EBA/GL/2017/05

11/09/2017

# Pamatnostādnes

## Pamatnostādnes par IKT riska novērtēšanu saskaņā ar Uzraudzības pārskata un novērtēšanas procesu (*SREP*)

# 1. Atbilstības un ziņošanas prasības

## Pamatnostādņu statuss

1. Šis dokuments ietver pamatnostādnes, kas izdotas saskaņā ar Regulas (EK) Nr. 1093/2010 16. pantu1. Kompetentajām iestādēm un finanšu iestādēm saskaņā ar Regulas (EK) Nr. 1093/2010 16. panta 3. punktu jādara viss iespējamais, lai ievērotu šīs pamatnostādnes.

2. Pamatnostādnēs izklāstīts EBI skatījums uz atbilstošām uzraudzības praksēm Eiropas Finanšu uzraudzības sistēmā jeb par to, kā konkrētā jomā jāpiemēro Savienības tiesību akti. Kompetentajām iestādēm, kas minētas Regulas (ES) Nr. 1093/2010 4.panta 2.punktā, uz kurām attiecas šīs pamatnostādnes, tās būtu 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 13.11.2017 jāpaziņo EBI, vai tās ievēro vai paredz ievērot šīs pamatnostādnes, vai jānorāda to neievērošanas iemesli. Ja šajā termiņā nebūs saņemts šāds paziņojums, EBI uzskatīs, ka kompetentās iestādes šos ieteikumus neievēro. Paziņojumi jāiesniedz, nosūtot EBI tīmekļa vietnē pieejamo veidlapu uz e-pasta adresi compliance@eba.europa.eu ar norādi „EBA/GL/2017/05”. Paziņojumus nosūta personas, kas ir pilnvarotas kompetento iestāžu vārdā ziņot par prasību izpildi. Par jebkurām izmaiņām atbilstības statusā arī ir jāziņo EBI.

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

1 Ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1093/2010 ( 2010. gada 24. novembris ), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), tiek grozīts Lēmums Nr. 716/2009/EK un atcelts Komisijas Lēmums 2009/78/EK (OV L331, 15.12.2010., 12.lpp).

# 2. Priekšmets, piemērošanas joma un definīcijas

## Priekšmets un piemērošanas joma

5. Šo pamatnostādņu, kas izstrādātas saskaņā ar Direktīvas 2013/36/ES[2] 107. panta 3. punktu, mērķis ir nodrošināt uzraudzības prakses konverģenci, novērtējot informācijas un komunikācijas tehnoloģiju (IKT) risku saskaņā ar uzraudzības pārskata un novērtēšanas procesu (*SREP*), kas minēts Direktīvas 2013/36/ES 97. pantā un papildus raksturots EBI pamatnostādnēs par kopējām procedūrām un metodoloģiju, ko izmanto uzraudzības pārskata un novērtēšanas procesā (*SREP*)[3]. Jo īpaši šīs pamatnostādnes precizē novērtējuma kritērijus, kas kompetentajām iestādēm jāpiemēro iestāžu pārvaldības un IKT stratēģijas uzraudzības novērtējumā un iestāžu IKT riska darījumu un kontroles pasākumu uzraudzības novērtējumā. Šīs pamatnostādnes ir EBI pamatnostādņu par *SREP* neatņemama sastāvdaļa.

6. Kompetentajām iestādēm jāpiemēro šīs pamatnostādnes atbilstoši *SREP* piemērošanas līmenim, kas norādīts EBI pamatnostādnēs par *SREP*, un saskaņā ar tajās noteikto minimālās iesaistīšanās modeli un proporcionalitātes prasībām.

## Adresāti

7. Šīs pamatnostādnes ir adresētas Regulas (ES) Nr. 1093/2010 4. panta 2. punkta i) apakšpunktā minētajām kompetentajām iestādēm.

## Definīcijas

8. Ja nav norādīts citādi, Direktīvā 2013/36/ES un Regulā (ES) Nr. 575/2013 izmantotajiem un definētajiem terminiem un EBI pamatnostādnēs *par SREP* noteiktajām definīcijām ir tāda pati nozīme šajās pamatnostādnēs. Šajās pamatnostādnēs papildus tiek piemērotas šādas definīcijas.

[2] Eiropas Parlamenta un Padomes Direktīva 2013/36/ES (2013. gada 26. jūnijs) par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu brokeru sabiedrību prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK1 (OV L 176, 27.6.2013.)

[3] EBA/GL/2014/13

| | |
|---|---|
| IKT sistēmas | IKT struktūra, kas ietilpst iestādes darbības atbalsta mehānismā vai savienojošajā tīklā. |
| IKT pakalpojumi | Pakalpojumi, kurus IKT sistēmas nodrošina vienam vai vairākiem iekšējiem vai ārējiem lietotājiem. Piemēram, datu ierakstīšanas, datu glabāšanas, datu apstrādes un ziņošanas pakalpojumi, kā arī uzraudzības, uzņēmējdarbības un lēmumu pieņemšanas atbalsta pakalpojumi. |
| IKT pieejamības un nepārtrauktības risks | Risks, ka IKT sistēmu darbība un pieejamība un dati tiek nelabvēlīgi ietekmēti, tostarp rodas nespēja laikus atjaunot iestādes sniegtos pakalpojumus, ko izraisa IKT aparatūras vai programmatūras sastāvdaļu atteice, IKT sistēmas pārvaldības nepilnības vai jebkurš cits notikums, kā papildus paskaidrots pielikumā. |
| IKT drošības risks | Risks, ka notiks neatļauta piekļuve IKT sistēmām un datiem no iestādes iekšienes vai ārpuses (piemēram, kiberuzbrukumi), kā papildus paskaidrots pielikumā. |
| IKT izmaiņu risks | Risks, ko rada iestādes nespēja laikus un kontrolētā veidā pārvaldīt IKT sistēmas izmaiņas, jo īpaši attiecībā uz lielām un sarežģītām izmaiņu programmām, kā papildus paskaidrots pielikumā. |
| IKT datu integritātes risks | Risks, ka IKT sistēmās uzglabātie un apstrādātie dati ir nepilnīgi, neprecīzi vai nesavienojami starp dažādām IKT sistēmām, piemēram, tādēļ, ka IKT kontroles pasākumi dažādos IKT datu dzīves cikla posmos ir vāji vai netiek īstenoti (t. i., izstrādājot datu arhitektūru, veidojot datu modeli un/vai datu vārdnīcas, pārbaudot ievadītos datus, kontrolējot datu ieguvi, pārsūtīšanu un apstrādi, tostarp atveidoto datu izvadi), tā pasliktinot iestādes spēju sniegt pakalpojumus un pareizi un laikus sagatavot (riska) pārvaldības un finanšu informāciju, kā papildus paskaidrots pielikumā. |
| IKT ārpakalpojumu radītais risks | Risks, ka, iesaistot trešo personu vai citu grupas vienību (ārpakalpojumi grupas ietvaros) IKT sistēmu vai ar tām saistītu pakalpojumu sniegšanā, tiks nelabvēlīgi ietekmēta iestādes darbība un riska pārvaldība, kā papildus paskaidrots pielikumā. |

# 3. Īstenošana

## Piemērošanas datums

9. Šīs pamatnostādnes piemēro no 2018. gada 1. janvāra.

# 4. Prasības IKT riska novērtējumam

## 1. sadaļa. Vispārēji noteikumi

10. Kompetentajām iestādēm jāveic IKT riska un pārvaldības mehānisma un IKT stratēģijas novērtējums *SREP* procesa ietvaros, izmantojot minimālās iesaistīšanās modeli un proporcionalitātes kritērijus, kas minēti EBI pamatnostādņu par *SREP* 2. sadaļā. Tas jo īpaši nozīmē, ka:

    a. IKT riska novērtējuma biežums būs atkarīgs no minimālās iesaistīšanās modeļa, ko nosaka iestādei piešķirtā *SREP* kategorija un tās konkrētā uzraudzības pārbaudes programma; un

    b. IKT novērtējuma dziļumam, detalizācijas pakāpei un intensitātei jābūt proporcionālai iestādes lielumam, struktūrai un operacionālajai videi, kā arī tās darbību raksturam, mērogam un sarežģītībai.

11. Visās šajās pamatnostādnēs proporcionalitātes principu piemēro uzraudzības iesaistes un dialoga ar iestādi apjomam, biežumam un intensitātei, un uzraudzības priekšstatiem par to, kādi standarti iestādei jāievēro.

12. Kompetentās iestādes var izmantot un ņemt vērā to darbu, ko iestāde vai kompetentā iestāde jau paveikusi saistībā ar citu risku vai *SREP* elementu novērtējumiem, lai varētu atjaunināt savu novērtējumu. Konkrēti, veicot šajās pamatnostādnēs minētos novērtējumus, kompetentajām iestādēm jāizvēlas vispiemērotākā uzraudzības novērtējuma metode un tāda metodika, kas ir vispiemērotākā un ir samērīga ar iestādi, tāpat kompetentajām iestādēm jāizmanto arī esošie un pieejamie dokumenti (piemēram, attiecīgie ziņojumi un citi dokumenti, sanāksmes ar (riska) pārvaldītājiem un konstatējumi uz vietas veiktās pārbaudēs), lai papildinātu kompetento iestāžu vērtējumu.

13. Kompetentajām iestādēm jāapkopo konstatējumi savos novērtējumos par šajās pamatnostādnēs minētajiem kritērijiem un jāizmanto tie, lai izdarītu secinājumus par *SREP* elementu novērtējumu, kā norādīts EBI pamatnostādnēs par *SREP*.

14. Jo īpaši novērtējumam par pārvaldību un IKT stratēģiju, kas veikts saskaņā ar šo pamatnostādņu 2. sadaļu, jārada secinājumi, kas informē par to konstatējumu kopsavilkumu, kuri iegūti, novērtējot iekšējo pārvaldību un iestādes mēroga kontroles pasākumus attiecībā uz katru *SREP* elementu, kā norādīts EBI pamatnostādņu par *SREP* 5. sadaļā, un tiem jāsniedz attiecīgs minētā *SREP* elementa izvērtējums. Kompetentajām iestādēm jāņem vērā arī tas, ka jebkura būtiska nelabvēlīga IKT stratēģijas novērtējuma ietekme uz iestādes darbības stratēģiju vai jebkuras bažas par to, ka iestādei var nepietikt IKT resursu un IKT spēju, lai varētu veikt un atbalstīt svarīgas plānotās stratēģiskās izmaiņas, ir jāiekļauj uzņēmējdarbības modeļa analīzē, kas veikts saskaņā ar EBI *SREP* pamatnostādņu 4. sadaļu.

15. IKT riska novērtējuma rezultāti, kā norādīti šo pamatnostādņu 3. sadaļā, jāņem vērā operacionālā riska novērtējuma secinājumos un jāuzskata par tādiem, kas ietekmē attiecīgo izvērtējumu, kā norādīts EBI pamatnostādņu par *SREP* 6.4. punktā.

16. Jāpiebilst, ka, lai gan vispārīgi kompetentajām iestādēm jāvērtē risku apakškategorijas pamatkategoriju ietvaros (t. i., IKT risks jāvērtē operacionālā riska ietvaros), ja kompetentās iestādes tomēr uzskata kādu apakškategoriju par būtisku, tās var vērtēt katru šādu apakškategoriju individuāli. Šim nolūkam, ja kompetentā iestāde atzīst IKT risku par būtisku, šīs pamatnostādnes ietver arī izvērtējuma tabulu (1. tabula), kas izmantojama, lai sniegtu atsevišķu apakškategorijas izvērtējumu IKT riskam, ievērojot EBI pamatnostādņu par *SREP* vispārējo pieeju tam, kā vērtējami kapitāla riski.

17. Lai noskaidrotu, vai IKT risks jāuzskata par būtisku un tādēļ to var novērtēt un piešķirt tam izvērtējumu kā atsevišķai operacionālā riska apakškategorijai, kompetentās iestādes var izmantot kritērijus, kas minēti EBI pamatnostādņu par *SREP* 6.1. punktā.

18. Piemērojot šīs pamatnostādnes, kompetentajām iestādēm attiecīgā gadījumā jāizskata pielikumā iekļautais neizsmeļošais saraksts ar IKT riska apakškategorijām un riska scenārijiem, ņemot vērā to, ka pielikums raksturo tos IKT riskus, kuri var radīt īpaši smagus zaudējumus. Kompetentās iestādes var izslēgt kādus IKT riskus, kas iekļauti šajā taksonomijā, ja tie nav būtiski novērtējumam. Paredzams, ka iestādes veidos pašas savu riska klasifikāciju, nevis izmantos pielikumā iekļauto IKT risku taksonomiju.

19. Ja šīs pamatnostādnes piemēro saistībā ar pārrobežu banku grupām un to vienībām un ir izveidota uzraudzības kolēģija, iesaistītajām kompetentajām iestādēm sadarbības ietvaros, ko tās īsteno saistībā ar *SREP* novērtējumu saskaņā ar EBI pamatnostādņu par *SREP* 11.1. punktu, visām grupas vienībām pēc iespējas konsekventāk būtu jāsaskaņo precīzi un sīki definētā katra informācijas elementa darbības joma.

# 2. sadaļa. Iestāžu pārvaldības un IKT stratēģijas novērtējums

## 2.1 Vispārējie principi

20. Kompetentajām iestādēm jānovērtē, vai iestādes vispārējā pārvaldība un iekšējās kontroles sistēma pienācīgi aptver IKT sistēmas un ar tām saistītos riskus un vai vadības struktūra pietiekami risina un pārvalda šos aspektus, jo IKT ir būtiskas pareizai iestādes darbībai.

21. Veicot šo novērtējumu, kompetentajām iestādēm jāatsaucas uz prasībām un standartiem par labu iekšējo pārvaldību un riska kontroles mehānismiem, kas minēti EBI Pamatnostādnēs par iekšējo pārvaldību (GL 44)[4] un starptautiskajās vadlīnijās šajā jomā, tādā mērā, kādā tās ir piemērojamas, ņemot vērā IKT sistēmu īpatnības un riskus.

22. Novērtējums šajā daļā neattiecas uz īpašiem elementiem IKT sistēmu pārvaldībā, riska pārvaldībā un kontroles pasākumos, kuri pievēršas konkrētu IKT risku pārvaldībai, kas apskatīti šo pamatnostādņu 3. sadaļā, bet attiecas uz šādām jomām:

    a. IKT stratēģija — vai iestādei ir IKT stratēģija, kas tiek pietiekami pārvaldīta un atbilst iestādes uzņēmējdarbības stratēģijai;

    b. vispārējā iekšējā pārvaldība — vai iestādes vispārējās iekšējās pārvaldības mehānismi ir pietiekami attiecībā uz iestādes IKT sistēmām; un

    c. IKT risks iestādes riska pārvaldības sistēmā — vai iestādes riska pārvaldības un iekšējās kontroles sistēma pietiekami aizsargā iestādes IKT sistēmas.

23. 22. punktā minētais a) apakšpunkts, kas sniedz informāciju par iestādes pārvaldības elementiem, galvenokārt jāņem vērā, novērtējot uzņēmējdarbības modeli, kas apskatīts EBI pamatnostādņu par *SREP* 4. sadaļā. Arī b) un c) apakšpunkts papildina novērtējumus par tematiem, kas apskatīti EBI pamatnostādņu par *SREP* 5. sadaļā, un novērtējums, kas aprakstīts šajās pamatnostādnēs, jāiekļauj attiecīgajā novērtējumā saskaņā ar EBI pamatnostādņu par *SREP* 5. sadaļu.

24. Šā novērtējuma rezultātiem attiecīgā gadījumā jāpapildina riska pārvaldības un kontroles pasākumu novērtējums, kas minēts šo pamatnostādņu 3. sadaļā.

## 2.2 IKT stratēģija

25. Šajā iedaļā kompetentajām iestādēm jānovērtē tas, vai iestādei ir izstrādāta IKT stratēģija — tā ir pakļauta pietiekamai pārraudzībai, ko veic iestādes vadības struktūra; tā atbilst uzņēmējdarbības

[4] EBI pamatnostādnes par iekšējo pārvaldību, *GL* 44, 2011. gada 27. septembris.

stratēģijai, jo īpaši attiecībā uz regulāru IKT atjaunināšanu un būtisku un sarežģītu IKT izmaiņu plānošanu vai ieviešanu; un tā sniedz atbalstu iestādes uzņēmējdarbības modelim.

### 2.2.1 IKT stratēģijas izstrāde un piemērotība

26. Kompetentajām iestādēm jānovērtē tas, vai iestādei ir izstrādāta sistēma, kas samērīga ar tās IKT darbību raksturu, mērogu un sarežģītību, lai varētu sagatavot un izstrādāt iestādes IKT stratēģiju. Veicot šo novērtējumu, kompetentajām iestādēm būtu jāapsver, vai:

    a. uzņēmējdarbības līnijas(-u) augstākā vadība[5] ir pietiekami iesaistīta iestādes stratēģisko IKT prioritāšu noteikšanā un tajā, vai, savukārt, IKT jomas augstākā līmeņa vadība ir informēta par uzņēmējdarbības pamata stratēģiju un iniciatīvu izstrādi, veidošanu un ierosināšanu, lai varētu nodrošināt pastāvīgu koordināciju starp IKT sistēmām, IKT pakalpojumiem, IKT funkciju (t. i., tām personām, kuras atbild par šo sistēmu un pakalpojumu pārvaldību un ieviešanu) un iestādes uzņēmējdarbības stratēģiju, un vai IKT tiek efektīvi atjauninātas;

    b. IKT stratēģija ir dokumentēta, un to atbalsta konkrēti īstenošanas plāni, jo īpaši attiecībā uz būtiskiem starpposma rezultātiem un resursu plānošanu (tostarp finanšu resursu un cilvēkresursu), lai nodrošinātu to reālistiskumu un varētu īstenot IKT stratēģiju;

    c. iestāde regulāri atjaunina savu IKT stratēģiju, jo īpaši gadījumos, kad mainās uzņēmējdarbības stratēģija, lai nodrošinātu pastāvīgu atbilstību starp IKT un darbības mērķiem, plāniem un pasākumiem vidējā termiņā un ilgtermiņā; un

    d. iestādes vadības struktūra apstiprina IKT stratēģiju un īstenošanas plānus un uzrauga to īstenošanu.

### 2.2.2 IKT stratēģijas īstenošana

27. Ja iestādes IKT stratēģija paredz īstenot būtiskas un sarežģītas izmaiņas IKT jomā vai izmaiņas ar būtisku ietekmi uz iestādes uzņēmējdarbības modeli, kompetentajām iestādēm jānovērtē, vai iestādei ir izstrādāta kontroles sistēma, kas pielāgota tās lielumam, IKT darbībām un darbības izmaiņu līmenim, lai atbalstītu efektīvu iestādes IKT stratēģijas īstenošanu. Veicot šo novērtējumu, kompetentajām iestādēm būtu jāapsver, vai kontroles sistēma:

    a. ietver pārvaldības procesus (piemēram, paveiktā darba un budžeta izpildes uzraudzību un ziņošanu) un attiecīgās struktūras (piemēram, projektu vadības biroju (PVB), IKT vadības grupu vai citu līdzīgu struktūru), lai varētu efektīvi atbalstīt IKT stratēģisko programmu īstenošanu;

    b. ir definējusi un sadalījusi pienākumus un atbildību par IKT stratēģisko programmu īstenošanu, pievēršot īpašu uzmanību galveno iesaistīto personu pieredzei svarīgu un sarežģītu IKT izmaiņu organizēšanā, vadīšanā un uzraudzībā un plašākas ietekmes uz organizāciju un cilvēkiem pārvaldībai (piemēram, pārvaldot pretošanos izmaiņām, mācības un saziņu);

[5] Augstākā vadība un vadības struktūra, kā definēts 2013. gada 26. jūnija Direktīvā 2013/36/ES — 3. panta 7. punktā "vadības struktūra" un 3. panta 9. punktā "augstākā vadība".

c. uzdod neatkarīgām kontroles un iekšējās revīzijas vienībām pārliecināties, ka ar IKT stratēģijas īstenošanu saistītie riski ir apzināti, novērtēti un efektīvi mīkstināti un ka IKT stratēģijas īstenošanai izstrādātā pārvaldības sistēma ir efektīva; un

d. paredz plānošanas un plānu pārskatīšanas procesu, kas nodrošina elastību, risinot būtiskas apzinātās problēmas (piemēram, radušās īstenošanas problēmas vai kavējumus) vai ārējas izmaiņas (piemēram, būtiskas izmaiņas uzņēmējdarbības vidē, tehnoloģiskās problēmas vai inovācijas), lai nodrošinātu, ka stratēģiskais īstenošanas plāns tiek laikus koriģēts.

## 2.3 Vispārējā iekšējā pārvaldība

28. Saskaņā ar EBI pamatnostādņu par *SREP* 5. sadaļu kompetentajām iestādēm jānovērtē, vai iestādei ir piemērota un pārredzama korporatīvā struktūra, kas ir "derīga paredzētajam mērķim", un vai iestāde ir ieviesusi piemērotus pārvaldības mehānismus. Īpaši ņemot vērā IKT sistēmas un saskaņā ar EBI pamatnostādnēm par iekšējo pārvaldību, šajā novērtējumā jāiekļauj novērtējums par to, vai iestāde pierāda, ka:

a) tai ir stabila un pārredzama organizatoriskā struktūra ar skaidru atbildību par IKT, tostarp vadības struktūra un tās komitejas, un galvenajām par IKT atbildīgajām personām (piemēram, informācijas vadītājam, operāciju direktoram vai citai līdzvērtīgai amatpersonai) ir pietiekama netieša vai tieša piekļuve vadības struktūrai, lai varētu nodrošināt, ka būtiska ar IKT saistīta informācija vai problēmas tiek atbilstoši paziņotas, apspriestas un izlemtas vadības struktūras līmenī; un

b) vadības struktūra ir informēta par riskiem, kas saistīti ar IKT, un risina tos.

29. Saskaņā ar EBI pamatnostādņu par *SREP* 5.2. punktu kompetentajām iestādēm jānovērtē, vai iestādes IKT ārpakalpojumu politika un stratēģija attiecīgā gadījumā ņem vērā IKT ārpakalpojumu ietekmi uz iestādes uzņēmējdarbību un uzņēmējdarbības modeli.

## 2.4 IKT risks iestādes riska pārvaldības sistēmā

30. Novērtējot iestādes riska pārvaldību un iekšējās kontroles pasākumus iestādes līmenī, kā paredzēts EBI pamatnostādņu par *SREP* 5. sadaļā, kompetentajām iestādēm jāapsver, vai iestādes riska pārvaldības un iekšējās kontroles sistēma pietiekami aizsargā iestādes IKT sistēmas tādā mērā, kas ir samērojams ar iestādes lielumu un darbību un tās IKT riska profilu, kā noteikts 3. sadaļā. Jo īpaši kompetentajām iestādēm jānosaka, vai:

a. vēlme uzņemties risku un *ICAAP* attiecas uz IKT riskiem kā daļu no plašākas operacionālā riska kategorijas, lai varētu definēt vispārējo riska stratēģiju un noteikt iekšējo kapitālu; un

b. IKT riski ietilpst iestādes līmeņa riska pārvaldības un iekšējās kontroles sistēmu piemērošanas jomā.

31. Kompetentajām iestādēm jāveic novērtējums saskaņā ar iepriekš esošo a) apakšpunktu, ņemot vērā gaidāmo un arī nelabvēlīgo scenāriju, piemēram, scenārijus, kas iekļauti konkrētās iestādes vai uzraudzības spriedzes testā.

32. Īpaši ņemot vērā b) apakšpunktu, kompetentajām iestādēm jānovērtē, vai neatkarīgās kontroles un iekšējās revīzijas vienības, kas minētas EBI pamatnostādņu par *SREP* 104. punkta a) un d) apakšpunktā un 105. punkta a) un c) apakšpunktā, ir piemērotas, lai varētu nodrošināt pietiekamu neatkarības līmeni starp IKT un kontroles un revīzijas vienībām, ņemot vērā iestādes lielumu un IKT riska profilu.

## 2.5 Konstatējumu kopsavilkums

33. Šie rezultāti jāiekļauj konstatējumu kopsavilkumā, kas paredzēts EBI pamatnostādņu par *SREP* 5. sadaļā, un tie jāņem vērā attiecīgā izvērtējumā atbilstoši apsvērumiem EBI pamatnostādņu par *SREP* 3. tabulā.

34. Novērtējot IKT stratēģiju, jāņem vērā šādi apstākļi, lai varētu pabeigt minēto novērtējumu:

a. ja kompetentās iestādes secina, ka iestādes pārvaldības sistēma nav atbilstīga, lai varētu izstrādāt un ieviest iestādes IKT stratēģiju saskaņā ar 2.2. punktu, tādā gadījumā tas jāņem vērā, novērtējot iestādes iekšējo pārvaldību saskaņā ar EBI pamatnostādņu par *SREP* 5. sadaļas 87. punkta a) apakšpunktu;

b. ja kompetentās iestādes no iepriekšējiem novērtējumiem saskaņā ar 2.2. punktu secina, ka veidosies ievērojama neatbilstība starp IKT stratēģiju un uzņēmējdarbības stratēģiju, kas var būtiski nelabvēlīgi ietekmēt iestādes ilgtermiņa darbības un/vai finanšu mērķus, iestādes ilgtspēju un/vai uzņēmējdarbības modeli, vai iestādes uzņēmējdarbības jomas/līnijas, kas noteikti kā visbūtiskākie EBI pamatnostādņu par *SREP* 62. punkta a) apakšpunktā, tādā gadījumā tas jānorāda uzņēmējdarbības modeļa novērtējumā, kas paredzēts pamatnostādņu par *SREP* 4. sadaļas 70. punkta b) un c) apakšpunktā; un

c. ja kompetentās iestādes no iepriekš minētajiem novērtējumiem saskaņā ar 2.2. punktu secina, ka iestādei var nebūt pietiekamu IKT resursu un IKT īstenošanas spēju, lai varētu ieviest un atbalstīt būtiskas plānotās stratēģiskās izmaiņas, tas jāņem vērā uzņēmējdarbības modeļa novērtējumā saskaņā ar EBI pamatnostādņu par *SREP* 4. sadaļas 70. punkta b) apakšpunktu.

# 3. sadaļa. Iestāžu IKT riska darījumu un kontroles pasākumu novērtējums

## 3.1 Vispārējie apsvērumi

35. Kompetentajām iestādēm jānovērtē tas, vai iestāde ir pareizi apzinājusi, novērtējusi un mazinājusi IKT riskus. Šim procesam jāiekļaujas operacionālā riska pārvaldības sistēmā un jābūt saderīgam ar pieeju, ko piemēro operacionālajam riskam.

36. Kompetentajām iestādēm vispirms ir jāapzina būtiskie raksturīgie IKT riski, kuriem ir vai var būt pakļauta iestāde, pēc tam jānovērtē iestādes IKT riska pārvaldības sistēmas, šā riska mazināšanas procedūru un kontroles pasākumu efektivitāte. Novērtējuma rezultāti jāiekļauj to konstatējumu kopsavilkumā, kurus ņem vērā, nosakot operacionālā riska izvērtējumu saskaņā ar pamatnostādnēm par *SREP*. Ja IKT risku atzīst par būtisku un kompetentās iestādes vēlas tam veltīt atsevišķu izvērtējumu, jāizmanto 1. tabula, izvērtējot to kā operacionālajam riskam pakārtotu risku.

37. Veicot novērtējumu saskaņā ar šo daļu, kompetentajām iestādēm jāizmanto visi pieejamie informācijas avoti, kā paredzēts EBI pamatnostādņu par *SREP* 6. sadaļas 127. punktā, piemēram, iestādes riska pārvaldības pasākumi, ziņojumi un rezultāti, kā pamats, lai varētu apzināt uzraudzības novērtējuma prioritātes. Kompetentajām iestādēm jāizmanto arī citi informācijas avoti, veicot šo novērtējumu, tostarp attiecīgā gadījumā šādi:

    a. IKT riska un kontroles pasākumu pašnovērtējumi (ja iesniegti *ICAAP* informācijā);
    b. ar IKT risku saistītā pārvaldības informācija (PI), kas iesniegta iestādes vadības struktūrai, piemēram, periodiskie un ar notikumiem saistītie IKT riska ziņojumi (tostarp operacionālo zaudējumu datubāzē) un dati par IKT riska darījumiem no iestādes riska pārvaldības vienības;
    c. ar IKT saistītās iekšējās un ārējās revīzijas slēdzieni, kas paziņoti iestādes revīzijas komitejai.

## 3.2 Būtisku IKT risku apzināšana

38. Kompetentajām iestādēm jāapzina būtiskie IKT riski, kuriem iestāde ir vai var būt pakļauta, veicot turpmāk minētos pasākumus.

### 3.2.1 Iestādes IKT riska profila pārskatīšana

39. Pārskatot iestādes IKT riska profilu, kompetentajām iestādēm jāizskata visa būtiskā informācija par iestādes IKT riska iedarbību, tostarp informācija saskaņā ar 37. punktu un apzinātās būtiskās nepilnības vai trūkumi IKT organizācijā un iestādes līmeņa kontroles pasākumos saskaņā ar šo pamatnostādņu 2. sadaļu, un attiecīgā gadījumā jāpārskata šī informācija proporcionālā veidā. Pārskatīšanas ietvaros kompetentajām iestādēm jāizvērtē:

    a. potenciālā ietekme, ko radītu ievērojami iestādes IKT sistēmu traucējumi uz finanšu sistēmu iekšzemes vai starptautiskā līmenī;

b. vai iestādei var rasties IKT drošības riski vai IKT pieejamības un darbības nepārtrauktības riski, ko nosaka atkarība no interneta, lielais daudzums novatorisko IKT risinājumu vai citu uzņēmējdarbības izplatīšanas kanālu, kas var palielināt kiberuzbrukumu iespējamību;
c. vai iestādei var palielināties IKT drošības riski, IKT pieejamības un darbības nepārtrauktības riski, IKT datu integritātes riski vai IKT izmaiņu riski, ko nosaka tās IKT sistēmu sarežģītība (piemēram, uzņēmumu apvienošanās vai iegādes rezultātā) vai novecojušais raksturs;
d. vai iestāde ievieš būtiskas izmaiņas savās IKT sistēmās un/vai IKT vienībā (piemēram, uzņēmumu apvienošanās, iegādes, atdalīšanās vai IKT pamatsistēmu nomaiņas rezultātā), kas var nelabvēlīgi ietekmēt IKT sistēmu stabilitāti vai pareizu darbību un var izraisīt būtiskus IKT pieejamības un darbības nepārtrauktības riskus, IKT drošības riskus, IKT izmaiņu riskus vai IKT datu integritātes riskus;
e. vai iestāde izmanto IKT vai IKT sistēmu ārpakalpojumus grupas ietvaros vai ārpus tās, un vai tas var radīt būtiskus IKT ārpakalpojumu riskus;
f. vai iestāde īsteno agresīvus IKT izmaksu samazināšanas pasākumus, kas var izraisīt nepieciešamo IKT ieguldījumu, resursu un IT ekspertīzes samazināšanos un palielināt visu to IKT risku veidu iedarbību, kuri norādīti taksonomijā;
g. vai svarīgu IKT darbību/datu centru atrašanās vieta (piemēram, reģioni vai valstis) var pakļaut iestādi dabas katastrofām (piemēram, plūdiem vai zemestrīcēm), politiskai nestabilitātei vai darba konfliktiem un pilsoņu nemieriem, kas var būtiski palielināt IKT pieejamības un darbības nepārtrauktības riskus un IKT drošības riskus.

### 3.2.2 Kritisko IKT sistēmu un pakalpojumu pārskatīšana

40. To IKT risku apzināšanas procesa ietvaros, kuri var radīt nozīmīgu prudenciālo ietekmi uz iestādi, kompetentajām iestādēm jāpārskata iestādes dokumentācija un jāsagatavo atzinums par to, kuras IKT sistēmas un pakalpojumi ir kritiski nepieciešami, lai varētu nodrošināt iestādes pamatdarbības atbilstošu norisi, pieejamību, nepārtrauktību un drošību.

41. Šajā nolūkā kompetentajām iestādēm jāpārskata metodika un procesi, ko iestāde piemēro, lai apzinātu IKT sistēmas un pakalpojumus, kas ir kritiski nepieciešami, ņemot vērā to, ka dažas IKT sistēmas un pakalpojumus iestāde var atzīt par kritiskiem uzņēmējdarbības nepārtrauktības un pieejamības aspektā, drošības aspektā (piemēram, krāpšanas novēršanai) un/vai konfidencialitātes aspektā (piemēram, datu konfidencialitāte). Veicot pārskatīšanu, kompetentajām iestādēm jāņem vērā tas, ka šīm kritiskajām IKT sistēmām un pakalpojumiem jāatbilst vismaz vienam no šādiem nosacījumiem:

a. tie atbalsta iestādes pamatdarbību un izplatīšanas kanālus (piemēram, bankomātus, interneta un mobilās bankas);

b. tie atbalsta būtiskos pārvaldības procesus un korporatīvās funkcijas, tostarp riska pārvaldību (piemēram, riska pārvaldības un kases pārvaldības sistēmas);

c. uz tiem attiecas īpašas juridiskās vai reglamentējošās prasības (ja tādas ir), kas paredz plašākas pieejamības, augstākas stabilitātes, konfidencialitātes vai drošības prasības (piemēram, datu aizsardzības tiesību akti vai iespējamie "atjaunošanas laika mērķi" (*RTO*, maksimālais laiks, kurā sistēma vai process jāatjauno pēc negadījuma) un "atjaunošanas punkta mērķis" (*RPO*,

maksimālais laikposms, kurā var zaudēt datus, iestājoties negadījumam)) attiecībā uz dažiem sistēmiski būtiskiem pakalpojumiem (ja un kad attiecināmi);

d. tie apstrādā vai uzglabā konfidenciālus vai jutīgus datus; neatļauta piekļuve tiem varētu būtiski ietekmēt iestādes reputāciju, finanšu rezultātus vai uzņēmējdarbības stabilitāti un nepārtrauktību (piemēram, datubāzes ar jutīgiem klientu datiem); un/vai

e. tie nodrošina pamatfunkcijas, kas ir būtiskas iestādes pareizai darbībai (piemēram, telekomunikāciju pakalpojumus, IKT un kiberdrošības pakalpojumus).

### 3.2.3 Būtisko IKT risku apzināšana kritiskajām IKT sistēmām un pakalpojumiem

42. Ņemot vērā pārskatīšanu, kas veikta iestādes IKT riska profilam un iepriekš minētajām kritiskajām IKT sistēmām un pakalpojumiem, kompetentajām iestādēm jāsagatavo atzinums par būtiskajiem IKT riskiem, kas saskaņā ar to uzraudzības lēmumu var būtiski ietekmēt iestādes kritisko IKT sistēmu un pakalpojumu uzraudzību.

43. Novērtējot IKT risku iespējamo ietekmi uz iestādes kritiskajām IKT sistēmām un pakalpojumiem, kompetentajām iestādēm jāņem vērā:

a. finansiālā ietekme, tostarp (bet ne tikai) līdzekļu vai aktīvu zaudējumi, iespējamās kompensācijas klientiem, juridiskās un sanācijas izmaksas, līgumiskie zaudējumi un zaudētie ieņēmumi;

b. uzņēmējdarbības traucējumu iespējamība, ņemot vērā (bet ne tikai) ietekmēto finanšu pakalpojumu kritiski svarīgo nozīmi; potenciāli skarto klientu un/vai filiāļu un darbinieku skaitu;

c. iespējamā ietekme uz iestādes reputāciju saistībā ar ietekmēto banku pakalpojumu vai operacionālo darbību kritiski svarīgo nozīmi (piemēram, klientu datu zādzība); skarto IKT sistēmu un pakalpojumu ārējais profils/redzamība (piemēram, mobilās vai tiešsaistes banku sistēmas, tirdzniecības vieta, bankomāti vai norēķinu sistēmas);

d. reglamentējošā ietekme, tostarp iespēja, ka regulators piemēros publisku cenzūru, naudas sodu vai pat mainīs atļaujas jomu;

e. stratēģiskā ietekme uz iestādi, piemēram, ja tiek apdraudēti vai nozagti stratēģiski svarīgi produkti vai uzņēmējdarbības plāni.

44. Pēc tam kompetentajām iestādēm jākartē apzinātie IKT riski, kas uzskatāmi par būtiskiem, iedalot tos turpmāk minētajās IKT riska kategorijās, kurām pielikumā ir sniegti papildu riska apraksti un piemēri. Kompetentajām iestādēm jāatzīst pielikumā norādītie IKT riski par daļu no novērtējuma saskaņā ar 3. sadaļu:

a. IKT pieejamības un nepārtrauktības risks
b. IKT drošības risks
c. IKT izmaiņu risks
d. IKT datu integritātes risks
e. IKT ārpakalpojumu radītais risks

Kartēšana palīdzēs kompetentajām iestādēm noteikt, kuri riski ir būtiski (ja tādi ir), tādēļ jāskata rūpīgāk un/vai dziļāk, veicot turpmākos novērtējuma pasākumus.

## 3.3 Kontroles pasākumu novērtējums, mazinot būtiskos IKT riskus

45. Lai novērtētu iestādes atlikušo IKT risku iedarbību, kompetentajam iestādēm jāpārskata tas, kā iestāde apzina, uzrauga, novērtē un mazina būtiskos riskus, ko kompetentās iestādes apzinājušas iepriekš minētajā novērtējumā.

46. Šim nolūkam attiecībā uz apzinātajiem būtiskajiem IKT riskiem, kompetentajām iestādēm jāpārskata spēkā esošā:

    a. IKT riska pārvaldības politika, procesi un riska pielaides robežvērtības;

    b. organizatoriskās pārvaldības un pārraudzības sistēma;

    c. iekšējās revīzijas apjoms un slēdzieni; un

    d. IKT riska kontroles pasākumi, kas īpaši attiecas uz apzināto būtisko IKT risku.

47. Novērtējumā jāņem vērā vispārējās riska pārvaldības un iekšējās kontroles sistēmas analīzes rezultāti, kā norādīts EBI pamatnostādņu par *SREP* 5. sadaļā, kā arī iestādes pārvaldība un stratēģija, kas apskatīta šo pamatnostādņu 2. sadaļā, jo būtisku nepilnību apzināšana šajās jomās var ietekmēt iestādes spēju pārvaldīt un mazināt IKT risku iedarbību. Ja attiecināms, kompetentajām iestādēm jāizmanto arī informācijas avoti, kas minēti šo pamatnostādņu 37. punktā.

48. Kompetentajām iestādēm jāveic turpmāk minētie novērtējuma pasākumi tādā veidā, kas ir samērīgs ar iestādes darbības raksturu, mērogu un sarežģītību, un jāveic tāda uzraudzības pārbaude, kas ir atbilstoša iestādes IKT riska profilam.

### 3.3.1 IKT riska pārvaldības politika, procesi un pielaides robežvērtības

49. Kompetentajām iestādēm jāpārskata, vai iestādei ir izstrādātas piemērotas riska pārvaldības politikas, procesi un pielaides robežvērtības attiecībā uz apzinātajiem būtiskajiem IKT riskiem. Tās var būt iekļautas operacionālā riska pārvaldības sistēmā vai atsevišķā dokumentā. Attiecībā uz šo novērtējumu kompetentajām iestādēm būtu jāapsver, vai:

    a. vadības struktūra ir formalizējusi un apstiprinājusi riska pārvaldības politiku un tajā ir pietiekami norādījumi par iestādes vēlmi uzņemties IKT risku un galvenajiem izvirzītajiem IKT riska pārvaldības mērķiem un/vai piemērotajām IKT riska pielaides robežvērtībām. Attiecīgā IKT riska pārvaldības politika jānosūta arī visām saistītajām ieinteresētajām personām;

    b. spēkā esošā politika aptver visus riska pārvaldībai svarīgos elementus attiecībā uz apzinātajiem būtiskajiem IKT riskiem;

    c. iestāde ir izstrādājusi procesu un pamatprocedūras attiecīgo būtisko IKT risku apzināšanai (piemēram, "riska un kontroles pašvērtējumi" *(RCSA)* un riska scenāriju analīze) un uzraudzībai; un

d. iestādei ir izstrādāta IKT riska pārvaldības ziņošanas kārtība, kas laikus nodrošina informāciju augstākajai vadībai un vadības struktūrai un ļauj šai augstākajai vadībai un/vai vadības struktūrai novērtēt un uzraudzīt, vai iestādes IKT riska mazināšanas plāni un pasākumi atbilst apstiprinātajai vēlmei uzņemties risku un/vai pielaides robežvērtībām (ja attiecināms), un uzraudzīt būtisko IKT risku izmaiņas.

### 3.3.2 Organizatoriskās pārvaldības un pārraudzības sistēma

50. Kompetentajām iestādēm jānovērtē, kā spēkā esošie riska pārvaldības pienākumi un atbildība ir iekļauta un integrēta iekšējā organizācijā, lai varētu vadīt un pārraudzīt apzinātos būtiskos IKT riskus. Šajā jomā kompetentajām iestādēm jānovērtē, vai iestāde pierāda:

a. ka ir skaidri pienākumi un atbildība, lai varētu apzināt, novērtēt, mazināt, paziņot un pārraudzīt attiecīgos būtiskos IKT riskus;
b. ka riska atbildība un pienākumi ir skaidri paziņoti, sadalīti un iekļauti visās attiecīgajās organizācijas daļās (piemēram, uzņēmējdarbības līnijās un IT) un procesos, tostarp arī pienākumi un atbildība par riska informācijas vākšanu un apkopošanu un tās paziņošanu augstākajai vadībai un/vai vadības struktūrai;
c. ka IKT riska pārvaldības pasākumi tiek īstenoti ar pietiekamiem un kvalitatīviem cilvēkresursiem un tehniskajiem resursiem. Lai varētu novērtēt spēkā esošo riska mazināšanas plānu ticamību, kompetentajām iestādēm arī jānovērtē, vai iestāde ir piešķīrusi pietiekamus finanšu līdzekļus un/vai citus nepieciešamos resursus to īstenošanai;
d. atbilstīgs turpinājuma darbs un vadības struktūras reakcija uz svarīgiem konstatējumiem, ko nodrošina neatkarīgas kontroles funkcijas attiecībā uz IKT risku(-iem), ņemot vērā dažu aspektu iespējamo deleģēšanu komitejai, ja tāda ir; un
e. izņēmumus no spēkā esošajiem IKT noteikumiem un politikām reģistrē, dokumentēti pārskata un paziņo neatkarīga kontroles funkcija, pievēršot uzmanību saistītajiem riskiem.

### 3.3.3 Iekšējās revīzijas apjoms un slēdzieni

51. Kompetentajām iestādēm jānovērtē, vai iekšējās revīzijas funkcija ir efektīva, veicot revīziju attiecībā uz spēkā esošo IKT riska kontroles sistēmu, pārskatot, vai:

a. IKT riska kontroles sistēma tiek revidēta nepieciešamajā kvalitātē, pietiekami dziļi un bieži un samērīgi ar iestādes lielumu, darbību un IKT riska profilu;
b. revīzijas plānā ir paredzēts revidēt kritiskos IKT riskus, ko apzinājusi iestāde;
c. svarīgie IKT revīzijas slēdzieni, tostarp saskaņotās darbības, ir paziņotas vadības struktūrai; un
d. IKT revīzijas slēdzieniem, tostarp saskaņotajām darbībām, tiek veikta pārraudzība, un progresa ziņojumus regulāri pārskata augstākā vadība un/vai revīzijas komiteja.

### 3.3.4 IKT riska kontroles pasākumi, kas īpaši attiecas uz apzinātajiem būtiskajiem IKT riskiem

52. Attiecībā uz apzinātajiem būtiskajiem IKT riskiem kompetentajām iestādēm jānovērtē, vai iestādei ir izstrādāti īpaši kontroles pasākumi šo risku novēršanai. Turpmākajās iedaļās ir iekļauts neizsmeļošs

saraksts ar īpašiem kontroles pasākumiem, kas jāizskata, novērtējot būtiskos riskus, kuri apzināti saskaņā ar 3.2.3. punktu, un tas ir kartēts šādās IKT riska kategorijās:

a. IKT pieejamības un darbības nepārtrauktības riski;
b. IKT drošības riski;
c. IKT izmaiņu riski;
d. IKT datu integritātes riski;
e. IKT ārpakalpojumu radītie riski.

### (a) Kontroles pasākumi būtisko IKT pieejamības un darbības nepārtrauktības risku pārvaldīšanai

53. Papildus EBI pamatnostādņu par *SREP* (279.–281. punkta) prasībām, kompetentajām iestādēm jānovērtē, vai iestādei ir izstrādāta piemērota sistēma IKT pieejamības un darbības nepārtrauktības risku apzināšanai, izprašanai, izmērīšanai un mazināšanai.

54. Attiecībā uz šo novērtējumu kompetentajām iestādēm būtu jo īpaši jāapsver, vai sistēma:

a. identificē kritiskos IKT procesus un attiecīgās IKT atbalsta sistēmas, kurām jābūt iekļautām uzņēmējdarbības stabilitātes un nepārtrauktības plānos ar:

   i. visaptverošu analīzi par savstarpējo saistību starp kritiskajiem uzņēmējdarbības procesiem un atbalsta sistēmām;

   ii. atkopšanas mērķu noteikšanu IKT atbalsta sistēmām (piemēram, parasti tos nosaka uzņēmums un/vai paredz *RTO* un *RPO* prasības);

   iii. veic atbilstošu darbības nepārtrauktības plānošanu, lai nodrošinātu, ka kritisko IKT sistēmu un pakalpojumu pieejamība, nepārtrauktība un atkopšana mazina iestādes darbības pārtraukumus pieņemamā līmenī.

b. uzrāda uzņēmējdarbības stabilitāti, tajā ir nepārtrauktības kontroles vides politikas, standarti un operacionālās kontroles pasākumi, kas ietver:

   i. pasākumus, kas novērš to, ka kāds atsevišķs scenārijs, negadījums vai katastrofa var ietekmēt IKT ražošanas un atkopšanas sistēmas;

   ii. IKT sistēmas dublēšanas un atkopšanas procedūras kritiskai programmatūrai un datiem, kas nodrošina šo dublējumu uzglabāšanu drošā un pietiekami attālinātā vietā, lai negadījums vai katastrofa nespētu šos kritiskos datus iznīcināt vai sabojāt;

   iii. uzraudzības risinājumus, lai varētu laikus atklāt IKT pieejamības vai darbības nepārtrauktības negadījumus;

   iv. dokumentētu incidentu pārvaldības un eskalācijas procesu, kas sniedz arī norādījumus par dažādiem negadījumu pārvaldības un eskalācijas pienākumiem un atbildību, krīzes komitejas(-u) locekļiem un komandķēdi ārkārtas gadījumā;

v. fiziskus pasākumus, lai aizsargātu iestādes kritisko IKT infrastruktūru (piemēram, datu centrus) no vides riskiem (piemēram, plūdiem un citām dabas katastrofām) un nodrošinātu piemērotu darbības vidi IKT sistēmām (piemēram, gaisa kondicionēšanu);

vi. procesus, pienākumus un atbildību, lai nodrošinātu, ka arī uz ārpakalpojumos nodotajām IKT sistēmām un pakalpojumiem attiecas piemēroti uzņēmējdarbības stabilitātes un nepārtrauktības risinājumi un plāni;

vii. IKT darbības un jaudas plānošanas un uzraudzības risinājumus kritiskajām IKT sistēmām un pakalpojumiem ar definētām pieejamības prasībām, lai varētu laikus atklāt būtiskus darbības un jaudas ierobežojumus;

viii. risinājumus, lai varētu aizsargāt kritiskās interneta darbības vai pakalpojumus (piemēram, e-bankas pakalpojumus), ja nepieciešams un attiecināms, pret pakalpojumu liegšanu un citiem kiberuzbrukumiem internetā, kuru mērķis ir nepieļaut vai traucēt piekļuvi šīm darbībām un pakalpojumiem.

c. sistēma testē IKT pieejamības un darbības nepārtrauktības risinājumus dažādos reālistiskos scenārijos, tostarp attiecībā uz kiberuzbrukumiem, kļūmjpārlēces testiem un dublēšanas testiem saistībā ar kritisko programmatūru un datiem, kas:

i. ir plānoti, formalizēti un dokumentēti, un šo testu rezultāti tiek izmantoti, lai stiprinātu IKT pieejamības un darbības nepārtrauktības risinājumu efektivitāti;

ii. ietver arī organizācijas ieinteresētās personas un funkcijas, piemēram, uzņēmējdarbības līniju vadību, tostarp darbības nepārtrauktības, negadījumu un krīzes reaģēšanas komandas, kā arī attiecīgas ārējās personas, kas ieinteresētas ekosistēmā;

iii. vadības struktūra un augstākā vadība ir pienācīgi iesaistīta (piemēram, krīzes vadības komandu sastāvā) un informēta par testu rezultātiem.

### (b) Kontroles pasākumi būtisko IKT drošības risku pārvaldīšanai

55. Kompetentajām iestādēm jānovērtē, vai iestādei ir izveidota efektīva sistēma IKT drošības risku apzināšanai, izprašanai, izmērīšanai un mazināšanai. Attiecībā uz šo novērtējumu kompetentajām iestādēm būtu jo īpaši jāņem vērā tas, vai sistēmai ir:

a. skaidri definēti pienākumi un atbildība attiecībā uz:

i. personu(-ām) un/vai komitejām, kas nodarbojas ar un/vai atbild par IKT drošības ikdienas pārvaldību un IKT drošības pamatpolitikas izstrādi, pievēršot uzmanību tām nepieciešamajai neatkarībai;
ii. IKT drošības kontroles pasākumu izstrādi, īstenošanu, vadību un uzraudzību;
iii. kritisko IKT sistēmu un pakalpojumu aizsardzību, piemēram, pieņemot ievainojamības novērtējuma procedūras, programmatūras ielāpu pārvaldības, darbstaciju aizsardzības (piemēram, pret ļaunprātīgas programmatūras vīrusiem), ielaušanās atklāšanas un novēršanas līdzekļus;

iv. ārēju vai iekšēju IKT drošības negadījumu uzraudzību, klasificēšanu un apstrādi, tostarp reaģēšanu uz negadījumiem un IKT sistēmu un pakalpojumu atsākšanu un atkopšanu;
v. regulāru un proaktīvu draudu novērtēšanu, lai uzturētu piemērotus drošības kontroles pasākumus.

b. IKT drošības politika, kas ņem vērā un attiecīgā gadījumā stingri ievēro starptautiski atzītos IKT drošības standartus un drošības principus (piemēram, "principle of least privilege ", t. i., ierobežojot piekļuvi ar minimālo līmeni, kas nodrošina normālu darbību attiecībā uz piekļuves tiesību pārvaldību, un “defence in depth” principu, t. i., slāņveida drošības mehānismiem, kas paaugstina sistēmas kopējo drošību, izstrādājot drošības arhitektūru);

c. procedūras, lai varētu apzināt IKT sistēmas, pakalpojumus un samērīgas drošības prasības, kas atbilst iespējamajam krāpšanas riskam un/vai iespējamajai konfidenciālo datu nepareizai un/vai ļaunprātīgai izmantošanai, kā arī dokumentētas drošības prasības, kas stingri jāizpilda attiecībā uz šīm apzinātajām IKT sistēmām, pakalpojumiem un datiem, atbilst iestādes riska pielaides līmenim un tiek uzraudzīta to pareiza izpilde;

d. dokumentētas drošības negadījumu pārvaldības un eskalācijas procedūras, kas sniedz arī norādījumus par dažādiem negadījumu pārvaldības un eskalācijas pienākumiem un atbildību, krīzes komitejas(-u) locekļiem un komandķēdi ārkārtas gadījumiem drošības jomā;

e. lietotāju un administratīvās darbības reģistrācija, lai varētu efektīvi uzraudzīt un laikus atklāt neatļautu darbību un reaģēt uz to, palīdzēt drošības negadījumu kriminālistiskā izmeklēšanā vai veikt šādu izmeklēšanu. Iestādē jābūt izstrādātai reģistrācijas politikai, kas definē atbilstīgus reģistrācijas ierakstu veidus un to uzglabāšanas laiku;

f. izpratnes veicināšanas un informācijas kampaņas vai iniciatīvas, lai informētu visus iestādes līmeņus par iestādes IKT sistēmu drošu lietošanu un aizsardzību un galvenajiem IKT drošības (un citiem) riskiem, kas ir jāapzinās, jo īpaši attiecībā uz esošajiem un topošajiem kiberdraudiem (piemēram, datorvīrusiem, iespējamo iekšējo vai ārējo ļaunprātīgo izmantošanu vai uzbrukumiem un kiberuzbrukumiem) un pienākumiem drošības pārkāpumu mazināšanā;

g. atbilstoši fiziskās drošības pasākumi (piemēram, videonovērošanas kameras, apsardzes signalizācija un drošības durvis), lai novērstu neatļautu fizisku piekļuvi kritiskām un jutīgām IKT sistēmām (piemēram, datu centriem);

h. pasākumi IKT sistēmu aizsardzībai pret uzbrukumiem no interneta (t. i., kiberuzbrukumiem) vai citiem ārējiem tīkliem (piemēram, tradicionālajiem telesakaru savienojumiem vai savienojumiem ar uzticamiem partneriem). Kompetentajām iestādēm jāpārskata, vai iestādes sistēma ņem vērā:

i. procesu un risinājumus, lai uzturētu pilnīgu un regulāri atjauninātu sarakstu un pārskatu par visiem uz āru vērstajiem tīkla savienojuma punktiem (piemēram, tīmekļa vietnēm, interneta lietotnēm, bezvadu internetu un attālināto piekļuvi), caur kuriem trešās personas varētu ielauzties iekšējās IKT sistēmās;

ii. stingri pārvaldītus un uzraudzītus drošības līdzekļus (piemēram, ugunsmūrus, starpniekserverus, e-pasta relejus, antivīrusu un satura skenerus), lai aizsargātu ienākošo un izejošo tīkla trafiku (piemēram, e-pastu), un uz āru vērstos tīkla savienojumus, caur kuriem trešās personas varētu ielauzties iekšējās IKT sistēmās;

iii. procesus un risinājumus, lai aizsargātu tīmekļa vietnes un lietotnes, kurām ir iespējams tieši uzbrukt no interneta un/vai ārpuses, kurus var izmantot kā ieejas punktus iekšējās IKT sistēmās. Parasti tā ir kombinācija, kas sastāv no atzītas drošas attīstības prakses, IKT sistēmas nostiprināšanas un ievainojamību skenēšanas prakses un/vai papildu drošības risinājumu ieviešanas, piemēram, tādu lietotņu kā ugunsmūris un/vai ielaušanās atklāšanas sistēma (*IDS*) un/vai pretielaušanās sistēma (*IPS*);

iv. regulāras drošības iekļūšanas pārbaudes, lai novērtētu īstenoto kiberpasākumu un iekšējo IKT drošības pasākumu un procesu efektivitāti. Šīs pārbaudes jāveic personālam un/vai ārējiem ekspertiem ar nepieciešamo kompetenci, dokumentējot pārbaužu rezultātus un secinājumus un paziņojot tos augstākajai vadībai un/vai vadības struktūrai. Ja nepieciešams un attiecināms, iestādei no šīm pārbaudēm jāmācās, kā papildus uzlabot drošības kontroles pasākumus un procesus un/vai iegūt pilnīgāku pārliecību par to efektivitāti.

### (c) Kontroles pasākumi būtisko IKT izmaiņu risku pārvaldīšanai

56. Kompetentajām iestādēm jānovērtē, vai iestādei ir izstrādāta efektīva sistēma IKT izmaiņu riska apzināšanai, izprašanai, mērīšanai un mazināšanai samērīgi ar iestādes darbības raksturu, mērogu un sarežģītību un iestādes IKT riska profilu. Iestādes sistēmai jāaptver riski, kas saistīti ar IKT sistēmu izmaiņu izstrādi, testēšanu un apstiprināšanu, tostarp programmatūras izstrādi vai izmainīšanu, pirms to pārcelšanas uz ražošanas vidi, un ar atbilstošas IKT dzīves cikla pārvaldības nodrošināšanu. Attiecībā uz šo novērtējumu kompetentajām iestādēm būtu jo īpaši jāņem vērā tas, vai sistēmai ir:

a. dokumentēti procesi IKT sistēmu izmaiņu pārvaldīšanai un kontrolēšanai (piemēram, konfigurācijas un ielāpu pārvaldībai) un datu pārvaldīšanai un kontrolēšanai (piemēram, kļūdu noteikšanai vai datu koriģēšanai), nodrošinot pienācīgu IKT riska pārvaldības iesaisti svarīgās IKT izmaiņās, kas var būtiski ietekmēt iestādes riska profilu vai iedarbību;

b. specifikācijas attiecībā uz nepieciešamo pienākumu sadali dažādos īstenoto IKT izmaiņu procesu posmos (piemēram, risinājuma izstrādē un izveidē, jaunas programmatūras un/vai izmaiņu testēšanā un apstiprināšanā, migrācijā un īstenošanā ražošanas vidē un kļūdu noteikšanā), akcentējot īstenotos risinājumus un pienākumu sadali, lai pārvaldītu un kontrolētu izmaiņas ražošanas IKT sistēmās un datos, ko veic IKT personāls (piemēram, izstrādātāji, IKT sistēmu administratori un datubāzu administratori) vai jebkuras citas personas (piemēram, lietotāji darba vajadzībām un pakalpojumu sniedzēji);

c. testēšanas vide, kas pietiekami atbilst ražošanas videi;

d. esošo lietotņu un IKT sistēmu aktīvu saraksts ražošanas vidē, kā arī testēšanas un izstrādes vidē, lai nepieciešamās izmaiņas (piemēram, versiju atjauninājumus vai uzlabojumus, sistēmu ielāpošanu un konfigurācijas izmaiņas) varētu pareizi pārvaldīt, īstenot un uzraudzīt attiecībā uz iesaistītajām IKT sistēmām;

e. procedūras izmantoto IKT sistēmu dzīves cikla uzraudzībai un pārvaldībai, lai varētu nodrošināt, ka tās arī turpmāk atbilst spēkā esošajām uzņēmējdarbības un riska pārvaldības prasībām un atbalsta tās, un nodrošināt, ka tirgotāji arī turpmāk atbalsta izmantotos IKT risinājumus un sistēmas un to visu papildina atbilstošas programmatūras izstrādes dzīves cikla *(SDLC*) procedūras;

f. programmatūras pirmkoda kontroles sistēma un atbilstošas procedūras neatļautu izmaiņu novēršanai programmatūras pirmkodā, kas izstrādātas pašā organizācijā;

g. procedūras jauno vai būtiski izmainīto IKT sistēmu un programmatūras drošības un neaizsargātības pārbaužu veikšanai pirms to laišanas ražošanā un pakļaušanas iespējamiem kiberuzbrukumiem;

h. procedūras un risinājumi konfidenciālo datu neatļautas vai netīšas izpaušanas novēršanai, nomainot, arhivējot, izmetot vai iznīcinot IKT sistēmas;

i. neatkarīgi pārskata un apstiprināšanas procesi, lai varētu samazināt cilvēka kļūdu riskus, veicot tādas izmaiņas IKT sistēmās, kas var būtiski kaitēt iestādes pieejamībai, darbības nepārtrauktībai vai drošībai (piemēram, būtiskas izmaiņas ugunsmūra konfigurācijā), vai iestādes drošībai (piemēram, izmaiņas ugunsmūros).

### (d) Kontroles pasākumi būtisko IKT datu integritātes risku pārvaldībai

57. Kompetentajām iestādēm jānovērtē, vai iestādei ir izstrādāta efektīva sistēma IKT datu integritātes riska apzināšanai, izprašanai, izmērīšanai un mazināšanai samērīgi ar iestādes darbības raksturu, mērogu un sarežģītību un iestādes IKT riska profilu. Iestādes sistēmai jāņem vērā riski, kas saistīti ar to datu integritātes saglabāšanu, kurus uzglabā un apstrādā IKT sistēmas. Attiecībā uz šo novērtējumu kompetentajām iestādēm būtu jo īpaši jāņem vērā tas, vai sistēmai ir:

a. politika, kas definē pienākumus un atbildību datu integritātes pārvaldīšanai IKT sistēmās (piemēram, datu arhitektam, datu aizsardzības amatpersonām [6], datu glabātājiem [7], datu īpašniekiem/pārziņiem[8]) un sniedz norādījumus par to, kuri dati ir kritiski datu integritātes aspektā un kuriem būtu jāveic īpaši IKT kontroles pasākumi (piemēram, automatizēti ievades apstiprināšanas kontroles pasākumi, datu pārsūtīšanas kontroles pasākumi, datu salīdzināšanas pasākumi u. c.) vai pārskati (piemēram, pārbaude par saderību ar datu arhitektūru) dažādos IKT datu dzīves cikla posmos;

b. dokumentēta datu arhitektūra, datu modelis un/vai vārdnīca, kas saskaņota ar attiecīgām iesaistītām personām uzņēmējdarbības un IT jomā, lai atbalstītu nepieciešamo datu konsekvenci visās IKT sistēmās un nodrošinātu to, ka datu arhitektūra, datu modelis un/vai vārdnīca arī turpmāk atbilst darbības un riska pārvaldības vajadzībām;

c. politika attiecībā uz gala lietotāja skaitļošanas *(End User Computing)* atļauto lietošanu un paļaušanos uz to, jo īpaši attiecībā uz svarīgu gala lietotāja skaitļošanas risinājumu apzināšanu, reģistrēšanu un dokumentēšanu (piemēram, apstrādājot svarīgus datus), un plānotajiem drošības līmeņiem, lai varētu novērst neatļautas izmaiņas gan pašā rīkā, gan tajā uzglabātajos datos;

d. dokumentēti izņēmumu apstrādes procesi, lai varētu risināt apzinātās IKT datu integritātes problēmas atbilstoši to kritiskumam un jutīgumam.

[6] Datu aizsardzības amatpersona atbild par datu apstrādi un lietošanu.

[7] Datu glabātājs atbild par datu drošu apsardzību, transportēšanu un uzglabāšanu.

[8] Datu pārzinis atbild par datu elementu pārvaldību un piemērotību — attiecībā uz saturu un metadatiem.

58. Attiecībā uz uzraudzītajām iestādēm, kas ietilpst Bāzeles Banku uzraudzības komitejas 239 efektīvas riska datu apkopošanas un riska ziņošanas principu[9] piemērošanas jomā, kompetentajām iestādēm jāpārskata iestādes riska analīze, ko nodrošina tās riska ziņošanas un datu apkopošanas spējas, salīdzinājumā ar principiem un par tiem sagatavoto dokumentāciju un ņemot vērā šo principu īstenošanas grafiku un pārejas mehānismus.

### (e) Kontroles pasākumi būtisko IKT ārpakalpojumu radīto risku pārvaldīšanai

59. Kompetentajām iestādēm jānovērtē, vai iestādes ārpakalpojumu stratēģija, kas atbilst *CEBS* pamatnostādņu par ārpakalpojumiem (2006. gads) prasībām un arī EBI pamatnostādņu par SREP 85. punkta d) apakšpunkta prasībai, tiek pareizi piemērota IKT ārpakalpojumiem, tostarp grupas iekšējiem ārpakalpojumiem, kas nodrošina IKT pakalpojumus grupas ietvaros. Novērtējot IKT ārpakalpojumu radītos riskus, kompetentajām iestādēm jāņem vērā tas, ka IKT ārpakalpojumu radītos riskus var daļēji apskatīt arī novērtējumā par raksturīgajiem operacionālajiem riskiem saskaņā ar EBI pamatnostādņu par *SREP* 240. punkta j) apakšpunktu, lai novērstu jebkādu darba dublēšanos vai divkāršu uzskaiti.

60. Kompetentajām iestādēm īpaši jānovērtē tas, vai iestādei ir izstrādāta efektīva sistēma IKT ārpakalpojumu radīto risku apzināšanai, izprašanai un izmērīšanai un jo īpaši kontroles pasākumi un kontroles vide, lai varētu mazināt riskus, kas saistīti ar būtiskiem IKT ārpakalpojumiem, kuri ir samērīgi ar iestādes lielumu, darbību un IKT riska profilu un ietver:

   a. novērtējumu par IKT ārpakalpojumu ietekmi uz iestādes riska pārvaldību saistībā ar pakalpojumu sniedzēju (piemēram, mākoņpakalpojumu sniedzēju) iesaisti un viņu pakalpojumiem iepirkuma procesa laikā, kas ir dokumentēts un ko augstākā vadība vai vadības struktūra ņem vērā, pieņemot lēmumu par kāda pakalpojuma nodošanu ārpakalpojumā. Iestādei jāpārskata IKT riska pārvaldības politika, IKT kontroles pasākumi un pakalpojumu sniedzēja kontroles vide, lai nodrošinātu, ka tā atbilst iestādes iekšējā riska pārvaldības mērķiem un vēlmei uzņemties risku. Šis pārskats ārpakalpojumu līguma perioda laikā regulāri jāatjaunina, ņemot vērā sniegto ārpakalpojumu raksturu;

   b. ārpakalpojumā nodotā pakalpojuma IKT risku uzraudzību ārpakalpojumu līguma perioda laikā iestādes riska pārvaldības ietvaros, uz kā pamata sagatavo iestādes IKT riska pārvaldības ziņojumus (piemēram, ziņojumus par uzņēmējdarbības nepārtrauktību un drošību);

   c. saņemto pakalpojumu uzraudzību un līmeņa salīdzinājumu ar līgumā noteikto pakalpojumu līmeni, kam jāietilpst ārpakalpojumu līgumā vai pakalpojuma līmeņa nolīgumā *(SLA)*; un

   d. pietiekamu darbinieku skaitu, resursus un kompetences, lai varētu uzraudzīt un pārvaldīt ārpakalpojumu radītos IKT riskus.

[9] Bāzeles komiteja banku uzraudzībai — Principi efektīvai riska datu apkopošanai un riska ziņošanai, 2013. gada janvāris, pieejami tiešsaistē: http://www.bis.org/publ/bcbs239.pdf.

## 3.4 Konstatējumu kopsavilkums un izvērtējums

61. Izmantojot iepriekš minēto novērtējumu, kompetentajām iestādēm jāsagatavo atzinums par iestādes IKT risku. Uz šā atzinuma pamata sagatavo konstatējumu kopsavilkumu, kurš kompetentajām iestādēm jāņem vērā, piešķirot operacionālā riska izvērtējumu saskaņā ar EBI *SREP* pamatnostādņu 6. tabulu. Kompetentajām iestādēm viedoklis par būtiskajiem IKT riskiem jāveido, pamatojoties uz turpmāk minētajiem apsvērumiem, kas iekļaujami operacionālā riska novērtējumā.

a. Riska apsvērumi

i. iestādes IKT riska profils un riska iedarbība;
ii. apzinātās kritiskās IKT sistēmas un pakalpojumi; un
iii. IKT riska būtiskums attiecībā uz kritiskajām IKT sistēmām.

b. Pārvaldības un kontroles pasākumu apsvērumi

i. vai pastāv atbilstība starp iestādes IKT riska pārvaldības politiku un stratēģiju un tās vispārējo stratēģiju un vēlmi uzņemties risku;
ii. vai IKT riska pārvaldības organizatoriskā sistēma ir stabila, ar skaidri noteiktiem pienākumiem un uzdevumu sadalījumu starp riska īpašniekiem un pārvaldības un kontroles funkcijām;
iii. vai IKT riska mērīšanas, uzraudzības un ziņošanas sistēmas ir piemērotas; un
iv. vai būtisko IKT risku kontroles sistēmas ir piemērotas.

62. Ja kompetentās iestādes atzīst IKT risku par būtisku un kompetentā iestāde pieņem lēmumu novērtēt šo risku un piešķirt tam punktus kā operacionālā riska apakškategorijai, turpmāk sniegtajā tabulā (1. tabula) ir sniegti apsvērumi par IKT riska izvērtējumu.

1. tabula. Uzraudzības apsvērumi IKT riska izvērtējumam

| Riska izvērtējums | Uzraudzības viedoklis | Raksturīgā riska apsvērumi | Pareizas pārvaldības un kontroles pasākumu apsvērumi |
|---|---|---|---|
| 1 | Nav konstatēts risks, ka radīsies nozīmīga prudenciālā ietekme uz iestādi, ņemot vērā raksturīgā riska līmeni, pārvaldību un kontroles pasākumus. | • Informācijas avoti, kas izmantojami saskaņā ar 37. punktu, nekonstatē nekādus būtiskus IKT riska darījumus.<br>• Analizējot iestādes IKT riska profila raksturu, kā arī pārskatot kritiskās IKT sistēmas un būtiskos IKT riskus IKT sistēmām un pakalpojumiem, nav konstatēti nekādi būtiski IKT riski. | |
| 2 | Mazs risks, ka radīsies nozīmīga prudenciālā | • Informācijas avoti, kas izmantojami saskaņā ar 37. punktu, nekonstatē nekādus | |

| | | | |
|---|---|---|---|
| | ietekme uz iestādi, ņemot vērā raksturīgā riska līmeni, pārvaldību un kontroles pasākumus. | būtiskus IKT riska darījumus.<br>• Analizējot iestādes IKT riska profila raksturu, kā arī pārskatot kritiskās IKT sistēmas un būtiskos IKT riskus IKT sistēmām un pakalpojumiem, ir konstatēti ierobežoti IKT riska darījumi (piemēram, ne vairāk kā 2 no 5 iepriekš noteiktajām IKT riska kategorijām). | • Iestādes IKT riska politika un stratēģija ir samērīga ar tās vispārējo stratēģiju un vēlmi uzņemties risku.<br>• IKT riska pārvaldības organizatoriskā sistēma ir stabila, ar skaidri noteiktiem pienākumiem un uzdevumu sadalījumu starp riska īpašniekiem un pārvaldības un kontroles funkcijām.<br>• IKT riska mērīšanas, uzraudzības un ziņošanas sistēmas ir piemērotas.<br>• IKT riska kontroles sistēma ir piemērota. |
| 3 | Vidējs risks, ka radīsies nozīmīga prudenciālā ietekme uz iestādi, ņemot vērā raksturīgā riska līmeni, pārvaldību un kontroles pasākumus. | • Informācijas avoti, kas izmantojami saskaņā ar 37. punktu, konstatē pazīmes, ka ir iespējami nozīmīgi IKT riska darījumi.<br>• Analizējot iestādes IKT riska profila raksturu, kā arī pārskatot kritiskās IKT sistēmas un būtiskos IKT riskus IKT sistēmām un pakalpojumiem, ir konstatēti paaugstināti IKT riska darījumi (piemēram, 3 vai vairāk no 5 iepriekš noteiktajām IKT riska kategorijām). | |
| 4 | Augsts risks, ka radīsies nozīmīga prudenciālā ietekme uz iestādi, ņemot vērā raksturīgā riska līmeni, pārvaldību un kontroles pasākumus. | • Informācijas avoti, kas izmantojami saskaņā ar 37. punktu, konstatē vairākas pazīmes par būtiskiem IKT riska darījumiem.<br>• Analizējot iestādes IKT riska profila raksturu, kā arī pārskatot kritiskās IKT sistēmas un būtiskos IKT riskus IKT sistēmām un pakalpojumiem, ir konstatēti augsta IKT riska darījumi (piemēram, 4 vai 5 no 5 iepriekš noteiktajām IKT riska kategorijām). | |

## Pielikums. IKT riska taksonomija

**Piecas IKT riska kategorijas ar neizsmeļošu tādu IKT risku sarakstu, kuriem potenciāli ir augsta pakāpe un/vai liela ietekme uz operacionālo, reputācijas vai finansiālo stāvokli**

| IKT riska kategorijas | IKT riski (neizsmeļošs saraksts[10]) | Riska apraksts | Piemēri |
|---|---|---|---|
| **IKT pieejamības un darbības nepārtrauktības riski** | Neatbilstoša kapacitātes pārvaldība | Nepietiekami resursi (piemēram, aparatūra, programmatūra, personāls, pakalpojumu sniedzēji) var izraisīt nespēju paplašināt pakalpojumu, lai apmierinātu uzņēmējdarbības vajadzības, novērstu sistēmas pārtraukumus, pakalpojuma pasliktināšanos un/vai operacionālas kļūdas. | • Jaudas nepietiekamība var ietekmēt pārraides ātrumu un tīkla (interneta) pieejamību tādiem pakalpojumiem kā interneta banka.<br>• Personāla trūkums (iekšējais vai trešās personas) var izraisīt sistēmas pārtraukumus un/vai operacionālas kļūdas. |
| | IKT sistēmas kļūmes | Pieejamības zaudēšana aparatūras kļūmes dēļ. | • Uzglabāšanas (cieto disku), serveru vai citu IKT iekārtu kļūmes/bojājumi, ko izraisa, piemēram, nepienācīga uzturēšana. |
| | | Pieejamības zaudēšana programmatūras kļūmes vai defekta dēļ. | • Bezgalīga cilpa lietotnes programmatūrā neļauj īstenot operāciju.<br>• Darbības pārtraukumi, ko izraisa novecojušu IKT sistēmu un risinājumu lietošana, lai gan tie vairs neatbilst pašreizējām pieejamības un stabilitātes prasībām un/vai tos vairs neatbalsta tirgotāji. |
| | Neatbilstoša IKT darbības nepārtrauktības un ārkārtas atkopšanas plānošana | Kļūme plānotajos IKT pieejamības un/vai darbības nepārtrauktības risinājumos, un/vai ārkārtas atkopšanā (piemēram, alternatīvajā atkopšanas datu centrā), aktivizējot, lai reaģētu uz negadījumu. | • Konfigurācijas atšķirības starp primāro un sekundāro datu centru var izraisīt alternatīvā datu centra nespēju nodrošināt plānoto pakalpojuma nepārtrauktību. |

[10] IKT riski ir iekļauti tajā riska kategorijā, kuru tie visvairāk ietekmē, taču tie var ietekmēt arī citas riska kategorijas.

| IKT riska kategorijas | IKT riski (neizsmeļošs saraksts[10]) | Riska apraksts | Piemēri |
|---|---|---|---|
| | Graujoši un destruktīvi kiberuzbrukumi | Dažādu nolūku vadīti uzbrukumi (piemēram, aktīvisms vai šantāža), kas izraisa sistēmu un tīkla pārslodzi, liedzot likumīgajiem lietotājiem piekļūt tiešsaistes datorpakalpojumiem. | • Izplatītie pakalpojuma liegšanas uzbrukumi tiek veikti, izmantojot daudzas interneta datorsistēmas, kuras kontrolē hakeris, un tās nosūta interneta pakalpojumiem (piemēram, e-bankai) lielu daudzumu šķietami leģitīmu pakalpojuma pieprasījumu. |
| **IKT drošības riski** | Kiberuzbrukumi un citi ārēji uzbrukumi saistībā ar IKT | Uzbrukumi, kas veikti no interneta vai ārējiem tīkliem un ir dažādu nolūku vadīti (piemēram, krāpšana, spiegošana, aktīvisms/sabotāža, kiberterorisms), izmantojot dažādus līdzekļus (piemēram, sociālā inženierija, ielaušanās mēģinājumi, izmantojot neaizsargātās vietas, ļaunprātīgas programmatūras izplatīšana), kas izraisa kontroles pārņemšanu pār iekšējām IKT sistēmām. | Dažādi uzbrukumu veidi<br>• *APT* (uzlabots pastāvīgs drauds) kontroles pārņemšanai pār iekšējām sistēmām vai informācijas zagšanai (piemēram, informācija, kas saistīta ar identitātes zādzību, un kredītkartes informācija).<br>• Ļaunprātīga programmatūra (piemēram, iebiedēšanas uzbrukumā), kas šifrē datus šantāžas nolūkā.<br>• Iekšējo IKT sistēmu inficēšana ar Trojas zirgu, lai varētu slēptā veidā veikt ļaunprātīgas darbības ar sistēmu.<br>• IKT sistēmas un/vai (tīkla) lietotnes neaizsargātības izmantošana (piemēram, *SQL* injekcija u. c.), lai iegūtu piekļuvi iekšējai IKT sistēmai. |
| | | Krāpniecisku norēķinu darījumu veikšana, ko hakeri īsteno, uzlaužot vai apejot e-bankas un norēķinu pakalpojumu drošības sistēmu un/vai uzbrūkot un izmantojot drošības ziņā neaizsargātās vietas iestādes iekšējās norēķinu sistēmās. | • Uzbrukumi e-bankai vai norēķinu pakalpojumiem, lai veiktu neatļautus darījumus.<br>• Krāpniecisku norēķinu darījumu izveide un izsūtīšana no iestādes iekšējām norēķinu sistēmām (piemēram, krāpnieciski *SWIFT* ziņojumi). |
| | | Krāpniecisku vērtspapīru darījumu veikšana, ko hakeri īsteno, uzlaužot vai apejot e-bankas pakalpojumu drošības sistēmas, tā iegūstot piekļuvi arī klientu vērtspapīru kontiem. | • "Pump and dump" uzbrukumi, kad uzbrucēji iegūst piekļuvi klientu e-bankas vērtspapīru kontiem un ievieto krāpnieciskus pirkšanas vai pārdošanas rīkojumus, lai ietekmētu tirgus cenu un/vai gūtu |

| IKT riska kategorijas | IKT riski (neizsmeļošs saraksts[10]) | Riska apraksts | Piemēri |
|---|---|---|---|
| | | | peļņu, izmantojot iepriekš izveidotas vērtspapīru pozīcijas. |
| | | Uzbrukumi komunikāciju savienojumiem un jebkura veida sarunām vai IKT sistēmām, lai ievāktu informāciju un/vai veiktu krāpšanu. | • Sarunu noklausīšanās/neaizsargātu autentifikācijas datu sūtījumu atklātā tekstā pārtveršana. |
| | Neatbilstoša iekšējā IKT drošība | Neatļautas piekļuves kritiskām IKT sistēmām iegūšana no iestādes iekšienes dažādiem nolūkiem (piemēram, krāpšana, negodīgu tirdzniecības darbību veikšana un slēpšana, datu zādzība, aktīvisms/sabotāža), izmantojot dažādus līdzekļus (piemēram, privilēģiju ļaunprātīga izmantošana un/vai eskalēšana, identitātes zādzības, sociālā inženierija, IKT sistēmu ievainojamības izmantošana, ļaunprātīgas programmatūras izplatīšana). | • Taustiņinformācijas (taustiņu datu) saglabātāju uzstādīšana, lai nozagtu lietotājvārdus un paroles un iegūtu neatļautu piekļuvi konfidenciāliem datiem un/vai veiktu krāpšanu.<br>• Vāju paroļu uzlaušana/uzminēšana, lai iegūtu nelikumīgas vai augstāka līmeņa piekļuves tiesības.<br>• Sistēmas administrators izmanto operētājsistēmas vai datubāzu lietotnes (veicot tiešas izmaiņas datubāzēs) krāpšanas veikšanai. |
| | | Neatļautas IKT manipulācijas, ko pieļauj neatbilstošas IKT piekļuves pārvaldības procedūras un prakse. | • Nevajadzīgu kontu neatspējošana vai neizdzēšana, piemēram, kad darbinieks maina amatu un/vai aiziet no iestādes, tostarp viesiem vai piegādātājiem, kuriem vairs nav vajadzīga piekļuve, kas nodrošina neatļautu piekļuvi IKT sistēmām.<br>• Pārāk lielu piekļuves tiesību un privilēģiju piešķiršana, kas nodrošina neatļautu piekļuvi un/vai pieļauj negodīgu darbību slēpšanu. |
| | | Drošības apdraudējumi, ko izraisa neinformētība drošības jomā, kuras dēļ darbinieki neizprot, neievēro vai neīsteno IKT drošības politiku un procedūras. | • Darbinieki, kuri tiek maldināti un palīdz veikt uzbrukumu (t. i., sociālā inženierija).<br>• Slikta prakse attiecībā uz pierakstīšanās informāciju — kopīgas paroles, "viegli uzminamu" paroļu lietošana, vienas paroles izmantošana dažādiem mērķiem utt.<br>• Nešifrētu konfidenciālu datu glabāšana klēpjdatoros un pārnēsājamos datu uzglabāšanas risinājumos (piemēram, USB zibatmiņās), ko var pazaudēt vai |

| IKT riska kategorijas | IKT riski (neizsmeļošs saraksts[10]) | Riska apraksts | Piemēri |
|---|---|---|---|
| | | | nozagt. |
| | | Konfidenciālas informācijas neatļauta glabāšana vai pārsūtīšana ārpus iestādes. | • Konfidenciālas informācijas nozagšana vai tīša nopludināšana vai nodošana nepiederošām personām vai plašai sabiedrībai. |
| | Neatbilstoša fiziskā IKT drošība | IKT aktīvu nepareiza izmantošana vai zādzība, tiem piekļūstot fiziski un radot šo aktīvu vai datu bojājumus vai zudumus vai padarot iespējamus citus apdraudējumus. | • Fiziska ielaušanās biroju ēkās un/vai datu centros, lai nozagtu IKT iekārtas (piemēram, datorus, klēpjdatorus, glabāšanas risinājumus) un/vai nokopētu datus, fiziski piekļūstot IKT sistēmām. |
| | | Tīši vai netīši bojājumi fiziskiem IKT aktīviem, ko rada terorisms, avārijas vai neveiksmīgas/kļūdainas manipulācijas, kuras veic iestādes darbinieki un/vai trešās personas (piegādātāji vai remontdarbinieki). | • Fiziskais terorisms (t. i., teroristu bumbas) vai IKT aktīvu sabotāža.<br>• Datu centra iznīcināšana ugunsgrēkā, ūdens noplūdē vai citos apstākļos. |
| | | Nepietiekama fiziskā aizsardzība pret dabas katastrofām, kas daļēji vai pilnībā iznīcina IKT sistēmas / datu centrus dabas katastrofā. | • Zemestrīces, pārmērīgs karstums, viesuļvētras, spēcīgi sniegputeņi, plūdi, ugunsgrēki un zibens spērieni. |
| **IKT izmaiņu riski** | Neatbilstoši IKT sistēmas izmaiņu un IKT izstrādes kontroles pasākumi | Negadījumi, kurus, piemēram, programmatūras, IKT sistēmu un datu izmaiņu rezultātā izraisa neatklātas kļūdas vai neaizsargātas vietas (piemēram, neparedzēta izmaiņu ietekme vai nepietiekamas testēšanas vai nepareizas izmaiņu pārvaldības prakses rezultātā slikti pārvaldītas izmaiņas). | • Nepietiekami testētas programmatūras vai konfigurācijas izmaiņu laišana ražošanā, kas rada neparedzētu nelabvēlīgu ietekmi uz datiem (piemēram, to bojājumus vai izdzēšanu) un/vai IKT sistēmas darbību (piemēram, tās avāriju vai darbības pasliktināšanos).<br>• Nekontrolētas IKT sistēmu vai datu izmaiņas ražošanas vidē.<br>• Vāji aizsargātu IKT sistēmu un interneta lietotņu laišana ražošanā, radot iespējas hakeriem uzbrukt sniegtajiem interneta pakalpojumiem un/vai ielauzties iekšējās IKT sistēmās.<br>• Nekontrolētas izmaiņas iekšēji izstrādātas programmatūras pirmkodā.<br>• Nepietiekama testēšana, kuras cēlonis ir neatbilstoša testēšanas vide. |

| IKT riska kategorijas | IKT riski (neizsmeļošs saraksts[10]) | Riska apraksts | Piemēri |
|---|---|---|---|
| | Neatbilstoša IKT arhitektūra | Vāja IKT arhitektūras pārvaldība, izstrādājot, veidojot un uzturot IKT sistēmas (piemēram, programmatūru, aparatūru un datus), laika gaitā var izraisīt to, ka IKT sistēmas kļūst sarežģīti, grūti un dārgi pārvaldāmas un smagas, vairs nepietiekami atbilstošas uzņēmējdarbības vajadzībām un nederīgas jaunākajām riska pārvaldības prasībām. | • Neatbilstoši pārvaldītas izmaiņas IKT sistēmās, programmatūrā un/vai datos ilgstošā laika posmā izraisa situāciju, kad IKT sistēmas un arhitektūras kļūst sarežģīti, neviendabīgi un grūti pārvaldāmas, radot daudzas nelabvēlīgas ietekmes uz uzņēmējdarbības un riska pārvaldību (piemēram, elastības un manevrētspējas zaudēšana, IKT negadījumi un kļūmes, lielas darbības izmaksas, novājināta IKT drošība un elastīgums, pazemināta datu kvalitāte un ziņošanas spējas).<br>• Komerciālo programmatūras pakotņu pārmērīga pielāgošana un piesaiste iekšēji izstrādātajai programmatūrai, kas rada nespēju ieviest turpmākos šīs komerciālās programmatūras izlaides un atjauninājumus un risku, ka tirgotājs vairs šo programmatūru neatbalstīs. |
| | Neatbilstoša dzīves cikla un ielāpu pārvaldība | Neatbilstoša tāda visu IKT aktīvu saraksta uzturēšana, kas varētu atbalstīt un papildināt pareizu dzīves cikla un ielāpu pārvaldības praksi. Tas rada situāciju, kad IKT sistēmas kļūst nepietiekami salāpītas (un tādēļ mazāk aizsargātas) un novecojušas, vairs nespējot atbalstīt uzņēmējdarbības un riska pārvaldības vajadzības. | • Nesalāpītas un novecojušas IKT sistēmas, kas var radīt nelabvēlīgu ietekmi uz uzņēmējdarbību un riska pārvaldību (piemēram, zaudējot elastību un manevrētspēju, pārtraucot IKT darbību, novājinot IKT drošību un elastīgumu). |
| **IKT datu integritātes riski** | Disfunkcionāla IKT datu apstrāde | Sistēmas, sakaru un/vai lietotņu kļūdu un kļūmju dēļ vai kļūdaini veicot datu ieguves, pārsūtīšanas un ielādēšanas *(ETL)* procesu, datus var sabojāt vai pazaudēt. | • IT sistēmas kļūda partiju apstrādē, kas rada nepareizas bilances klientu bankas kontos.<br>• Nepareizi izpildīti datu pieprasījumi.<br>• Datu zaudējums, ko izraisa datu replikācijas (dublēšanas) kļūda. |
| | Nepareizi izstrādāti datu apstiprināšanas kontroles | Kļūdas, kas saistītas ar neesošu vai neefektīvu automātiskās datu ievades un apstiprināšanas kontroli (piemēram, attiecībā uz izmantotiem trešo personu datiem) un datu pārsūtīšanas, apstrādes un izvades | • Datu ievades nepietiekama vai nederīga formatēšana/apstiprināšana lietotnēs un/vai lietotāju saskarnēs.<br>• Datu salīdzināšanas kontroles neesamība attiecībā |

| IKT riska kategorijas | IKT riski (neizsmeļošs saraksts[10]) | Riska apraksts | Piemēri |
|---|---|---|---|
| | pasākumi IKT sistēmās | kontroli IKT sistēmās (piemēram, ievades derīguma kontroli un datu salīdzināšanu). | uz radītajiem izejas datiem<br>• Kontroles neesamība attiecībā uz izpildītajiem datu izvilkuma procesiem (piemēram, datubāzes pieprasījumiem), radot kļūdainus datus.<br>• Kļūmīgu ārējo datu izmantošana. |
| | Nepietiekami kontrolētas datu izmaiņas ražošanas IKT sistēmās | Datu kļūdas, kas ieviesušās tādēļ, ka netiek pietiekami kontrolēta pareizība un pamatotība datu manipulācijām IKT sistēmu ražošanā. | • Izstrādātāji vai datubāzu administratori, kuriem ir tieša piekļuve un kuri nekontrolēti izmaina datus ražošanas IKT sistēmās, piemēram, notiekot IKT negadījumam. |
| | Nepareizi izstrādāta un/vai pārvaldīta datu arhitektūra, datu plūsmas, datu modeļi vai datu vārdnīcas | Nepareizi pārvaldīta datu arhitektūra, datu modeļi, datu plūsmas vai datu vārdnīcas var radīt vairākas to pašu datu versijas IKT sistēmās, un tie vairs nebūs saskanīgi, jo tiks atšķirīgi piemēroti datu modeļi vai datu definīcijas un/vai atšķirsies pamatā esošais datu ģenerēšanas un izmainīšanas process. | • Atšķirīgu klientu datubāzu esamība atsevišķam produktam vai iestādes vienībai, kas satur atšķirīgas datu definīcijas un laukus, rada nesalīdzinātus un grūti salīdzināmus integrētos klientu datus visas finanšu iestādes vai grupas līmenī. |
| **IKT ārpakalpojumu radītie riski** | Neatbilstoša trešās personas vai citas grupas vienības pakalpojumu elastība | Kritisku ārpakalpojumā nodotu IKT pakalpojumu, telesakaru pakalpojumu un iekārtu nepieejamība. Pakalpojumu sniedzējam uzticētu kritisku/jutīgu datu zudumi vai bojājumi. | • Pamatpakalpojumu nepieejamība, ko izraisa kļūmes (ārpakalpojumu) piegādātāju IKT sistēmās vai lietotnēs.<br>• Sakaru savienojumu pārtraukumi.<br>• Energoapgādes traucējumi. |
| | Neatbilstoša ārpakalpojumu pārvaldība | Būtiska pakalpojumu pasliktināšanās vai kļūmes, ko rada ārpakalpojumu sniedzēja neefektīva sagatavotība vai kontroles procesi.<br>Neefektīva ārpakalpojumu pārvaldība var izraisīt nepieciešamo prasmju un spēju trūkumu pilnībā apzināt, novērtēt, mazināt un uzraudzīt IKT riskus, un tā var ierobežot iestādes operacionālās spējas. | • Nekvalitatīvas negadījumu apstrādes procedūras, nepietiekami līgumiskie kontroles mehānismi un garantijas, kas paredzētas pakalpojumu sniegšanas nolīgumā un palielina atbildīgo personu atkarību no trešām personām un tirgotājiem.<br>• Neatbilstoša izmaiņu pārvaldības kontrole attiecībā uz pakalpojumu sniedzēja IKT vidi var izraisīt būtisku pakalpojumu pasliktināšanos vai kļūmes. |

| IKT riska kategorijas | IKT riski (neizsmeļošs saraksts[10]) | Riska apraksts | Piemēri |
|---|---|---|---|
| | Neatbilstoša trešās personas vai citas grupas vienības drošība | Hakeru uzbrukumi trešo personu pakalpojumu sniedzēju IKT sistēmām, kas tieši ietekmē ārpakalpojumus vai kritiskos/konfidenciālos datus, kurus glabā pakalpojumu sniedzējs.<br>Pakalpojumu sniedzēja darbinieki iegūst neatļautu piekļuvi kritiskajiem/jutīgajiem datiem, kurus glabā pakalpojumu sniedzējs. | • Noziedznieku vai teroristu hakeru uzbrukumi pakalpojumu sniedzējiem kā ieejas punktam iestādes IKT sistēmās vai lai piekļūtu/iznīcinātu kritiskos vai jutīgos datus, kurus glabā pakalpojumu sniedzējs.<br>• Ļaunprātīgi pakalpojumu sniedzēja darbinieki mēģina nozagt un pārdot jutīgus datus. |