svarīgām darījumdarbības funkcijām un procesiem, lai:
        i) sadarbotos ar attiecīgajām ieinteresētajām personām nolūkā efektīvi reaģēt uz incidentu un atgūt tā radītos zaudējumus;

ii) savlaicīgi sniegtu informāciju ārējām personām (piemēram, klientiem, citiem tirgus dalībniekiem, uzraudzības iestādei) attiecīgā gadījumā un saskaņā ar piemērojamiem noteikumiem.

1.6. IKT projektu un izmaiņu vadība

1.6.1. IKT projektu vadība

61. Lai efektīvi atbalstītu IKT stratēģijas īstenošanu, finanšu iestādei ir jāīsteno programma un/vai projekta vadības process, kurā noteiktas lomas, atbildība un pārskatatbildība.

62. Finanšu iestādei ir pienācīgi jāuzrauga un jāsamazina riski, kas rodas no to IKT projektu portfeļa (programmu vadība), ņemot vērā arī riskus, kas var rasties dažādu projektu savstarpējas atkarības faktoru dēļ un vairāku projektu atkarības faktoru dēļ no tiem pašiem resursiem un/vai kompetences.

63. Finanšu iestādei ir jāizveido un jāīsteno IKT projektu vadības politika, kurā tiktu ietverti vismaz:

    a) projekta mērķi;
    b) lomas un atbildība;
    c) projekta risku novērtējums;
    d) projekta plāns, laika grafiks un posmi;
    e) svarīgākie atskaites punkti;
    f) izmaiņu pārvaldības prasības.

64. IKT projektu vadības politikai ir jānodrošina, ka informācijas drošības prasības analizē un apstiprina funkcija, kas ir neatkarīga no izstrādes funkcijas.

65. Finanšu iestādei ir jānodrošina, ka visas jomas, kuras ietekmē IKT projekts, tiek pārstāvētas projekta komandā un ka projekta komandai ir nepieciešamās zināšanas, lai nodrošinātu drošu un veiksmīgu projekta īstenošanu.

66. Par IKT projektu izveidi un progresu un ar tiem saistītajiem riskiem ir jāziņo vadības struktūrai gan atsevišķi, gan projektus apkopojot, atkarībā no IKT projektu nozīmīguma un lieluma, pēc vajadzības gan regulāri, gan *ad hoc* veidā. Finanšu iestādēm savā riska pārvaldības sistēmā ir jāiekļauj projekta risks.

1.6.2. IKT sistēmu iegāde un attīstība

67. Finanšu iestādēm ir jāizstrādā un jāievieš process, kas reglamentē IKT sistēmu iegādi, izstrādi un uzturēšanu. Šis process ir jāizstrādā, izmantojot uz risku balstītu pieeju.

68. Finanšu iestādei ir jānodrošina, ka pirms jebkādas IKT sistēmu iegādes vai izstrādes funkcionālās un nefunkcionālās prasības (tostarp informācijas drošības prasības) ir skaidri definētas un tās apstiprinājusi attiecīgā darījumdarbības vadība.

69. Finanšu iestādei ir jānodrošina, ka tiek veikti pasākumi, lai izstrādes un ieviešanas laikā ražošanas vidē mazinātu IKT sistēmu nejaušas izmaiņas vai ar nodomu veiktu manipulāciju risku.

70. Finanšu iestādēm vajadzētu būt ieviestai metodoloģijai IKT sistēmu pārbaudei un apstiprināšanai pirms to sākotnējās izmantošanas. Šajā metodoloģijā ir jāņem vērā darījumdarbības procesu un aktīvu kritiskais svarīgums. Pārbaudei ir jānodrošina, ka jaunās IKT sistēmas darbojas kā paredzēts. Tām ir arī jāizmanto testēšanas vide, kas atbilstoši atspoguļo ražošanas vidi.

71. Finanšu iestādēm ir jāpārbauda IKT sistēmas, IKT pakalpojumi un informācijas drošības pasākumi, lai identificētu iespējamās drošības nepilnības, pārkāpumus un incidentus.

72. Finanšu iestādei ir jāīsteno atsevišķas IKT vides, lai nodrošinātu pienācīgu pienākumu nodalīšanu un mazinātu nepārbaudītu ražošanas sistēmu izmaiņu ietekmi. Konkrēti, finanšu iestādei ir jānodrošina ražošanas vides nodalīšana no izstrādes, testēšanas un citas vides, kas nav saistīta ar ražošanu. Finanšu iestādei ir jānodrošina ražošanas datu integritāte un konfidencialitāte vidē, kurā notiek ražošana. Ražošanas datiem piekļuve ir tikai pilnvarotiem lietotājiem.

73. Finanšu iestādēm ir jāīsteno pasākumi, lai aizsargātu iekšēji izstrādāto IKT sistēmu pirmkodu integritāti. Tām ir arī visaptveroši jādokumentē ISKT sistēmu izstrāde, ieviešana, darbība un/vai konfigurēšana, lai samazinātu nevajadzīgu atkarību no attiecīgo jomu ekspertiem. IKT sistēmas dokumentācijā attiecīgā gadījumā ir jāietver vismaz lietotāja dokumentācija, tehniskās sistēmas dokumentācija un darbības procedūras.

74. Finanšu iestādes procesi IKT sistēmu iegādei un izstrādei ir jāpiemēro arī attiecībā uz IKT sistēmām, kuras izstrādā vai pārvalda darījumdarbības funkcijas galalietotāji ārpus IKT organizācijas (piemēram, galalietotāju skaitļošanas lietojumprogrammas), izmantojot uz risku balstītu pieeju. Finanšu iestādei ir jāuztur tādu lietojumprogrammu reģistrs, kuras atbalsta kritiski svarīgas darījumdarbības funkcijas vai procesus.

1.6.3. IKT izmaiņu pārvaldība

75. Finanšu iestādēm ir jāizveido un jāievieš IKT izmaiņu pārvaldības process, lai nodrošinātu, ka visas izmaiņas IKT sistēmās tiek reģistrētas, pārbaudītas, novērtētas, apstiprinātas, īstenotas un pārbaudītas kontrolētā veidā. Finanšu iestādēm veicot izmaiņas ārkārtas situācijās (t. i., izmaiņas, kas jāievieš pēc iespējas ātrāk), vajadzētu ievērot procedūras, kas nodrošina atbilstošus aizsardzības pasākumus.

76. Finanšu iestādēm ir jānosaka, vai izmaiņas esošajā darbības vidē ietekmē esošos drošības pasākumus, vai jāpieņem papildu pasākumi, lai mazinātu saistītos riskus. Šīm izmaiņām vajadzētu būt saskaņā ar finanšu iestāžu oficiālo izmaiņu pārvaldības procesu.

1.7. Darbības nepārtrauktības pārvaldība

77. Finanšu iestādēm ir jāizveido pareizs darbības nepārtrauktības pārvaldības (DNP) process, lai maksimāli palielinātu spēju pastāvīgi nodrošināt pakalpojumus un ierobežotu zaudējumus nopietnu darījumdarbības traucējumu gadījumā saskaņā ar Direktīvas 2013/36/ES 85. panta 2. punktu un EBI pamatnostādņu par iekšējo pārvaldību (EBA/GL/2017/11) VI sadaļu.

1.7.1. Ietekmes uz darījumdarbību analīze

78. Pareizas darbības nepārtrauktības pārvaldības ietvaros finanšu iestādēm ir jāveic darījumdarbības ietekmes analīze (DIA), kvantitatīvi un kvalitatīvi analizējot to pakļautību nopietniem darījumdarbības traucējumiem un novērtējot to iespējamo ietekmi (tostarp uz konfidencialitāti, integritāti un pieejamību), izmantojot iekšējo un/vai ārējo datu (piemēram, trešo personu – pakalpojumu sniedzēju datu, kas attiecas uz darījumdarbības procesu, vai publiski pieejamo datu, kas var būt saistīti ar DIA) un scenāriju analīzi. DIA ir jāņem vērā arī identificēto un klasificēto darījumdarbības funkciju, atbalsta procesu, trešo personu un informācijas aktīvu, kā arī to savstarpējās atkarības kritiskais svarīgums saskaņā ar 1.3.3. iedaļu.

79. Finanšu iestādēm ir jānodrošina, ka to IKT sistēmas un IKT pakalpojumi ir izstrādāti un saskaņoti ar to DIA, piemēram, veidojot dažu kritiski svarīgu komponentu rezervi, lai novērstu traucējumus, ko izraisa notikumi, kas ietekmē šos komponentus.

1.7.2. Darbības nepārtrauktības plānošana

80. Pamatojoties uz savām DIA, finanšu iestādēm ir jāizveido plāni darbības nepārtrauktības nodrošināšanai (darbības nepārtrauktības plāni, DNP), kas ir jādokumentē, un tie ir jāapstiprina to vadības struktūrām. Plānos jo īpaši ir jāapsver riski, kas varētu nelabvēlīgi ietekmēt IKT sistēmas un IKT pakalpojumus. Plānos ir jāietver atbalsts mērķiem aizsargāt un, ja vajadzīgs, atjaunot darījumdarbības funkciju konfidencialitāti, integritāti un pieejamību, atbalstot procesus un informācijas aktīvus. Šo plānu izstrādes laikā, ja vajadzīgs, finanšu iestādēm ir jāveic saskaņošana ar attiecīgām iekšējām un ārējām ieinteresētajām personām.

81. Finanšu iestādēm ir jāievieš darbības nepārtrauktības plāni, lai nodrošinātu, ka tās var pienācīgi reaģēt uz iespējamiem neveiksmju scenārijiem un ka tās spēj atgūt savas kritiski svarīgās darījumdarbības darbības pēc traucējumiem atjaunošanas laika mērķa (ALM, maksimālais laiks, kurā sistēma vai process ir jāatjauno pēc incidenta) un atjaunošanas punkta mērķa (APM, maksimālais laiks, kurā ir pieļaujams, ka incidenta gadījumā dati tiek zaudēti) ietvaros. Smagu darījumdarbības traucējumu gadījumos, kuriem vajadzīgi īpaši darbības nepārtrauktības plāni, finanšu iestādēm ir jānosaka prioritātes darījumdarbības turpināšanas darbībām, izmantojot uz risku balstītu pieeju, kuras pamatā var būt riska novērtējumi, kas veikti saskaņā ar 1.3.3. iedaļu. MPS tas var ietvert, piemēram, kritiski svarīgo darījumu turpmākās apstrādes atvieglošanu, turpinot stāvokļa uzlabošanas pasākumus.

82. Finanšu iestādei savos darbības nepārtrauktības plānos ir jāapsver virkne dažādu scenāriju, ar kuriem tā varētu saskarties, ietverot ārkārtas, bet iespējamus scenārijus, tostarp kiberuzbrukuma scenāriju, un ir jānovērtē šo scenāriju iespējamā ietekme. Pamatojoties uz šiem scenārijiem, finanšu iestādei ir jāapraksta, kā tiek nodrošināta IKT sistēmu un pakalpojumu nepārtrauktība, kā arī finanšu iestādes informācijas drošība.

1.7.3. Reaģēšanas un atjaunošanas plāni

83. Pamatojoties uz DIA (78. punkts) un ticamiem scenārijiem (82. punkts), finanšu iestādēm ir jāizstrādā reaģēšanas un atjaunošanas plāni. Šajos plānos ir jāprecizē, kādi apstākļi var izraisīt plānu aktivizēšanu un kādas darbības ir jāveic, lai nodrošinātu vismaz finanšu iestāžu kritiski svarīgo IKT sistēmu un IKT pakalpojumu pieejamību, nepārtrauktību un atjaunošanu. Reaģēšanas un atjaunošanas plāniem vajadzētu būt vērstiem uz finanšu iestāžu operāciju atjaunošanas mērķu sasniegšanu.

84. Reaģēšanas un atjaunošanas plānos ir jāapsver gan īstermiņa, gan ilgtermiņa atjaunošanās iespējas. Plānos vajadzētu:

    a) koncentrēties uz kritiski svarīgo darījumdarbības funkciju operāciju atjaunošanu, atbalsta procesiem, informācijas aktīviem un to savstarpējās atkarības faktoriem, lai novērstu nelabvēlīgu ietekmi uz finanšu iestāžu darbību un finanšu sistēmu, tostarp uz maksājumu sistēmām un maksājumu pakalpojumu lietotājiem, un lai nodrošinātu nenokārtoto maksājuma darījumu izpildi;
    b) tie ir jādokumentē un jānodrošina, ka tie ir pieejami darbības un atbalsta vienībām un tiem ir viegli piekļūt ārkārtas gadījumā;
    c) jāatjaunina, ņemot vērā incidentos, pārbaudēs gūto pieredzi, konstatētie jaunie riski, kā arī apdraudējumi un atjaunošanas mērķi un prioritātes, kam bijušas izmaiņas.

85. Plānos ir jāapsver arī alternatīvas iespējas, ja izmaksu, risku, loģistikas vai neparedzētu apstākļu dēļ atjaunošana īstermiņā var nebūt iespējama.

86. Turklāt reaģēšanas un atveseļošanas plānu ietvaros finanšu iestādei ir jāapsver un jāīsteno nepārtrauktības pasākumi, lai mazinātu trešo personu – pakalpojumu sniedzēju neveiksmes, kas ir būtiski svarīgi finanšu iestādes IKT pakalpojumu nepārtrauktībai (saskaņā ar EBI pamatnostādnēm par ārpakalpojumu izmantošanu (EBA/GL/2019/02) attiecībā uz darbības nepārtrauktības plāniem).

1.7.4. Plānu pārbaude

87. Finanšu iestādēm ir periodiski jāpārbauda savi DNP. Jo īpaši tām ir jānodrošina, ka to kritiski svarīgo darījumdarbības funkciju, atbalsta procesu, informācijas aktīvu un to savstarpējās atkarības faktoru (tostarp vajadzības gadījumā trešo personu nodrošināto) DNP tiek pārbaudīti vismaz reizi gadā, saskaņā ar 89. punktu.

88. DNP ir jāatjaunina vismaz reizi gadā, pamatojoties uz pārbaudes rezultātiem, jaunāko informāciju par apdraudējumiem un pieredzi, kas gūta no iepriekšējiem notikumiem. Jebkuras izmaiņas atjaunošanas mērķos (tostarp ALM un APM) un/vai izmaiņas darījumdarbības funkcijās, atbalsta procesos un informācijas aktīvos, vajadzības gadījumā ir arī jāapsver kā pamats DNP atjauninā̄šanai.

89. Finanšu iestādēm, pārbaudot savus DNP, ir jāparāda, ka tās spēj saglabāt savas darījumdarbības dzīvotspēju, līdz tiek atjaunotas kritiski svarīgās operācijas. Jo īpaši tām vajadzētu:

a) iekļaut atbilstošu, smagu, bet ticamu scenāriju kopuma pārbaudi, ietverot tos, kas tiek ņemti vērā DNP izstrādē (kā arī attiecīgā gadījumā trešo personu sniegto pakalpojumu pārbaudi); tajā ir jāiekļauj kritisko darījumdarbības funkciju pārslēgšana, atbalsta procesi un informācijas aktīvi ārkārtas situācijas seku novēršanas vidē un jāpierāda, ka tos var izmantot šādā veidā pietiekami ilgā laika posmā un ka pēc tam var atjaunot normālu darbību;
b) tās ir jāizstrādā tā, lai risinātu pieņēmumus, kuri ir DNP pamatā, ietverot pārvaldības režīmu un plānus saziņai krīzes laikā; un
c) jāiekļauj procedūras, kas vajadzīgas, lai pārbaudītu personāla un darbuzņēmēju, IKT sistēmu un IKT pakalpojumu spēju adekvāti reaģēt uz 89. punkta a) apakšpunktā noteiktajiem scenārijiem.

90. Pārbaužu rezultāti ir jādokumentē, kā arī jāanalizē visas identificētās nepilnības, kas izriet no pārbaudēm, tās jārisina un jāziņo vadības struktūrai.

1.7.5. Saziņa krīzes laikā

91. Finanšu iestādēm ir jānodrošina, ka traucējumu vai ārkārtas situācijas gadījumā, kā arī darbības nepārtrauktības plānu īstenošanas laikā tiem ir vajadzētu būt sagatavotiem efektīviem krīzes saziņas pasākumiem, lai visas attiecīgās iekšējās un ārējās ieinteresētās personas, tostarp kompetentās iestādes, ja to pieprasa valsts noteikumi, un arī attiecīgie pakalpojumu sniedzēji (ārpakalpojumu sniedzēji, darījumdarbības subjektu grupas vienības vai trešās personas – pakalpojumu sniedzēji) tiktu savlaicīgi un atbilstošā veidā informēti.

1.8. Maksājumu pakalpojumu lietotāja attiecību pārvaldība

92. MPS ir jāizveido un jāievieš procesi ar mērķi uzlabot MPL informētību par drošības riskiem, kas saistīti ar maksājumu pakalpojumiem, nodrošinot palīdzību un norādījumus MPL.

93. Maksājumu pakalpojumu lietotājiem (MPL) piedāvātā palīdzība un norādījumi ir jāatjaunina, ņemot vērā jaunus apdraudējumus un ievainojamību, un izmaiņas jāpaziņo MPL.

94. Ja produkta funkcionalitāte to pieļauj, MPS ir jāļauj MPL atspējot konkrētas maksājumu funkcijas, kas saistītas ar maksājumu pakalpojumiem, ko MPS piedāvā MPL.

95. Ja saskaņā ar Direktīvas (ES) 2015/2366 68. panta 1. punktu MPS ir vienojies ar maksātāju par tērēšanas limitu maksājumu darījumiem, kas veikti, izmantojot konkrētu maksājumu instrumentu, MPS ir jānodrošina maksātājam iespēja koriģēt šos ierobežojumus līdz maksimālajai robežai, par kuru ir notikusi vienošanās.

96. MPS ir jānodrošina MPL iespēja saņemt brīdinājumus par sāktiem maksājumu darījumiem un/vai neveiksmīgiem mēģinājumiem sākt maksājumu darījumus, kas ļauj tiem konstatēt krāpniecisku vai ļaunprātīgu savu kontu izmantošanu.

97. MPS ir pastāvīgi jāinformē MPL par drošības procedūru atjauninājumiem, kas ietekmē MPL saistībā ar maksājumu pakalpojumu nodrošināšanu.

98. MPS ir jānodrošina MPL palīdzība attiecībā uz visiem jautājumiem, pieprasījumiem par atbalstu un paziņojumiem par novirzēm vai problēmām attiecībā uz drošības jautājumiem, kas saistīti ar maksājumu pakalpojumiem. MPL vajadzētu būt pienācīgi informētiem par to, kā var saņemt šādu palīdzību.